HARDENING WINDOWS SERVER 2019

Daniel Hidalgo Pagés

· CreateNewLocalAdminAccount, #Mandatory otherwise the system access is lost

```
function CreateNewLocalAdminAccount {
    CreateUserAccount $NewLocalAdmin $NewLocalAdminPassword $true
}
```

Esta función crea una nueva cuenta de administrador local. Toma tres parámetros como argumentos: el nombre de la nueva cuenta de administrador local, la contraseña de la nueva cuenta de administrador local y un indicador booleano para indicar si la cuenta se debe habilitar. Esta función crea una nueva cuenta de usuario con los parámetros proporcionados, y si el indicador booleano es verdadero, habilita la cuenta.

· RenameAdministratorAccount, #2.3.1.5

```
function RenameAdministratorAccount {
    #2.3.1.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account
    Write-Info "2.3.1.5 (L1) Configure 'Accounts: Rename administrator account'"
    SetSecurityPolicy "NewAdministratorName" ("`"$($AdminNewAccountName)`"")
    Set-LocalUser -Name $AdminNewAccountName -Description " "
}
```

Esta función renombra la cuenta de administrador local. Toma dos argumentos como parámetros: el nuevo nombre de la cuenta de administrador local y el nombre de la cuenta de administrador local actual. Esta función actualiza la configuración de seguridad especificada para renombrar la cuenta de administrador local con el nombre proporcionado. Esta función también actualiza el nombre de la cuenta de usuario local con el nuevo nombre proporcionado.

· RenameGuestAccount, #2.3.1.6

```
function RenameGuestAccount {
    #2.3.1.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account
    Write-Info "2.3.1.6 (L1) Configure 'Accounts: Rename guest account'"
    SetSecurityPolicy "NewGuestName" ("`"$($GuestNewAccountName)`"")
    Set-LocalUser -Name $GuestNewAccountName -Description " "
}
```

Esta función renombra la cuenta de invitado local. Toma dos argumentos como parámetros: el nuevo nombre de la cuenta de invitado local y el nombre de la cuenta de invitado local actual. Esta función actualiza la configuración de seguridad especificada para renombrar la cuenta de invitado local con el nombre proporcionado. Esta función también actualiza el nombre de la cuenta de usuario local con el nuevo nombre proporcionado.

· EnforcePasswordHistory, #1.1.1

```
function EnforcePasswordHistory
{
    #1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored)
    Write-Info "1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored)"
    Write-Before ("Before hardening: *******                ")
    Write-Output ( net accounts | Select-String -SimpleMatch 'Length of password history maintained' )
    Write-After ("After hardening: *******                  ")
    net accounts /uniquepw:24
}
```

Esta función establece la configuración "Enforce password history" para asegurar que se mantengan 24 o más contraseñas. Toma un parámetro como argumento: el número de contraseñas que se deben mantener. Esta función imprime el estado actual de la configuración antes de aplicar el ajuste, luego aplica el ajuste con el comando net accounts y finalmente imprime el estado de la configuración después de aplicar el ajuste.

· MaximumPasswordAge, #1.1.2

```
function MaximumAccountPasswordAge {
    #2.3.6.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age
    Write-Info "2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge" (,"4,30")
}
```

La función MaximumAccountPasswordAge establece la política de seguridad "MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge" con el valor "4,30". Esta política de seguridad especifica el número máximo de días permitidos para que una cuenta de máquina tenga la misma contraseña antes de que expire. Esto se debe a que, si una cuenta de máquina mantiene la misma contraseña por un período de tiempo prolongado, aumenta el riesgo de que un atacante la descifre. Establecer el valor de la política en "30 o menos días, pero no en 0" ayuda a proteger los recursos de la red.

· MinimumPasswordAge, #1.1.3

```
function MinimumPasswordAge
{

    #1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Scored)
    Write-Info "1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Scored)"
    Write-Before ("Before hardening: *******                ")
    Write-Output (net accounts | Select-String -SimpleMatch 'Minimum password age' )
    Write-After ("After hardening: *******                  ")
    net accounts /minpwage:1
}
```

La función MinimumPasswordAge establece la política de seguridad "MinimumPasswordAge" con el valor "1". Esta política de seguridad especifica el número mínimo de días que un usuario debe esperar antes de cambiar su contraseña. Esto ayuda a evitar que los usuarios cambien sus contraseñas demasiado a menudo y a garantizar que su contraseña se mantenga segura durante un período de tiempo prolongado. Establecer el valor de la política en "1 o más día (s)" ayuda a proteger los recursos de la red.

· MinimumPasswordLength, #1.1.4

```powershell
function MinimumPasswordLength{

    #1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Scored)
    Write-Info "1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Scored)"
    Write-Before ("Before hardening: *******              ")
    Write-Output ( net accounts | Select-String -SimpleMatch 'Minimum password length')
    Write-After ("After hardening: *******                ")
    net accounts /MINPWLEN:14
}
```

La función MinimumPasswordLength establece la política de seguridad "Minimum password length" con el valor de "14 o más caracteres". Esta política de seguridad especifica el número mínimo de caracteres que un usuario debe usar al elegir

· WindowsPasswordComplexityPolicyMustBeEnabled, #1.1.5

```powershell
function WindowsPasswordComplexityPolicyMustBeEnabled
{

    #1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Scored)
    Write-Info "1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Scored)"
    secedit /export /cfg ${env:appdata}\secpol.cfg
    (Get-Content ${env:appdata}\secpol.cfg).replace("PasswordComplexity = 0", "PasswordComplexity = 1") | Out-File ${env:appdata}\secpol.cfg
    secedit /configure /db c:\windows\security\local.sdb /cfg ${env:appdata}\secpol.cfg /areas SECURITYPOLICY
    Remove-Item -force ${env:appdata}\secpol.cfg -confirm:$false

}
```

Habilita la política de complejidad de la contraseña de Windows. Utiliza el comando "secedit" para exportar y configurar la directiva de seguridad, y luego reemplaza la directiva de complejidad de contraseña para habilitarla. A continuación, elimina el archivo de configuración temporal que se ha creado. Esto garantiza que la configuración de seguridad se aplique a todos los usuarios.

Secedit configura y analiza la seguridad del sistema comparando la configuración de seguridad actual con las plantillas de seguridad especificadas.

· AccountLockoutDuration, #1.2.1

```powershell
function AccountLockoutDuration
{

    #1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored)
    Write-Info "1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored)"
    Write-Before ("Before hardening: *******              ")
    Write-Output ( net accounts | Select-String -SimpleMatch 'lockout duration')

    Write-After ("After hardening: *******                ")
    net accounts /lockoutduration:30
}
```

Esta función establece la duración de bloqueo de la cuenta en 15 minutos o más. Utiliza el comando "net accounts" para mostrar el estado actual de la directiva de bloqueo de cuenta y luego establece la duración de bloqueo de cuenta en 30 minutos. Esto garantiza que las cuentas estén bloqueadas durante un período suficiente de tiempo para evitar intentos de inicio de sesión automatizados.

· DisablePasswordReversibleEncryption, #1.1.6

```powershell
function DisablePasswordReversibleEncryption {

    #1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Scored)
    Write-Info "1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Scored)"
    secedit /export /cfg ${env:appdata}\secpol.cfg
    (Get-Content ${env:appdata}\secpol.cfg).replace("ClearTextPassword = 1", "ClearTextPassword = 0") | Out-File ${env:appdata}\secpol.cfg
    secedit /configure /db c:\windows\security\local.sdb /cfg ${env:appdata}\secpol.cfg /areas SECURITYPOLICY
    Remove-Item -force ${env:appdata}\secpol.cfg -confirm:$false
}
```

DisablePasswordReversibleEncryption es una función de PowerShell que deshabilita la reversión de encriptación para contraseñas en el equipo local. Esta función utiliza comandos de Windows como secedit y Get-Content para leer y modificar la configuración de seguridad. Esto garantiza que las contraseñas almacenadas localmente no se almacenen de forma reversible, lo que protege contra intentos de descifrado.

Get-Content es un cmdlet de PowerShell que lee el contenido de un archivo de texto y devuelve la información como un objeto de cadena. Esta función se usa para leer archivos de configuración como .cfg, .ini, .xml, etc. y luego usar la información leída para realizar alguna acción.

· AccountLockoutDuration, #1.2.1

```powershell
function AccountLockoutDuration
{
    #1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored)
    Write-Info "1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored)"
    Write-Before ("Before hardening: *******              ")
    Write-Output ( net accounts | Select-String -SimpleMatch 'lockout duration')

    Write-After ("After hardening: *******                 ")
    net accounts /lockoutduration:30
}
```

AccountLockoutDuration es una función de PowerShell que establece la duración de bloqueo de cuenta en el equipo local. Esta función usa el comando de Windows net accounts para leer y establecer la duración de bloqueo. Esto garantiza que, si un usuario intenta ingresar con una contraseña incorrecta, la cuenta se bloqueará durante un período de tiempo especificado, lo que impide que los atacantes intenten adivinar la contraseña.

Select-String es un cmdlet de PowerShell que busca cadenas de texto en archivos de texto. Esta función se usa para buscar una cadena de caracteres específica en un archivo de texto y devolver la línea donde se encuentra. Esta función también se puede usar para buscar en varios archivos a la vez.

· AccountLockoutThreshold, #1.2.2

```powershell
function AccountLockoutThreshold
{
    #1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored)
    Write-Info "1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored)"
    Write-Before ("Before hardening: *******             ")
    Write-Output ( net accounts | Select-String -SimpleMatch 'lockout threshold' )

    Write-After ("After hardening: *******                ")
    net accounts /lockoutthreshold:3

}
```

AccountLockoutThreshold es una función de PowerShell que hace lo mismo que la anterior. Write-Output es un cmdlet de PowerShell que imprime la salida de un cmdlet a la consola.

Esta función se usa para mostrar los resultados de un cmdlet en la pantalla para que el usuario los vea. Esta función también se puede usar para enviar la salida a otro cmdlet para realizar alguna otra acción.

· ResetAccountLockoutCounter, #1.2.3

```
function  ResetAccountLockoutCounter
{
    # 1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Scored)
    Write-Info "1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Scored)"
    Write-Before ("Before hardening: *******              ")
    Write-Output ( net accounts | Select-String -SimpleMatch 'Lockout observation window' )

    Write-After ("After hardening: *******                ")
    net accounts /lockoutwindow:30
}
```

ResetAccountLockoutCounter es una función de PowerShell que establece el tiempo de reinicio del contador de bloqueo de cuenta en el equipo local. Esta función usa el comando de Windows net accounts para leer y establecer el tiempo de reinicio. Esto garantiza que después de un período de tiempo específico, el contador de bloqueo de cuenta se reiniciará, lo que impide que los atacantes intenten adivinar la contraseña.

· NoOneTrustCallerACM, #2.2.1

```
function NoOneTrustCallerACM {
    #2.2.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller
    Write-Info "2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Scored)"
    SetUserRight "SeTrustedCredManAccessPrivilege" ($SID_NOONE)
}
```

Esta función establece la configuración de seguridad "Acceso a gestor de credenciales como llamante de confianza" a "Nadie". Esto significa que ningún usuario tendrá acceso a la función de gestor de credenciales en el equipo. Esto puede ser útil si se desea limitar el acceso a los datos del usuario en el equipo.

· #2.2.2 Not Applicable to Member Server

```
function NoOneTrustCallerACM {
    #2.2.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller
    Write-Info "2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Scored)"
    SetUserRight "SeTrustedCredManAccessPrivilege" ($SID_NOONE)
}
function DenyGuestBatchLogon {
    #2.2.22 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job
    Write-Info "2.2.22 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'"
    SetUserRight "SeDenyBatchLogonRight" (,$SID_GUESTS)
}

function DenyGuestServiceLogon {
    #2.2.23 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service
    Write-Info "2.2.23 (L1) Ensure 'Deny log on as a service' to include 'Guests'"
    SetUserRight "SeDenyServiceLogonRight" (,$SID_GUESTS)
}

function DenyGuestLocalLogon {
    #2.2.24 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally
    Write-Info "2.2.24 (L1) Ensure 'Deny log on locally' to include 'Guests'"
    SetUserRight "SeDenyInteractiveLogonRight" (,$SID_GUESTS)
}

function DenyRemoteDesktopServiceLogon {
    #2.2.26 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services
    Write-Info "2.2.26 (L1) Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account'"
    SetUserRight "SeDenyRemoteInteractiveLogonRight" ($SID_LOCAL_ACCOUNT, $GuestNewAccountName)
}

function NoOneTrustedForDelegation {
    #2.2.28 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable computer and user accounts to be trusted f
    Write-Info "2.2.28 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'"
    SetUserRight "SeDelegateSessionUserImpersonatePrivilege" (,$SID_NOONE)
}

function ForceShutdownFromRemoteSystem {
    #2.2.29 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system
    Write-Info "2.2.29 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'"
    SetUserRight "SeRemoteShutdownPrivilege" (,$SID_ADMINISTRATORS)
}
```

Estas funciones definen los derechos de usuario para evitar que los invitados inicien sesión en el sistema, se conecten a través de una sesión remota y realicen transferencias de delegación. Esto ayuda a garantizar que los usuarios no autorizados no tengan acceso al sistema. También se establece una configuración para asegurar que sólo los administradores puedan forzar el apagado del sistema desde un sistema remoto.

· AccessComputerFromNetwork, #2.2.3

```
function GenerateSecurityAudits {
    #2.2.30 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits
    Write-Info "2.2.30 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Scored)"
    SetUserRight "SeAuditPrivilege" ($SID_LOCAL_SERVICE,$SID_NETWORK_SERVICE)
}

function ImpersonateClientAfterAuthentication {
    #2.2.32 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication
    Write-Info "Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE, IIS_IUSRS'"
    SetUserRight "SeImpersonatePrivilege" ($SID_LOCAL_SERVICE,$SID_NETWORK_SERVICE,$SID_ADMINISTRATORS,$SID_SERVICE)
}

function IncreaseSchedulingPriority {
    #2.2.33 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority
    Write-Info "2.2.33 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'"
    SetUserRight "SeIncreaseBasePriorityPrivilege" ($SID_ADMINISTRATORS,$SID_WINDOW_MANAGER_GROUP)
}

function LoadUnloadDeviceDrivers {
    #2.2.34 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers
    Write-Info "2.2.34 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'"
    SetUserRight "SeLoadDriverPrivilege" (,$SID_ADMINISTRATORS)
}

function NoOneLockPagesInMemory {
    #2.2.35 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory
    Write-Info "2.2.35 (L1) Ensure 'Lock pages in memory' is set to 'No One'"
    SetUserRight "SeLockMemoryPrivilege" (,$SID_NOONE)
}

function ManageAuditingAndSecurity {
    #2.2.38 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log
    Write-Info "2.2.38 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators'"
    SetUserRight "SeSecurityPrivilege" (,$SID_ADMINISTRATORS)
}

function NoOneModifiesObjectLabel {
    #2.2.39 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label
    Write-Info "2.2.39 (L1) Ensure 'Modify an object label' is set to 'No One'"
    SetUserRight "SeRelabelPrivilege" (,$SID_NOONE)
}
```

Estas funciones realizan la tarea de configurar los permisos de usuario en Windows. Establecen los usuarios específicos y grupos que tendrán los permisos necesarios para realizar tareas específicas en el sistema. Estas configuraciones se usan como parte de una auditoría para garantizar la seguridad de la red.

· NoOneActAsPartOfOperatingSystem, #2.2.4

```
function NoOneActAsPartOfOperatingSystem {
    #2.2.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system
    Write-Info "2.2.4 (L1) Ensure 'Act as part of the operating system' is set to 'No One' (Scored)"
    SetUserRight "SeTcbPrivilege" ($SID_NOONE)
}
```

Esta función establece el derecho de usuario "Act as part of the operating system" para "Nadie". Esta configuración se usa para garantizar que ningún usuario tenga permisos para actuar como parte del sistema operativo. Esto se usa como parte de una auditoría de seguridad para garantizar que la red esté protegida.

· ChangeSystemTime, #2.2.11

```
function ChangeSystemTime {
    #2.2.11 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time
    Write-Info "2.2.11 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'"
    SetUserRight "SeSystemtimePrivilege" ($SID_ADMINISTRATORS,$SID_LOCAL_SERVICE)
}
```

ChangeSystemTime es una función de scripting de Windows PowerShell que se utiliza para configurar los derechos de usuario para permitir que los usuarios con privilegios de administrador y el servicio local cambien la hora y la fecha del sistema. Esta configuración se encuentra en 'Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time'.

· ChangeTimeZone, #2.2.12

· CreatePagefile, #2.2.13

· NoOneCreateTokenObject, #2.2.14

· CreateGlobalObjects, #2.2.15

· NoOneCreatesSharedObjects,#2.2.16

· #2.2.17 Not Applicable to Member Server

· CreateSymbolicLinks, #2.2.18

· DebugPrograms, #2.2.19

```powershell
function ChangeTimeZone {
    #2.2.12 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the time zone
    Write-Info "2.2.12 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE'"
    SetUserRight "SeTimeZonePrivilege" ($SID_LOCAL_SERVICE,$SID_ADMINISTRATORS)
}

function CreatePagefile {
    #2.2.13 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile
    Write-Info "2.2.13 (L1) Ensure 'Create a pagefile' is set to 'Administrators'"
    SetUserRight "SeCreatePagefilePrivilege" (,$SID_ADMINISTRATORS)
}

function NoOneCreateTokenObject {
    #2.2.14 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a token object
    Write-Info "2.2.14 (L1) Ensure 'Create a token object' is set to 'No One'"
    SetUserRight "SeCreateTokenPrivilege" (,$SID_NOONE)
}

function CreateGlobalObjects {
    #2.2.15 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create global objects
    Write-Info "2.2.15 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'"
    SetUserRight "SeCreateGlobalPrivilege" ($SID_ADMINISTRATORS,$SID_LOCAL_SERVICE, $SID_NETWORK_SERVICE,$SID_SERVICE)
}

function NoOneCreatesSharedObjects {
    #2.2.16 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create permanent shared objects
    Write-Info "2.2.16 (L1) Ensure 'Create permanent shared objects' is set to 'No One'"
    SetUserRight "SeCreatePermanentPrivilege" (,$SID_NOONE)
}

function CreateSymbolicLinks {
    #2.2.18 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create symbolic links
    Write-Info "2.2.18 (L1) Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines'"
    SetUserRight "SeCreateSymbolicLinkPrivilege" ($SID_ADMINISTRATORS,$SID_VIRTUAL_MACHINE)
}

function DebugPrograms {
    #2.2.19 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs
    Write-Info "2.2.19 (L1) Ensure 'Debug programs' is set to 'Administrators'"
    SetUserRight "SeDebugPrivilege" (,$SID_ADMINISTRATORS)
}
```

Estas funciones de PowerShell tienen como objetivo configurar los derechos de usuario de Windows. Por ejemplo, ChangeTimeZone establece el derecho de usuario 'Cambiar zona horaria' para que solo administradores y el servicio local tengan acceso. CreatePagefile establece el derecho de usuario 'Crear un archivo de página' para que solo los administradores tengan acceso. NoOneCreateTokenObject establece el derecho de usuario 'Crear un objeto de token' para que nadie tenga acceso. CreateGlobalObjects establece el derecho de usuario 'Crear objetos globales' para que los administradores, el servicio local, el servicio de red y el servicio tengan acceso. NoOneCreatesSharedObjects establece el derecho de usuario 'Crear objetos compartidos permanentes' para que nadie tenga acceso. CreateSymbolicLinks establece el derecho de usuario 'Crear enlaces simbólicos' para que los administradores y la máquina virtual NT tengan acceso. DebugPrograms establece el derecho de usuario 'Depurar programas' para que solo los administradores tengan acceso.

- **#2.2.20 Not Applicable to Member Server**
- **DenyNetworkAccess, #2.2.21**
- **DenyGuestBatchLogon, #2.2.22**
- **DenyGuestServiceLogon, #2.2.23**

- **DenyGuestLocalLogon, #2.2.24**
- **2.2.25 Not Applicable to Member Server**
- **DenyRemoteDesktopServiceLogon, #2.2.26**
- **2.2.27 Not Applicable to Member Server**
- **NoOneTrustedForDelegation, #2.2.28**
- **ForceShutdownFromRemoteSystem, #2.2.29**

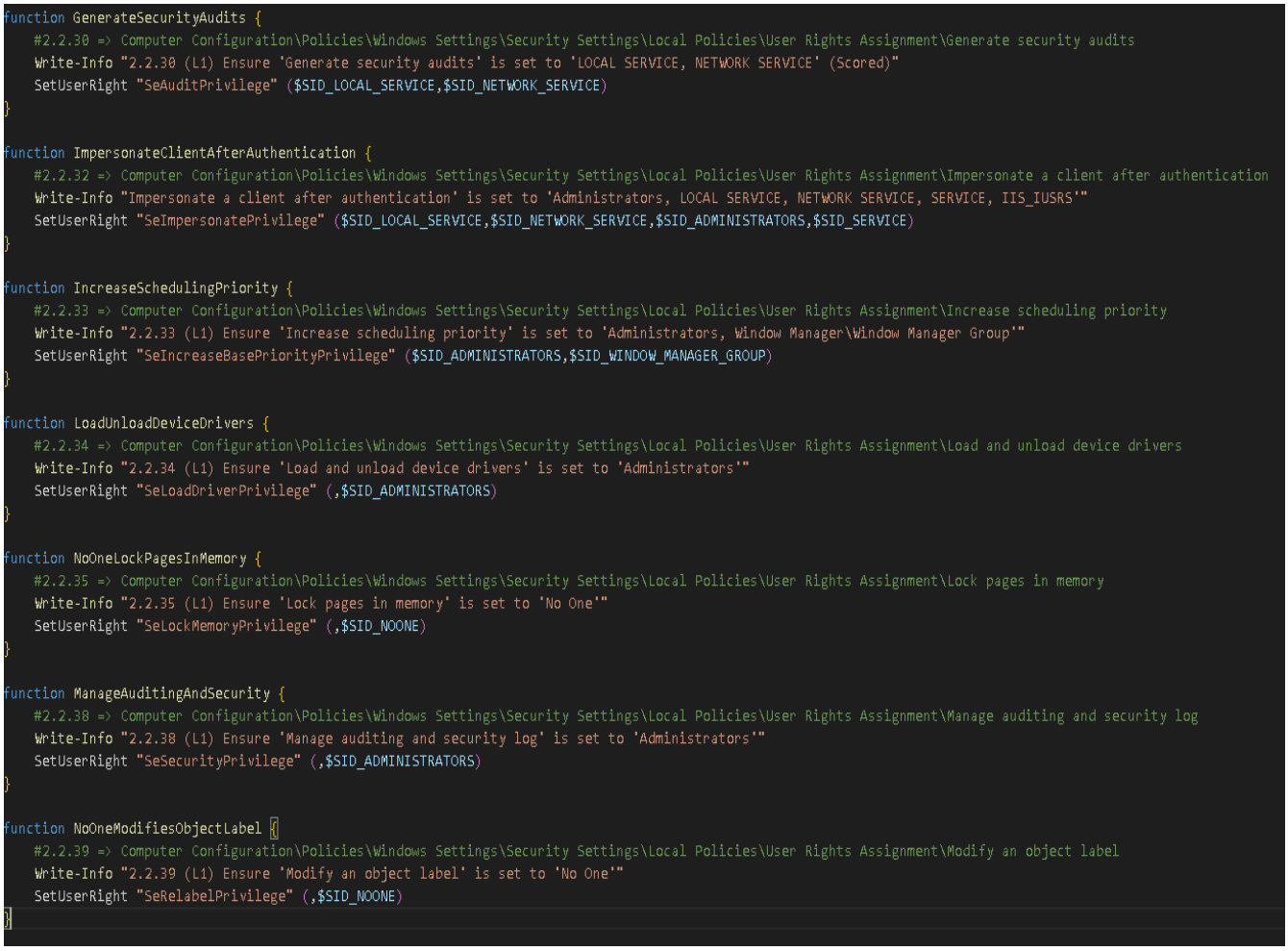
```
function DenyNetworkAccess {
    #2.2.21 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network
    Write-Info "2.2.21 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group'"
    SetUserRight "SeDenyNetworkLogonRight" ($SID_LOCAL_ACCOUNT, $($AdminNewAccountName),$($SID_GUESTS))
}

function DenyGuestBatchLogon {
    #2.2.22 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job
    Write-Info "2.2.22 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'"
    SetUserRight "SeDenyBatchLogonRight" (,$SID_GUESTS)
}

function DenyGuestServiceLogon {
    #2.2.23 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service
    Write-Info "2.2.23 (L1) Ensure 'Deny log on as a service' to include 'Guests'"
    SetUserRight "SeDenyServiceLogonRight" (,$SID_GUESTS)
}

function DenyGuestLocalLogon {
    #2.2.24 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally
    Write-Info "2.2.24 (L1) Ensure 'Deny log on locally' to include 'Guests'"
    SetUserRight "SeDenyInteractiveLogonRight" (,$SID_GUESTS)
}

function DenyRemoteDesktopServiceLogon {
    #2.2.26 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services
    Write-Info "2.2.26 (L1) Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account'"
    SetUserRight "SeDenyRemoteInteractiveLogonRight" ($SID_LOCAL_ACCOUNT, $GuestNewAccountName)
}

function NoOneTrustedForDelegation {
    #2.2.28 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable computer and user accounts to be trusted f
    Write-Info "2.2.28 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'"
    SetUserRight "SeDelegateSessionUserImpersonatePrivilege" (,$SID_NOONE)
}

function ForceShutdownFromRemoteSystem {
    #2.2.29 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system
    Write-Info "2.2.29 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'"
    SetUserRight "SeRemoteShutdownPrivilege" (,$SID_ADMINISTRATORS)
}
```

Estas funciones de PowerShell tienen como propósito configurar los derechos de usuario para garantizar la seguridad de un sistema operativo Windows. DenyNetworkAccess evita que los usuarios "Invitados", "Cuentas locales" y "Miembros del grupo Administradores" tengan acceso a la red. DenyGuestBatchLogon, DenyGuestServiceLogon y DenyGuestLocalLogon evitan que los usuarios "Invitados" sean capaces de iniciar sesión como trabajo por lotes, servicio o localmente, respectivamente. DenyRemoteDesktopServiceLogon impide que los usuarios "Invitados" y "Cuentas locales" se conecten a través de Remote Desktop Services. NoOneTrustedForDelegation impide que se delegue ninguna cuenta o computadora y ForceShutdownFromRemoteSystem impide

que cualquier usuario que no sea miembro del grupo Administradores pueda apagar el sistema desde un equipo remoto.

SetUserRight es una función de PowerShell que se utiliza para configurar los derechos de usuario de un sistema operativo Windows. Esta función se utiliza para añadir o quitar usuarios y grupos a determinados derechos de usuario. Por ejemplo, SetUserRight puede ser utilizado para establecer el derecho de un usuario para iniciar sesión en un equipo determinado o para ejecutar un servicio particular.

- **GENERATESECURITYAUDITS, #2.2.30**
- **2.2.31 NOT APPLICABLE TO MEMBER SERVER**
- **IMPERSONATECLIENTAFTERAUTHENTICATION, #2.2.32**
- **INCREASESCHEDULINGPRIORITY, #2.2.33**
- **LOADUNLOADDEVICEDRIVERS, #2.2.34**
- **NOONELOCKPAGESINMEMORY, #2.2.35**
- **2.2.36 NOT APPLICABLE TO MEMBER SERVER**
- **2.2.37 NOT APPLICABLE TO MEMBER SERVER**
- **MANAGEAUDITINGANDSECURITY, #2.2.38**
- **NOONEMODIFIESOBJECTLABEL, #2.2.39**



```powershell
function GenerateSecurityAudits {
    #2.2.30 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits
    Write-Info "2.2.30 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Scored)"
    SetUserRight "SeAuditPrivilege" ($SID_LOCAL_SERVICE,$SID_NETWORK_SERVICE)
}

function ImpersonateClientAfterAuthentication {
    #2.2.32 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication
    Write-Info "Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE, IIS_IUSRS'"
    SetUserRight "SeImpersonatePrivilege" ($SID_LOCAL_SERVICE,$SID_NETWORK_SERVICE,$SID_ADMINISTRATORS,$SID_SERVICE)
}

function IncreaseSchedulingPriority {
    #2.2.33 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority
    Write-Info "2.2.33 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'"
    SetUserRight "SeIncreaseBasePriorityPrivilege" ($SID_ADMINISTRATORS,$SID_WINDOW_MANAGER_GROUP)
}

function LoadUnloadDeviceDrivers {
    #2.2.34 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers
    Write-Info "2.2.34 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'"
    SetUserRight "SeLoadDriverPrivilege" (,$SID_ADMINISTRATORS)
}

function NoOneLockPagesInMemory {
    #2.2.35 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory
    Write-Info "2.2.35 (L1) Ensure 'Lock pages in memory' is set to 'No One'"
    SetUserRight "SeLockMemoryPrivilege" (,$SID_NOONE)
}

function ManageAuditingAndSecurity {
    #2.2.38 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log
    Write-Info "2.2.38 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators'"
    SetUserRight "SeSecurityPrivilege" (,$SID_ADMINISTRATORS)
}

function NoOneModifiesObjectLabel {
    #2.2.39 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label
    Write-Info "2.2.39 (L1) Ensure 'Modify an object label' is set to 'No One'"
    SetUserRight "SeRelabelPrivilege" (,$SID_NOONE)
}
```

Estas funciones de PowerShell son parte de un conjunto de directivas de seguridad destinadas a mejorar la seguridad de un sistema Windows. Estas funciones específicas se utilizan para establecer los derechos de usuario necesarios para asegurar que los recursos de sistema sean seguros y se protejan contra el uso indebido.

- GenerateSecurityAudits establece el derecho de usuario "SeAuditPrivilege" para "LOCAL SERVICE" y "NETWORK SERVICE", lo que permite que los servicios de seguridad generen auditorías de seguridad.

- ImpersonateClientAfterAuthentication establece el derecho de usuario "SeImpersonatePrivilege" para "Administradores", "LOCAL SERVICE", "NETWORK SERVICE" y "SERVICE", lo que permite a los usuarios o servicios "impersonar" a un cliente después de la autenticación.

- IncreaseSchedulingPriority establece el derecho de usuario "SeIncreaseBasePriorityPrivilege" para "Administradores" y "Window Manager\Window Manager Group", lo que permite a los usuarios o servicios aumentar la prioridad de la programación.

- LoadUnloadDeviceDrivers establece el derecho de usuario "SeLoadDriverPrivilege" para "Administradores", lo que permite a los usuarios o servicios cargar y descargar controladores de dispositivos.

- NoOneLockPagesInMemory establece el derecho de usuario "SeLockMemoryPrivilege" para "No One", lo que impide que los usuarios o servicios bloquen páginas en la memoria. - ManageAuditingAndSecurity establece el derecho de usuario "SeSecurityPrivilege" para "Administradores", lo que permite a los usuarios o servicios administrar la auditoría y el registro de seguridad.

- NoOneModifiesObjectLabel establece el derecho de usuario "SeRelabelPrivilege" para "No One", lo que impide que los usuarios o servicios modifiquen la etiqueta de un objeto.

· FirmwareEnvValues, #2.2.40

· VolumeMaintenance, #2.2.41

· ProfileSingleProcess, #2.2.42

· ProfileSystemPerformance, #2.2.43

· ReplaceProcessLevelToken, #2.2.44

· RestoreFilesDirectories, #2.2.45

· SystemShutDown, #2.2.46

· 2.2.47 Not Applicable to Member Server

· TakeOwnershipFiles, #2.2.48

```powershell
function FirmwareEnvValues {
    #2.2.40 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values
    Write-Info "2.2.40 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators'"
    SetUserRight "SeSystemEnvironmentPrivilege" (,$SID_ADMINISTRATORS)
}

function VolumeMaintenance {
    #2.2.41 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Perform volume maintenance tasks
    Write-Info "2.2.41 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators'"
    SetUserRight "SeManageVolumePrivilege" (,$SID_ADMINISTRATORS)

}

function ProfileSingleProcess {
    #2.2.42 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process
    Write-Info "2.2.42 (L1) Ensure 'Profile single process' is set to 'Administrators'"
    SetUserRight "SeProfileSingleProcessPrivilege" (,$SID_ADMINISTRATORS)
}

function ProfileSystemPerformance {
    #2.2.43 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance
    Write-Info "2.2.43 (L1) Ensure 'Profile system performance' is set to 'Administrators,NT SERVICE\WdiServiceHost'"
    SetUserRight "SeSystemProfilePrivilege" ($SID_ADMINISTRATORS,$SID_WDI_SYSTEM_SERVICE)
}

function ReplaceProcessLevelToken {
    #2.2.44 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token
    Write-Info "2.2.44 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'"
    SetUserRight "SeAssignPrimaryTokenPrivilege" ($SID_LOCAL_SERVICE, $SID_NETWORK_SERVICE)
}

function RestoreFilesDirectories {
    #2.2.45 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories
    Write-Info "2.2.45 (L1) Ensure 'Restore files and directories' is set to 'Administrators'"
    SetUserRight "SeRestorePrivilege" (,$SID_ADMINISTRATORS)
}

function SystemShutDown {
    #2.2.46 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system
    Write-Info "2.2.46 (L1) Ensure 'Shut down the system' is set to 'Administrators'"
    SetUserRight "SeShutdownPrivilege" (,$SID_ADMINISTRATORS)
}

function TakeOwnershipFiles {
    #2.2.48 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects
    Write-Info "2.2.48 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators'"
    SetUserRight "SeTakeOwnershipPrivilege" (,$SID_ADMINISTRATORS)
}
```

Estas funciones se usan para establecer los derechos de usuario en un sistema Windows. La función FirmwareEnvValues establece el derecho "Modificar valores del entorno de firmware" para los usuarios con el identificador de seguridad (SID) de Administradores. La función VolumeMaintenance establece el derecho "Realizar tareas de mantenimiento de volumen" para los usuarios con el SID de Administradores. La función ProfileSingleProcess establece el derecho "Perfil de un solo proceso" para los usuarios con el SID de Administradores. La función ProfileSystemPerformance establece el derecho "Perfil de rendimiento del sistema" para los usuarios con el SID de Administradores y el SID de WdiServiceHost. La función ReplaceProcessLevelToken establece el derecho "Reemplazar un token de nivel de proceso" para los usuarios con el SID de Servicio local y el SID de Servicio de red. La función RestoreFilesDirectories establece el derecho "Restaurar archivos y directorios" para los usuarios con el SID de Administradores. La función SystemShutDown establece el derecho "Apagar el sistema" para los usuarios con el SID de Administradores. Finalmente, la función TakeOwnershipFiles establece el derecho "Tomar posesión de archivos u otros objetos" para los usuarios con el SID de Administradores.

· DisableAdministratorAccount, #2.3.1.1

· DISABLEMICROSOFTACCOUNTS, #2.3.1.2

· DISABLEGUESTACCOUNT, #2.3.1.3

· LIMITBLANKPASSWORDCONSOLE, #2.3.1.4

```
function DisableAdministratorAccount {
    #2.3.1.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status
    Write-Info "2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'"
    SetSecurityPolicy "EnableAdminAccount" ,"0"
}

function DisableMicrosoftAccounts {
    #2.3.1.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts
    Write-Info "2.3.1.2 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoConnectedUser" ,"4,3"
}

function DisableGuestAccount {
    #2.3.1.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status
    Write-Info "2.3.1.3 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'"
    SetSecurityPolicy "EnableGuestAccount" ,"0"
}

function LimitBlankPasswordConsole {
    #2.3.1.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Limit local account use of blank passwords t
    Write-Info "2.3.1.4 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse" ,"4,1"
}
```

Estas funciones son parte de un programa de PowerShell que se utiliza para configurar la seguridad en Windows.

La primera función, DisableAdministratorAccount, establece la configuración de seguridad para deshabilitar la cuenta de administrador. Esto se hace modificando la directiva de seguridad "Cuentas: Estado de la cuenta de administrador" para establecerla en "Deshabilitado".

La segunda función, DisableMicrosoftAccounts, establece la configuración de seguridad para bloquear las cuentas de Microsoft. Esto se hace modificando la directiva de seguridad "Cuentas: Bloquear cuentas de Microsoft" para establecerla en "Los usuarios no pueden agregar o iniciar sesión con cuentas de Microsoft".

La tercera función, DisableGuestAccount, establece la configuración de seguridad para deshabilitar la cuenta de invitado. Esto se hace modificando la directiva de seguridad "Cuentas: Estado de la cuenta de invitado" para establecerla en "Deshabilitado".

La cuarta función, LimitBlankPasswordConsole, establece la configuración de seguridad para limitar el uso de contraseñas en blanco para iniciar sesión en la consola local. Esto se hace modificando la directiva de seguridad "Cuentas: Limite el uso de contraseñas en blanco para iniciar sesión en la consola local" para establecerla en "Habilitado".

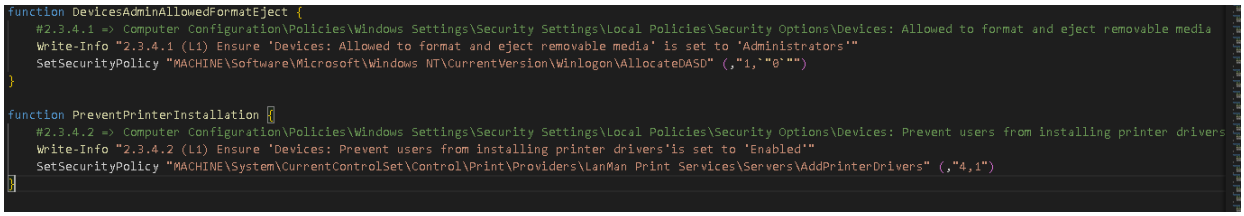
· AUDITFORCESUBCATEGORYPOLICY, #2.3.2.1

· AUDITFORCESHUTDOWN, #2.3.2.2

```
function AuditForceSubCategoryPolicy {
    #2.3.2.1 =>Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows
    Write-Info "2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings to override audit policy category settings' is set to 'Enabled' "
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy" ,"4,1"
}

function AuditForceShutdown {
    #2.3.2.2 Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log secu
    Write-Info "2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail" ,"4,0"
}
```

Estas dos funciones se utilizan para configurar la auditoría de Windows. La primera función, AuditForceSubCategoryPolicy, establece la política de auditoría para que las subcategorías de la política de auditoría anulen las categorías de la política de auditoría. La segunda función, AuditForceShutdown, deshabilita la opción de apagado inmediato del sistema si no se pueden registrar los informes de auditoría. Estas funciones se utilizan para asegurar que la auditoría se configure y se configure correctamente.

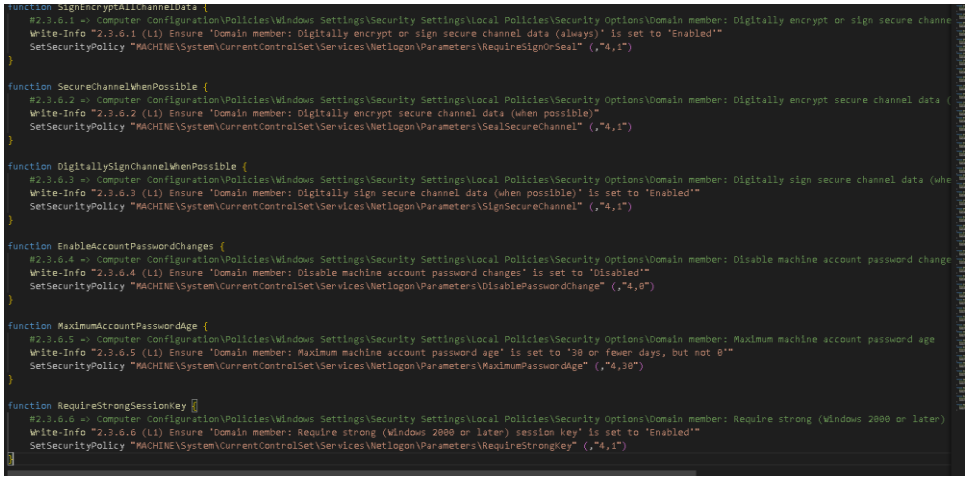
- **DevicesAdminAllowedFormatEject, #2.3.4.1**
- **PreventPrinterInstallation, #2.3.4.2**



```
function DevicesAdminAllowedFormatEject {
    #2.3.4.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media
    Write-Info "2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD" (,"1,`"0`"")
}

function PreventPrinterInstallation {
    #2.3.4.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers
    Write-Info "2.3.4.2 (L1) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers" (,"4,1")
}
```

Estas dos funciones son usadas para configurar los ajustes de seguridad de un equipo. La primera función, DevicesAdminAllowedFormatEject, configura la política de seguridad para permitir a los administradores formatear y expulsar medios extraíbles. La segunda función, PreventPrinterInstallation, configura la política de seguridad para evitar que los usuarios instalen controladores de impresora.

- **SignEncryptAllChannelData, #2.3.6.1**
- **SecureChannelWhenPossible, #2.3.6.2**
- **DigitallySignChannelWhenPossible, #2.3.6.3**
- **EnableAccountPasswordChanges, #2.3.6.4**
- **MaximumAccountPasswordAge, #2.3.6.5**
- **RequireStrongSessionKey, #2.3.6.6**



```
function SignEncryptAllChannelData {
    #2.3.6.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channe
    Write-Info "2.3.6.1 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal" (,"4,1")
}

function SecureChannelWhenPossible {
    #2.3.6.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (
    Write-Info "2.3.6.2 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel" (,"4,1")
}

function DigitallySignChannelWhenPossible {
    #2.3.6.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally sign secure channel data (whe
    Write-Info "2.3.6.3 (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel" (,"4,1")
}

function EnableAccountPasswordChanges {
    #2.3.6.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password change
    Write-Info "2.3.6.4 (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange" (,"4,0")
}

function MaximumAccountPasswordAge {
    #2.3.6.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age
    Write-Info "2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge" (,"4,30")
}

function RequireStrongSessionKey {
    #2.3.6.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later)
    Write-Info "2.3.6.6 (L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey" (,"4,1")
}
```

Estas funciones están diseñadas para ayudar a los usuarios a configurar la seguridad de los canales de seguridad y la cuenta de la máquina en un dominio. La función SignEncryptAllChannelData configura la Política de Seguridad de Windows para que los

canales de seguridad sean cifrados o firmados digitalmente siempre. La función SecureChannelWhenPossible configura la Política de Seguridad de Windows para que los canales de seguridad se cifren cuando sea posible. La función DigitallySignChannelWhenPossible configura la Política de Seguridad de Windows para que los canales de seguridad se firmen digitalmente cuando sea posible. La función EnableAccountPasswordChanges configura la Política de Seguridad de Windows para deshabilitar los cambios de contraseña de la cuenta de la máquina. La función MaximumAccountPasswordAge configura la Política de Seguridad de Windows para estable.

- **RequireCtlAltDel, #2.3.7.1**
- **DontDisplayLastSigned, #2.3.7.2**
- **MachineInactivityLimit, #2.3.7.3**
- **LogonLegalNotice, #2.3.7.4**
- **LogonLegalNoticeTitle, #2.3.7.5**
- **PreviousLogonCache, #2.3.7.6**
- **PromptUserPassExpiration, #2.3.7.7**
- **RequireDomainControllerAuth, #2.3.7.8**
- **SmartCardRemovalBehaviour, #2.3.7.9**

```
function RequireCtlAltDel {
    #2.3.7.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL
    Write-Info "2.3.7.1 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD" ,"4,0")
}

function DontDisplayLastSigned {
    #2.3.7.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Don't display last signed-in
    Write-Info "2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName" ,"4,0")
}

function MachineInactivityLimit {
    #2.3.7.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
    Write-Info "2.3.7.3 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' "
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\InactivityTimeoutSecs" ,"4,900")
}

function LogonLegalNotice {
    #2.3.7.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message text for users attempting
    Write-Info "2.3.7.4 (L1) Configure 'Interactive logon: Message text for users attempting to log on'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText" ("7",$LogonLegalNoticeMessage)
}

function LogonLegalNoticeTitle {
    #2.3.7.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message title for users attemptin
    Write-Info "2.3.7.5 (L1) Configure 'Interactive logon: Message title for users attempting to log on'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption" (,"1,`"$($LogonLegalNoticeMessageTitle)`"")
}
```

```
function PreviousLogonCache {
    #2.3.7.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache
    Write-Info "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)'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount" (,"1,`"4`"")
}

function PromptUserPassExpiration {
    #2.3.7.7 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password befo
    Write-Info "2.3.7.7 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning" (,"4,5")
}

function RequireDomainControllerAuth {
    #2.3.7.8 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Require Domain Controller Authentic
    Write-Info "2.3.7.8 (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon" (,"4,1")
}

function SmartCardRemovalBehaviour {
    #2.3.7.9 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior
    Write-Info "2.3.7.9 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption" (,"1,`"1`"")
}
```

Estas son funciones de configuración de seguridad para una computadora. La primera función, RequireCtlAltDel, establece la configuración de seguridad para evitar que los usuarios requieran la combinación de teclas CTRL + ALT + DEL para iniciar sesión. La segunda función, DontDisplayLastSigned, establece la configuración de seguridad para evitar que se muestre el último usuario que inició sesión. La tercera función, MachineInactivityLimit, establece la configuración de seguridad para establecer un límite de inactividad de 900 segundos o menos. La cuarta función, LogonLegalNotice, establece la configuración de seguridad para mostrar un aviso legal para los usuarios que intentan iniciar sesión. La quinta función, LogonLegalNoticeTitle, establece la configuración de seguridad para establecer un título para el aviso legal para los usuarios que intentan iniciar sesión. La sexta función, PreviousLogonCache, establece la configuración de seguridad para limitar el número de inicios de sesión anteriores a almacenar en caché a 4 o menos. La séptima función, PromptUserPassExpiration, establece la configuración de seguridad para pedir a los usuarios que cambien su contraseña antes de que expire entre 5 y 14 días. La octava función, RequireDomainControllerAuth, establece la configuración de seguridad para requerir autenticación de controlador de dominio para desbloquear la estación de trabajo. La novena función, SmartCardRemovalBehaviour, establece la configuración de seguridad para establecer el comportamiento de eliminación de tarjetas inteligentes en "Bloquear estación de trabajo" o un nivel superior.

- **NetworkClientSignCommunications, #2.3.8.1**

- **EnableSecuritySignature, #2.3.8.2**

- **DisableSmbUnencryptedPassword, #2.3.8.3**

```
function NetworkClientSignCommunications {
    #2.3.8.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communication
    Write-Info "2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature" (,"4,1")
}

function EnableSecuritySignature {
    #2.3.8.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communication
    Write-Info "2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' "
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature" (,"4,1")
}

function DisableSmbUnencryptedPassword {
    #2.3.8.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to
    Write-Info "2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword" (,"4,0")
}
```

NetworkClientSignCommunications es una función que configura una política de seguridad para permitir que el cliente de red firme digitalmente las comunicaciones. Esto asegura que la información transmitida entre el cliente y el servidor sea verificada y segura.

EnableSecuritySignature es una función que configura una política de seguridad para permitir que el servidor y el cliente acuerden digitalmente las comunicaciones. Esto asegura que la información transmitida entre el servidor y el cliente sea verificada y segura.

DisableSmbUnencryptedPassword es una función que desactiva la opción para que el cliente envíe contraseñas sin cifrar a servidores SMB de terceros. Esto asegura que la información transmitida entre el cliente y el servidor SMB de terceros sea segura.

- **IdleTimeSuspendingSession, #2.3.9.1**

- **NetworkServerAlwaysDigitallySign, #2.3.9.2**
- **EnableSecuritySignature, #2.3.9.3**
- **LanManServerEnableForcedLogOff, #2.3.9.4**
- **LanManServerSmbServerNameHardeningLevel, #2.3.9.5**

```
function IdleTimeSuspendingSession {
    #2.3.9.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required
    Write-Info "2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect" ,"4,15"
}

function NetworkServerAlwaysDigitallySign {
    #2.3.9.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communication
    Write-Info "2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature" ,"4,1"
}

function LanManSrvEnableSecuritySignature{
    #2.3.9.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communication
    Write-Info "2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature" ,"4,1"
}

function LanManServerEnableForcedLogOff {
    #2.3.9.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logo
    Write-Info "2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff" ,"4,1"
}

function LanManServerSmbServerNameHardeningLevel {
    #2.3.9.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Server SPN target name valid
    Write-Info "2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\SmbServerNameHardeningLevel" ,"4,1"
}
```

Estas cinco funciones están relacionadas con la configuración de seguridad de un servidor de red. La primera función, IdleTimeSuspendingSession, configura la cantidad de tiempo que un usuario puede estar inactivo antes de que su sesión sea suspendida. La segunda función, NetworkServerAlwaysDigitallySign, configura si las comunicaciones siempre se deben firmar digitalmente en el servidor de red. La tercera función, LanManSrvEnableSecuritySignature, configura si la firma de seguridad se habilita para las comunicaciones si el cliente lo acepta. La cuarta función, LanManServerEnableForcedLogOff, configura si los clientes se desconectarán cuando expire el horario de inicio de sesión. La quinta función, LanManServerSmbServerNameHardeningLevel, configura el nivel de validación de nombre de objetivo de SPN del servidor de red.

- **LSAAnonymousNameDisabled, #2.3.10.1**
- **RestrictAnonymousSAM, #2.3.10.2**
- **RestrictAnonymous, #2.3.10.3**
- **DisableDomainCreds, #2.3.10.4**
- **EveryoneIncludesAnonymous, #2.3.10.5**
- **2.3.10.6 Not Applicable to Member Server**
- **NullSessionPipes, #2.3.10.7**
- **AllowedExactPaths, #2.3.10.8**
- **AllowedPaths, #2.3.10.9**

- **RestrictNullSessAccess, #2.3.10.10**
- **RestrictRemoteSAM, #2.3.10.11**
- **NullSessionShares, #2.3.10.12**
- **LsaForceGuest, #2.3.10.13**

```
function LSAAnonymousNameDisabled {
    #2.3.10.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation
    Write-Info "2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'"
    SetSecurityPolicy "LSAAnonymousNameLookup" (,"0")
}

function RestrictAnonymousSAM {
    #2.3.10.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of
    Write-Info "2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM" (,"4,1")
}

function RestrictAnonymous {
    #2.3.10.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of
    Write-Info "2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous" (,"4,1")
}

function DisableDomainCreds {
    #2.3.10.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and
    Write-Info "2.3.10.4 (L2) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds" (,"4,1")
}

function EveryoneIncludesAnonymous {
    #2.3.10.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to and
    Write-Info "2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous" (,"4,0")
}

function NullSessionPipes {
    #2.3.10.7 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Named Pipes that can be accessed anon
    Write-Info "2.3.10.7 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes" ("7", " ")
}

function AllowedExactPaths {
    #2.3.10.8 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths
    Write-Info "2.3.10.8 (L1) Configure 'Network access: Remotely accessible registry paths'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Machine" (
        "7",
        "System\CurrentControlSet\Control\ProductOptions",
        "System\CurrentControlSet\Control\Server Applications",
        "Software\Microsoft\Windows NT\CurrentVersion")
}

function AllowedPaths {
    #2.3.10.9 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths a
    Write-Info "2.3.10.9 (L1) Configure 'Network access: Remotely accessible registry paths and sub-paths'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine" (
        "7",
```

```
function RestrictNullSessAccess {
    #2.3.10.10 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named P
    Write-Info "2.3.10.10 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess" (,"4,1")
}

function RestrictRemoteSAM {
    #2.3.10.11 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict clients allowed to make rem
    Write-Info "2.3.10.11 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\RestrictRemoteSAM" (,"1,O:BAG:BAD:(A;;RC;;;BA)")
}

function NullSessionShares {
    #2.3.10.12 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymou
    Write-Info "2.3.10.12 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares" (,"7,")
}

function LsaForceGuest {
    #2.3.10.13 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local
    Write-Info "2.3.10.13 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest" (,"4,0")
}
```

La función LSAAnonymousNameDisabled establece la política de acceso de red 'Allow anonymous SID/Name translation' a 'Disabled'. La función RestrictAnonymousSAM establece la política de acceso de red 'Do not allow anonymous enumeration of SAM accounts' a 'Enabled'. La función RestrictAnonymous establece la política de acceso de red 'Do not allow anonymous enumeration of SAM accounts and shares' a 'Enabled'. La función DisableDomainCreds establece la política de acceso de red 'Do not allow storage of passwords and credentials for network authentication' a 'Enabled'. La función EveryoneIncludesAnonymous establece la política de acceso de red 'Let Everyone permissions apply to anonymous users' a 'Disabled'. La función NullSessionPipes establece la política de acceso de red 'Named Pipes that can be accessed anonymously'. La función AllowedExactPaths establece la política de acceso de red 'Remotely accessible registry paths'. La función AllowedPaths establece la política de acceso de red 'Remotely accessible registry paths and sub-paths'. La función RestrictNullSessAccess establece la política de acceso de red 'Restrict anonymous access to Named Pipes and Shares' a 'Enabled'. La función RestrictRemoteSAM establece la política de acceso de red 'Restrict clients allowed to make remote calls to SAM' a 'Administrators: Remote Access: Allow'. La función NullSessionShares establece la política de acceso de red 'Shares that can be accessed anonymously' a 'None'. Por último, la función LsaForceGuest establece la política de acceso de red 'Sharing and security model for local accounts' a 'Classic - local users authenticate as themselves'.

- **LsaUseMachineId, #2.3.11.1**
- **AllowNullSessionFallback, #2.3.11.2**
- **AllowOnlineID, #2.3.11.3**
- **SupportedEncryptionTypes, #2.3.11.4**
- **NoLMHash, #2.3.11.5**
- **ForceLogoff, #2.3.11.6**
- **LmCompatibilityLevel, #2.3.11.7**
- **LDAPClientIntegrity, #2.3.11.8**
- **NTLMMinClientSec, #2.3.11.9**
- **NTLMMinServerSec, #2.3.11.10**

```
function LsaUseMachineId {
    #2.3.11.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer
    Write-Info "2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\UseMachineId" ,"4,1"
}

function AllowNullSessionFallback {
    #2.3.11.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fall
    Write-Info "2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\allownullsessionfallback " ,"4,0"
}

function AllowOnlineID {
    #2.3.11.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests
    Write-Info "2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\pku2u\AllowOnlineID " ,"4,0"
}

function SupportedEncryptionTypes {
    #2.3.11.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Configure encryption types allowed
    Write-Info "2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\SupportedEncryptionTypes" ,"4,2147483640"
}

function NoLMHash {
    #2.3.11.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value
    Write-Info "2.3.11.5 Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash" ,"4,1"
}

function ForceLogoff {
    #2.3.11.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Force logoff when logon hours expir
    Write-Info "2.3.11.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'"
    SetSecurityPolicy "ForceLogoffWhenHourExpire" ,"1"
}

function LmCompatibilityLevel {
    #2.3.11.7 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level
    Write-Info "2.3.11.7 Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel" ,"4,5"
}
```

```
function LDAPClientIntegrity {
    #2.3.11.8 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LDAP client signing requirements
    Write-Info "2.3.11.8 Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity" ,"4,1"
}

function NTLMMinClientSec {
    #2.3.11.9 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM S
    Write-Info "2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session sec
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec" ,"4,537395200"
}

function NTLMMinServerSec {
    #2.3.11.10 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM
    Write-Info "2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session se
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec" ,"4,537395200"
}
```

La función LsaUseMachineId establece la política de seguridad "Network security: Allow Local System to use computer identity for NTLM" para permitir que el sistema operativo local utilice la identidad del equipo para NTLM. La función AllowNullSessionFallback desactiva la opción "Network security: Allow LocalSystem NULL session fallback". Estas funciones tienen como objetivo mejorar la seguridad del sistema operativo, asegurando que los ajustes específicos estén configurados para evitar ataques de seguridad.

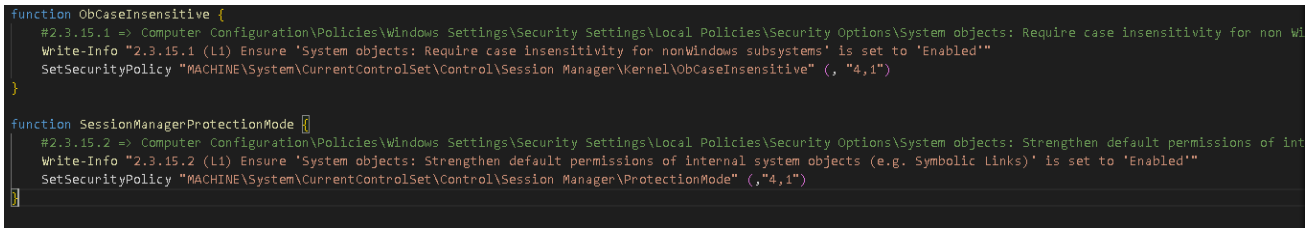
· SHUTDOWNWITHOUTLOGON, #2.3.13.1

```
function ShutdownWithoutLogon {
    #2.3.13.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having
    Write-Info "2.3.13.1 (L1) Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon" ,"4,0"
}
```

ShutdownWithoutLogon es una función de Powershell que modifica la configuración de seguridad para deshabilitar el apagado del sistema sin tener que iniciar sesión. Esto significa

que el usuario debe iniciar sesión en el sistema antes de que se permita apagar el sistema. Esto se configura a través de la directiva de grupo "Apagado: Permitir que el sistema se apague sin tener que iniciar sesión" que se encuentra en Configuración del equipo \ Políticas \ Configuración de Windows \ Políticas de seguridad \ Opciones de seguridad local. Esta función de Powershell modifica la directiva de grupo para establecer su valor en "Deshabilitado".

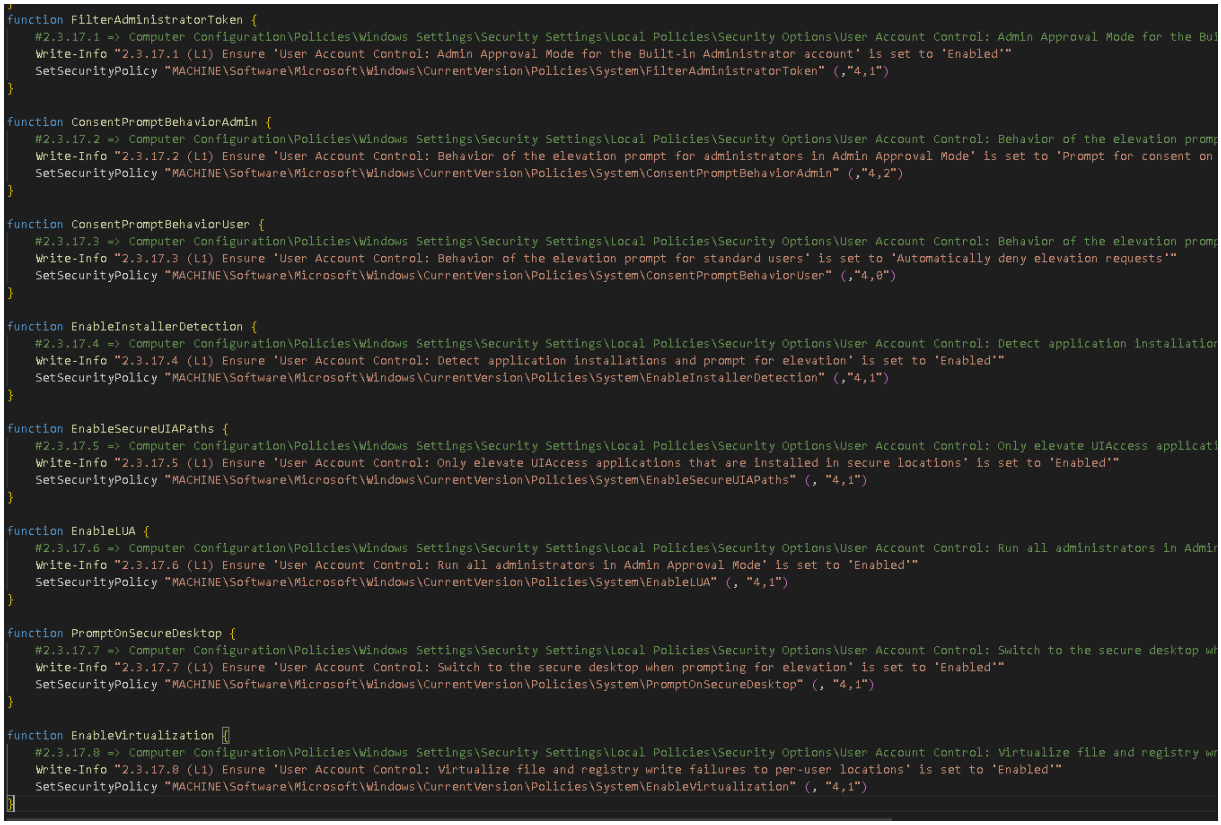
- **ObCaseInsensitive, #2.3.15.1**
- **SessionManagerProtectionMode, #2.3.15.2**



```
function ObCaseInsensitive {
    #2.3.15.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Require case insensitivity for non Wi
    Write-Info "2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for nonWindows subsystems' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive" (, "4,1")
}

function SessionManagerProtectionMode {
    #2.3.15.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Strengthen default permissions of int
    Write-Info "2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode" (,"4,1")
}
```

Estas dos funciones son parte de un script de PowerShell que se utiliza para configurar ajustes de seguridad en un equipo. La primera función, ObCaseInsensitive, establece el ajuste "System objects: Require case insensitivity for nonWindows subsystems" en "Habilitado". La segunda función, SessionManagerProtectionMode, establece el ajuste "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)" en "Habilitado". Estas dos funciones se utilizan para aumentar la seguridad del equipo configurando los ajustes de seguridad adecuados.

- **FilterAdministratorToken, #2.3.17.1**
- **ConsentPromptBehaviorAdmin, #2.3.17.2**
- **ConsentPromptBehaviorUser, #2.3.17.3**
- **EnableInstallerDetection, #2.3.17.4**
- **EnableSecureUIAPaths, #2.3.17.5**
- **EnableLUA, #2.3.17.6**
- **PromptOnSecureDesktop, #2.3.17.7**
- **EnableVirtualization, #2.3.17.8**

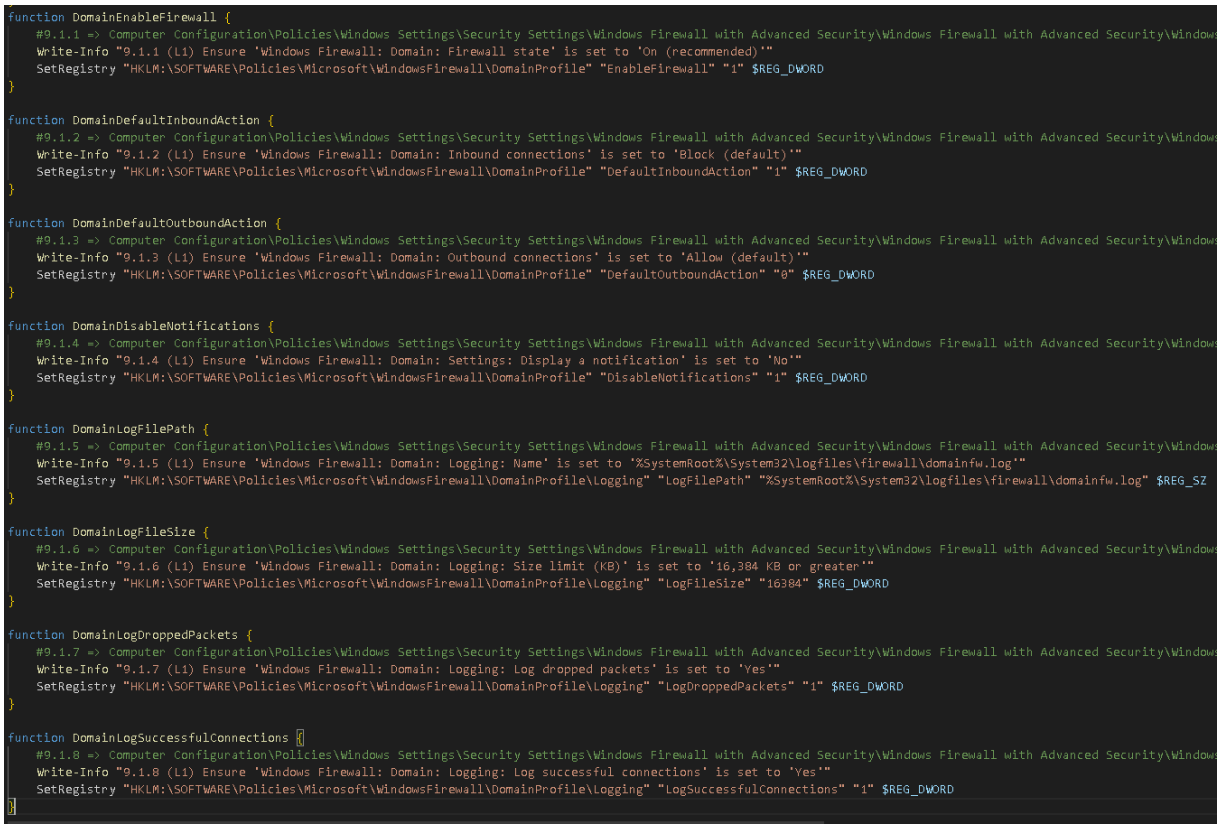


```
function FilterAdministratorToken {
    #2.3.17.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Bui
    Write-Info "2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorToken" (,"4,1")
}

function ConsentPromptBehaviorAdmin {
    #2.3.17.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation promp
    Write-Info "2.3.17.2 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin" (,"4,2")
}

function ConsentPromptBehaviorUser {
    #2.3.17.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation promp
    Write-Info "2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser" (,"4,0")
}

function EnableInstallerDetection {
    #2.3.17.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installatior
    Write-Info "2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableInstallerDetection" (,"4,1")
}

function EnableSecureUIAPaths {
    #2.3.17.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applicati
    Write-Info "2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableSecureUIAPaths" (, "4,1")
}

function EnableLUA {
    #2.3.17.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admir
    Write-Info "2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA" (, "4,1")
}

function PromptOnSecureDesktop {
    #2.3.17.7 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop wh
    Write-Info "2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop" (, "4,1")
}

function EnableVirtualization {
    #2.3.17.8 => Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry wr
    Write-Info "2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'"
    SetSecurityPolicy "MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableVirtualization" (, "4,1")
}
```

Estas 8 funciones son parte de un script de Powershell para asegurar la configuración de seguridad de la cuenta de administrador predeterminada en un sistema operativo Windows. Estas funciones configuran una serie de ajustes de seguridad relacionados con el control de cuentas de usuario (UAC). Estos ajustes incluyen habilitar el modo de aprobación de administrador para la cuenta de administrador incorporada, establecer el comportamiento del cuadro de diálogo de elevación para los administradores en modo de aprobación de administrador, establecer el comportamiento del cuadro de diálogo de elevación para los usuarios estándar, habilitar la detección de instalación de aplicaciones y solicitar elevación, habilitar la ejecución de todos los administradores en modo de aprobación de administrador, habilitar el cambio al escritorio seguro al solicitar elevación, habilitar la virtualización de fallas de escritura de archivos y registro en ubicaciones por usuario y habilitar la elevación de aplicaciones UIAccess instaladas en ubicaciones seguras. Estos ajustes de seguridad ayudan a proteger el sistema de amenazas externas.

- **DomainEnableFirewall, #9.1.1**
- **DomainDefaultInboundAction, #9.1.2**
- **DomainDefaultOutboundAction, #9.1.3**
- **DomainDisableNotifications", #9.1.4**
- **DomainLogFilePath, #9.1.5**
- **DomainLogFileSize, #9.1.6**
- **DomainLogDroppedPackets, #9.1.7**

- **DomainLogSuccessfulConnections, #9.1.8**



```
function DomainEnableFirewall {
    #9.1.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile" "EnableFirewall" "1" $REG_DWORD
}

function DomainDefaultInboundAction {
    #9.1.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile" "DefaultInboundAction" "1" $REG_DWORD
}

function DomainDefaultOutboundAction {
    #9.1.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile" "DefaultOutboundAction" "0" $REG_DWORD
}

function DomainDisableNotifications {
    #9.1.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile" "DisableNotifications" "1" $REG_DWORD
}

function DomainLogFilePath {
    #9.1.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging" "LogFilePath" "%SystemRoot%\System32\logfiles\firewall\domainfw.log" $REG_SZ
}

function DomainLogFileSize {
    #9.1.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging" "LogFileSize" "16384" $REG_DWORD
}

function DomainLogDroppedPackets {
    #9.1.7 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging" "LogDroppedPackets" "1" $REG_DWORD
}

function DomainLogSuccessfulConnections {
    #9.1.8 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging" "LogSuccessfulConnections" "1" $REG_DWORD
}
```

Configura la seguridad de Windows Firewall con Advanced Security en una computadora de dominio. La primera función (DomainEnableFirewall) asegura que el estado del firewall esté configurado en "Activado" (recomendado). La segunda función (DomainDefaultInboundAction) asegura que la conexión entrante esté configurada para bloquear (por defecto). La tercera función (DomainDefaultOutboundAction) asegura que la conexión saliente esté configurada para permitir (por defecto). La cuarta función (DomainDisableNotifications) asegura que las notificaciones estén deshabilitadas. La quinta función (DomainLogFilePath) asegura que la ubicación del archivo de registro esté configurada en "%SystemRoot%\System32\logfiles\firewall\domainfw.log". La sexta función (DomainLogFileSize) asegura que el tamaño del archivo de registro sea de 16,384 KB o mayor. La séptima función (DomainLogDroppedPackets) asegura que se registren los paquetes descartados. La octava función (DomainLogSuccessfulConnections) asegura que se registren las conexiones exitosas.

- **PrivateEnableFirewall, #9.2.1**
- **PrivateDefaultInboundAction, #9.2.2**
- **PrivateDefaultOutboundAction, #9.2.3**
- **PrivateDisableNotifications, #9.2.4**
- **PrivateLogFilePath, #9.2.5**
- **PrivateLogFileSize, #9.2.6**

- **PRIVATELOGDROPPEDPACKETS, #9.2.7**
- **PRIVATELOGSUCCESSFULCONNECTIONS, #9.2.8**

```
function PrivateEnableFirewall {
    #9.2.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile" "EnableFirewall" "1" $REG_DWORD
}

function PrivateDefaultInboundAction {
    #9.2.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile" "DefaultInboundAction" "1" $REG_DWORD
}

function PrivateDefaultOutboundAction {
    #9.2.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile" "DefaultOutboundAction" "0" $REG_DWORD
}

function PrivateDisableNotifications {
    #9.2.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile" "DisableNotifications" "1" $REG_DWORD
}

function PrivateLogFilePath {
    #9.2.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging" "LogFilePath" "%SystemRoot%\System32\logfiles\firewall\privatefw.log" $REG_SZ
}

function PrivateLogFileSize {
    #9.2.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging" "LogFileSize" "16384" $REG_DWORD
}

function PrivateLogDroppedPackets {
    #9.2.7 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging" "LogDroppedPackets" "1" $REG_DWORD
}

function PrivateLogSuccessfulConnections {
    #9.2.8 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging" "LogSuccessfulConnections" "1" $REG_DWORD
}
```

La primera función PrivateEnableFirewall se encarga de asegurarse de que el firewall esté activo. La segunda función, PrivateDefaultInboundAction, se encarga de establecer la acción predeterminada para las conexiones entrantes como bloquear (predeterminado). La tercera función, PrivateDefaultOutboundAction, se encarga de establecer la acción predeterminada para las conexiones salientes como permitir (predeterminado). La cuarta función, PrivateDisableNotifications, se encarga de asegurarse de que las notificaciones estén deshabilitadas. La quinta función, PrivateLogFilePath, se encarga de establecer la ubicación del archivo de registro de firewall. La sexta función, PrivateLogFileSize, se encarga de asegurarse de que el tamaño del archivo de registro sea de 16384 KB o mayor. La séptima función, PrivateLogDroppedPackets, se encarga de asegurarse de que los paquetes descartados se registren. La octava función, PrivateLogSuccessfulConnections, se encarga de asegurarse de que las conexiones exitosas se registren.

- **PUBLICENABLEFIREWALL, #9.3.1**
- **PUBLICDEFAULTINBOUNDACTION, #9.3.2**
- **PUBLICDEFAULTOUTBOUNDACTION, #9.3.3**
- **PUBLICDISABLENOTIFICATIONS, #9.3.4**
- **PUBLICALLOWLOCALPOLICYMERGE, #9.3.5**
- **PUBLICALLOWLOCALIPSECPOLICYMERGE , #9.3.6**
- **PUBLICLOGFILEPATH, #9.3.7**

- **PUBLICLOGFILESIZE, #9.3.8**
- **PUBLICLOGDROPPEDPACKETS, #9.3.9**
- **PUBLICLOGSUCCESSFULCONNECTIONS, #9.3.10**

```
function PublicEnableFirewall {
    #9.3.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile" "EnableFirewall" "1" $REG_DWORD
}

function PublicDefaultInboundAction {
    #9.3.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile" "DefaultInboundAction" "1" $REG_DWORD
}

function PublicDefaultOutboundAction {
    #9.3.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile" "DefaultOutboundAction" "0" $REG_DWORD
}

function PublicDisableNotifications {
    #9.3.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile" "DisableNotifications" "1" $REG_DWORD
}

function PublicAllowLocalPolicyMerge {
    #9.3.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile" "PublicAllowLocalPolicyMerge" "0" $REG_DWORD
}

function PublicAllowLocalIPsecPolicyMerge {
    #9.3.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile" "PublicAllowLocalIPsecPolicyMerge" "0" $REG_DWORD
}

function PublicLogFilePath {
    #9.3.7 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging" "LogFilePath" "%SystemRoot%\System32\logfiles\firewall\publicfw.log" $REG_SZ
}
```

```
function PublicLogFileSize {
    #9.3.8 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging" "LogFileSize" "16384" $REG_DWORD
}

function PublicLogDroppedPackets {
    #9.3.9 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging" "LogDroppedPackets" "1" $REG_DWORD
}

function PublicLogSuccessfulConnections {
    #9.3.10 => Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows
    Write-Info "9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging" "LogSuccessfulConnections" "1" $REG_DWORD
}
```

Estas funciones están relacionadas con la configuración del Firewall de Windows. La función PublicEnableFirewall establece la configuración para habilitar el Firewall para el perfil público. La función PublicDefaultInboundAction establece la conexión entrante predeterminada en bloqueo en el perfil público. La función PublicDefaultOutboundAction establece la conexión saliente predeterminada en permitir en el perfil público. La función PublicDisableNotifications establece la configuración para deshabilitar las notificaciones del Firewall para el perfil público. La función PublicAllowLocalPolicyMerge establece la configuración para deshabilitar la aplicación de reglas de Firewall locales para el perfil público. La función PublicAllowLocalIPsecPolicyMerge establece la configuración para deshabilitar la aplicación de reglas de seguridad de conexión locales para el perfil público. La función PublicLogFilePath establece el nombre del archivo de registro del Firewall para el perfil público. La función PublicLogFileSize establece el límite de tamaño de archivo de registro para el perfil público. La función PublicLogDroppedPackets establece la configuración para registrar paquetes descartados para el perfil público. La función

PublicLogSuccessfulConnections establece la configuración para registrar conexiones exitosas para el perfil público.

- **AUDITCREDENTIALVALIDATION, #17.1.1**
- **AUDITCOMPUTERACCOUNTMANAGEMENT, #17.2.1**
- **17.2.2 NOT APPLICABLE TO MEMBER SERVER**
- **17.2.3 NOT APPLICABLE TO MEMBER SERVER**
- **17.2.4 NOT APPLICABLE TO MEMBER SERVER**
- **AUDITSECURITYGROUPMANAGEMENT, #17.2.5**
- **AUDITUSERACCOUNTMANAGEMENT, #17.2.6**

```
function AuditComputerAccountManagement {
    #17.2.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Application
    Write-Info "17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"Application Group Management" /success:disable /failure:disable
}

function AuditSecurityGroupManagement {
    #17.2.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Security Gr
    Write-Info "17.2.5 (L1) Ensure 'Audit Security Group Management' is set to include 'Success'"
    Auditpol /set /subcategory:"Security Group Management" /success:enable /failure:disable
}

function AuditUserAccountManagement {
    #17.2.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit User Accoun
    Write-Info "17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
}
```

Estas son tres funciones relacionadas con la configuración de auditoría de cuentas de usuario. La primera función, AuditComputerAccountManagement, establece la configuración de Auditoría de Grupo de Aplicaciones para solo el éxito. La segunda función, AuditSecurityGroupManagement, establece la configuración de Auditoría de Grupo de Seguridad para incluir el éxito. La tercera función, AuditUserAccountManagement, establece la configuración de Auditoría de Cuenta de Usuario para el éxito y el fracaso. Estas funciones se utilizan para asegurar que los cambios realizados en las cuentas de usuario sean auditados apropiadamente.

- **AUDITPNPACTIVITY, #17.3.1**
- **AUDITPROCESSCREATION, #17.3.2**

```
function AuditPNPActivity {
    #17.3.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit PNP Activity
    Write-Info "17.3.1 (L1) Ensure 'Audit PNP Activity' is set to include 'Success'"
    Auditpol /set /subcategory:"Plug and Play Events" /success:enable /failure:disable
}

function AuditProcessCreation {
    #17.3.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Crea
    Write-Info "17.3.2 (L1) Ensure 'Audit Process Creation' is set to include 'Success'"
    Auditpol /set /subcategory:"Process Creation" /success:enable /failure:disable
}
```

La primera función, AuditPNPActivity, configura el registro de auditoría avanzada para auditar la actividad de Plug and Play. Esto significa que todas las veces que un dispositivo Plug and Play se conecta o desconecta del equipo, un registro de auditoría se generará. La segunda función, AuditProcessCreation, configura el registro de auditoría avanzada para auditar la creación de procesos. Esto significa que todas las veces que un nuevo proceso se

inicia en el equipo, un registro de auditoría se generará. En ambos casos, los registros de auditoría se configuran para capturar sólo los intentos de éxito, sin los intentos de fallo.

- **AUDITACCOUNTLOCKOUT, #17.5.1**
- **AUDITGROUPMEMBERSHIP, #17.5.2**
- **AUDITLOGOFF, #17.5.3**
- **AUDITLOGON, #17.5.4**
- **AUDITOTHERLOGONLOGOFFEVENTS, #17.5.5**
- **AUDITSPECIALLOGON, #17.5.6**

```
function AuditAccountLockout {
    #17.5.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout
    Write-Info "17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'"
    Auditpol /set /subcategory:"Account Lockout" /success:disable /failure:enable
}

function AuditGroupMembership  {
    #17.5.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Group Membership
    Write-Info "17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success'"
    Auditpol /set /subcategory:"Group Membership" /success:enable /failure:disable
}

function AuditLogoff {
    #17.5.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff
    Write-Info "17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success'"
    Auditpol /set /subcategory:"Logoff" /success:enable /failure:disable
}

function AuditLogon {
    #17.5.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon
    Write-Info "17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"Logon" /success:enable /failure:enable
}

function AuditOtherLogonLogoffEvents {
    #17.5.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logo
    Write-Info "17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"Other Logon/Logoff Events" /success:enable /failure:enable
}

function AuditSpecialLogon {
    #17.5.6 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon
    Write-Info "17.5.6 (L1) Ensure 'Audit Special Logon' is set to include 'Success'"
    Auditpol /set /subcategory:"Special Logon" /success:enable /failure:disable
}
```

Estas seis funciones son parte de un script de PowerShell para configurar la política de auditoría de Windows. Estas funciones ajustan los parámetros de configuración de la política de auditoría para diferentes opciones de inicio de sesión y cierre de sesión. Estos parámetros incluyen el bloqueo de cuentas, la membresía de grupo, la desconexión, el inicio de sesión, otros eventos de inicio y cierre de sesión y el inicio especial. Cada función ajusta estos parámetros para habilitar el éxito o el fracaso de los eventos específicos.

- **AUDITDETAILEDFILESHARE, #17.6.1**
- **AUDITFILESHARE, #17.6.2**
- **AUDITOTHEROBJECTACCESSEVENTS, #17.6.3**
- **AUDITREMOVABLESTORAGE, #17.6.4**

```
function AuditDetailedFileShare {
    #17.6.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Detailed File S
    Write-Info "17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure'"
    Auditpol /set /subcategory:"Detailed File Share" /success:disable /failure:enable
}

function AuditFileShare {
    #17.6.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit File Share
    Write-Info "17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"File Share" /success:enable /failure:enable
}

function AuditOtherObjectAccessEvents {
    #17.6.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Other Object Ac
    Write-Info "17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"Other Object Access Events" /success:enable /failure:enable
}

function AuditRemovableStorage {
    #17.6.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Removable Stora
    Write-Info "17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"Removable Storage" /success:enable /failure:enable
}
```

Estas cuatro funciones son utilizadas para ajustar el registro de auditoría de Windows en el equipo. La función AuditDetailedFileShare establece la configuración de auditoría para Detailed File Share para incluir fallas. La función AuditFileShare establece la configuración de auditoría para File Share para incluir tanto éxitos como fallas. La función AuditOtherObjectAccessEvents establece la configuración de auditoría para Other Object Access Events para incluir tanto éxitos como fallas. La función AuditRemovableStorage establece la configuración de auditoría para Removable Storage para incluir tanto éxitos como fallas.

- **AUDITPOLICYCHANGE, #17.7.1**
- **AUDITAUTHENTICATIONPOLICYCHANGE, #17.7.2**
- **AUDITAUTHORIZATIONPOLICYCHANGE, #17.7.3**
- **AUDITMPSSVCRULELEVELPOLICYCHANGE, #17.7.4**
- **AUDITOTHERPOLICYCHANGEEVENTS, #17.7.5**

```
}
function AuditPolicyChange {
    #17.7.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Ch
    Write-Info "17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success'"
    Auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:disable
}

function AuditAuthenticationPolicyChange {
    #17.7.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication
    Write-Info "17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success'"
    Auditpol /set /subcategory:"Authentication Policy Change" /success:enable /failure:disable
}

function AuditAuthorizationPolicyChange {
    #17.7.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authorization P
    Write-Info "17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success'"
    Auditpol /set /subcategory:"Authorization Policy Change" /success:enable /failure:disable
}

function AuditMPSSVCRuleLevelPolicyChange {
    #17.7.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit MPSSVC RuleLeve
    Write-Info "17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"MPSSVC Rule-Level Policy Change" /success:enable /failure:enable
}

function AuditOtherPolicyChangeEvents {
    #17.7.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Other Policy Ch
    Write-Info "17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure'"
    Auditpol /set /subcategory:"Other Policy Change Events" /success:disable /failure:enable
}
```

Estas 5 funciones son parte de una configuración de auditoría de seguridad para un sistema de Windows. Estas funciones específicas establecen los parámetros de auditoría para el cambio de políticas como el cambio de políticas de auditoría, el cambio de políticas de autenticación, el cambio de políticas de autorización, el cambio de políticas a nivel de regla para el servidor de administración de servicios y los demás eventos de cambio de políticas.

Estas funciones configuran la auditoría para que se registren los éxitos y los fracasos de cada uno de estos eventos de cambio de políticas.

- **AUDITSPECIALLOGON, #17.8.1**

```
function AuditSpecialLogon {
    #17.8.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privi
    Write-Info "17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"Sensitive Privilege Use" /success:enable /failure:enable
}
```

Esta es una función en PowerShell que configura el conteo de auditoría para el uso de privilegios sensibles para registrar tanto éxitos como fracasos. Esto significa que cuando un usuario intenta usar un privilegio sensible, se guardará un registro de si el intento fue exitoso o no. Esto ayuda a detectar y prevenir el abuso de privilegios sensibles.

- **AUDITIPSECDRIVER, #17.9.1**
- **AUDITOTHERSYSTEMEVENTS, #17.9.2**
- **AUDITSECURITYSTATECHANGE, #17.9.3**
- **AUDITSECURITYSYSTEMEXTENSION, #17.9.4**
- **AUDITSYSTEMINTEGRITY, #17.9.5**

```
function AuditIPsecDriver  {
    #17.9.1 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver
    Write-Info "17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"IPsec Driver" /success:enable /failure:enable
}

function AuditOtherSystemEvents  {
    #17.9.2 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Other System Events
    Write-Info "17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"Other System Events" /success:enable /failure:enable
}

function AuditSecurityStateChange {
    #17.9.3 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security State Chang
    Write-Info "17.9.3 (L1) Ensure 'Audit Security State Change' is set to include 'Success'"
    Auditpol /set /subcategory:"Security State Change" /success:enable /failure:disable
}

function AuditSecuritySystemExtension {
    #17.9.4 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Exte
    Write-Info "17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success'"
    Auditpol /set /subcategory:"Security System Extension" /success:enable /failure:disable
}

function AuditSystemIntegrity {
    #17.9.5 => Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit System Integrity
    Write-Info "17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure'"
    Auditpol /set /subcategory:"System Integrity" /success:enable /failure:enable
}
```

Estas cinco funciones son usadas para configurar la política de auditoría avanzada del sistema de Windows. Estas funciones especifican los parámetros de auditoría para IPsec Driver, Other System Events, Security State Change, Security System Extension y System Integrity. Estas funciones habilitarán el registro de auditoría para éxitos y fallas.

- **PREVENTENABLINGLOCKSCREENCAMERA, #18.1.1.1**
- **PREVENTENABLINGLOCKSCREENSLIDESHOW, #18.1.1.2**

```
function PreventEnablingLockScreenCamera {
    #18.1.1.1 => Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen camera
    Write-Info "18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Personalization" "NoLockScreenCamera" "1" $REG_DWORD
}

function PreventEnablingLockScreenSlideShow {
    #18.1.1.2 => Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen slide show
    Write-Info "18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Personalization" "NoLockScreenSlideshow" "1" $REG_DWORD
}
```

Esta función está diseñada para asegurar que el usuario no pueda habilitar la cámara de bloqueo de la pantalla ni el slideshow del bloqueo de la pantalla en un sistema operativo Windows. Establece los valores correspondientes en el Registro de Windows para deshabilitar estas funciones.

· DisallowUsersToEnableOnlineSpeechRecognitionServices, #18.1.2.1

```
function DisallowUsersToEnableOnlineSpeechRecognitionServices {
    #18.1.2.1 => Computer Configuration\Policies\Administrative Templates\Control Panel\Regional and Language Options\Allow users to enable online speech recognition se
    Write-Info "18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\InputPersonalization" "AllowInputPersonalization" "0" $REG_DWORD
}
```

Esta función es utilizada para deshabilitar los servicios de reconocimiento de voz en línea en una computadora. Esto es logrado estableciendo la clave de registro "AllowInputPersonalization" en "HKLM:\SOFTWARE\Policies\Microsoft\InputPersonalization" para el valor "0" de tipo DWORD. Esto evita que los usuarios habiliten los servicios de reconocimiento de voz en línea en la computadora.

· DisallowOnlineTips, #18.1.3

```
function DisallowOnlineTips {
    #18.1.3 => Computer Configuration\Policies\Administrative Templates\Control Panel\Allow Online Tips
    Write-Info "18.1.3 (L2) Ensure 'Allow Online Tips' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" "AllowOnlineTips" "0" $REG_DWORD
}
```

Esta función establece un valor de registro para deshabilitar los consejos en línea en Windows. Esta configuración se encuentra en el Explorador de Windows y se puede encontrar en la configuración de grupo de la sección "Control Panel" bajo "Allow Online Tips". Esto deshabilitará la pantalla emergente que aparece cuando se abre el Explorador de Windows, que ofrece consejos útiles sobre cómo usar Windows.

· LocalAccountTokenFilterPolicy, #18.3.1

· ConfigureSMBv1ClientDriver, #18.3.2

· ConfigureSMBv1server, #18.3.3

· DisableExceptionChainValidation, #18.3.4

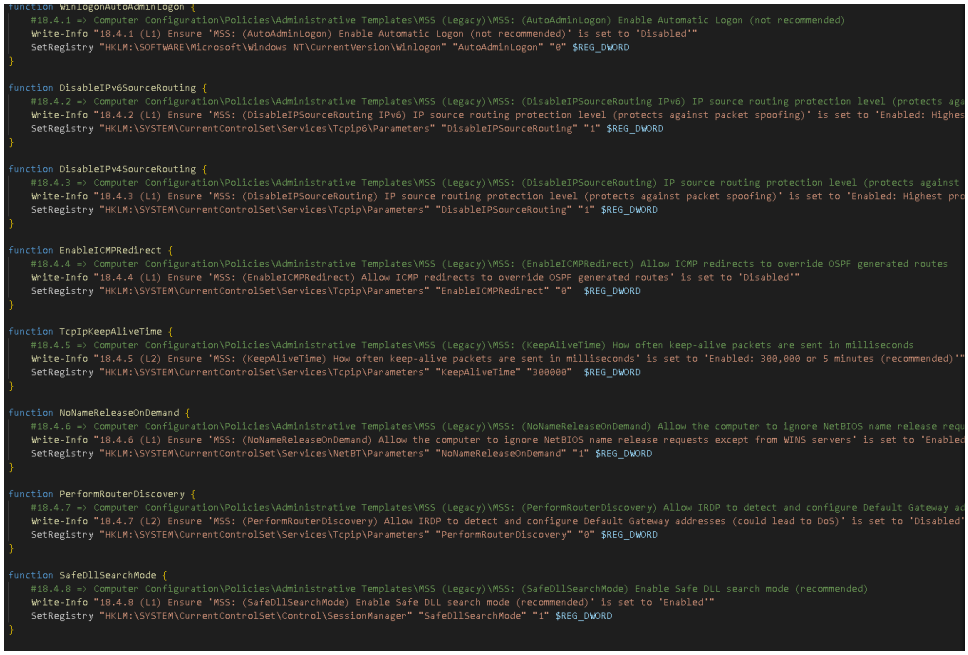
· 18.3.5 Not Applicable to Member Server

· WDigestUseLogonCredential, #18.3.6

```
function DisallowUsersToEnableOnlineSpeechRecognitionServices {
    #18.1.2.1 => Computer Configuration\Policies\Administrative Templates\Control Panel\Regional and Language Options\Allow users to enable online speech recognition
    Write-Info "18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\InputPersonalization" "AllowInputPersonalization" "0" $REG_DWORD
}
function DisallowOnlineTips  {
    #18.1.3 => Computer Configuration\Policies\Administrative Templates\Control Panel\Allow Online Tips
    Write-Info "18.1.3 (L2) Ensure 'Allow Online Tips' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" "AllowOnlineTips" "0" $REG_DWORD
}
function LocalAccountTokenFilterPolicy {
    #18.3.1 => Computer Configuration\Policies\Administrative Templates\MS Security Guide\Apply UAC restrictions to local accounts on network logons
    Write-Info "18.3.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" "LocalAccountTokenFilterPolicy" "1" $REG_DWORD
}

function ConfigureSMBv1ClientDriver  {
    #18.3.2 => Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure SMB v1 client driver
    Write-Info "18.3.2 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\mrxsmb1" "Start" "1" $REG_DWORD
}

function ConfigureSMBv1server {
    #18.3.3 => Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure SMB v1 server
    Write-Info "18.3.3 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" "SMB1" "0" $REG_DWORD
}

function DisableExceptionChainValidation {
    #18.3.4 => Computer Configuration\Policies\Administrative Templates\MS Security Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)
    Write-Info "18.3.4 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\kernel" "DisableExceptionChainValidation" "1" $REG_DWORD
}

function WDigestUseLogonCredential   {
    #18.3.6 => Computer Configuration\Policies\Administrative Templates\MS Security Guide\WDigest Authentication (disabling may require KB2871997)
    Write-Info "18.3.6 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" "UseLogonCredential" "0" $REG_DWORD
}
```

Estas seis funciones son parte de un script de PowerShell que se utiliza para configurar la seguridad en una computadora. La primera función, LocalAccountTokenFilterPolicy, establece el valor de registro de "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" a "LocalAccountTokenFilterPolicy" a "1" como un DWORD. La segunda función, ConfigureSMBv1ClientDriver, establece el valor de registro de "HKLM:\SYSTEM\CurrentControlSet\Services\mrxsmb1" a "Start" a "1" como un DWORD. La tercera función, ConfigureSMBv1server, establece el valor de registro de "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" a "SMB1" a "0" como un DWORD. La cuarta función, DisableExceptionChainValidation, establece el valor de registro de "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\

- **WinlogonAutoAdminLogon, #18.4.1**
- **DisableIPv6SourceRouting, #18.4.2**
- **DisableIPv4SourceRouting, #18.4.3**
- **EnableICMPRedirect, #18.4.4**
- **TcpIpKeepAliveTime, #18.4.5**
- **NoNameReleaseOnDemand, #18.4.6**
- **PerformRouterDiscovery, #18.4.7**
- **SafeDllSearchMode, #18.4.8**
- **ScreenSaverGracePeriod, #18.4.9**
- **TcpMaxDataRetransmissionsV6, #18.4.10**
- **TcpMaxDataRetransmissions, #18.4.11**
- **SecurityWarningLevel, #18.4.12**



```
function WinlogonAutoAdminLogon {
    #18.4.1 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)
    Write-Info "18.4.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "AutoAdminLogon" "0" $REG_DWORD
}

function DisableIPv6SourceRouting {
    #18.4.2 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects ag
    Write-Info "18.4.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highes
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters" "DisableIPSourceRouting" "1" $REG_DWORD
}

function DisableIPv4SourceRouting {
    #18.4.3 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against
    Write-Info "18.4.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest pro
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" "DisableIPSourceRouting" "1" $REG_DWORD
}

function EnableICMPRedirect {
    #18.4.4 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes
    Write-Info "18.4.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" "EnableICMPRedirect" "0"  $REG_DWORD
}

function TcpIpKeepAliveTime {
    #18.4.5 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds
    Write-Info "18.4.5 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" "KeepAliveTime" "300000"  $REG_DWORD
}

function NoNameReleaseOnDemand {
    #18.4.6 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requ
    Write-Info "18.4.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\NetBT\Parameters" "NoNameReleaseOnDemand" "1" $REG_DWORD
}

function PerformRouterDiscovery {
    #18.4.7 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway ad
    Write-Info "18.4.7 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" "PerformRouterDiscovery" "0" $REG_DWORD
}

function SafeDllSearchMode {
    #18.4.8 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
    Write-Info "18.4.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Control\SessionManager" "SafeDllSearchMode" "1" $REG_DWORD
}
```

```
function ScreenSaverGracePeriod {
    #18.4.9 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace per
    Write-Info "18.4.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled:
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "ScreenSaverGracePeriod" "5" $REG_DWORD
}

function TcpMaxDataRetransmissionsV6 {
    #18.4.10 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retrans
    Write-Info "18.4.10 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters" "TcpMaxDataRetransmissions" "3" $REG_DWORD
}

function TcpMaxDataRetransmissions {
    #18.4.11 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitte
    Write-Info "18.4.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" "TcpMaxDataRetransmissions" "3" $REG_DWORD
}

function SecurityWarningLevel {
    #18.4.12 => Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the s
    Write-Info "18.4.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\Eventlog\Security" "WarningLevel" "90" $REG_DWORD
}
```

Cada función configura una opción específica en la configuración del registro del equipo. Por ejemplo, la función WinlogonAutoAdminLogon establece la configuración "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" "AutoAdminLogon" "0" $REG_DWORD para deshabilitar el inicio automático de sesión. Otra función, DisableIPv6SourceRouting, establece la configuración "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters" "DisableIPSourceRouting" "1" $REG_DWORD para desactivar el nivel de protección IP source routing.

- **NETBIOSNODETYPE, #18.5.4.1**

- **ENABLEMULTICAST, #18.5.4.2**

```
function NetBIOSNodeType {
    #18.5.4.1 => Navigate to the Registry path articulated in the Remediation section and confirm it is set as prescribed.
    Write-Info "18.5.4.1 (L1) Set 'NetBIOS node type' to 'P-node' (Ensure NetBT Parameter 'NodeType' is set to '0x2 (2)')"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\NetBT\Parameters" "NodeType" "2" $REG_DWORD
}

function EnableMulticast {
    #18.5.4.2 => Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Turn off multicast name resolution
    Write-Info "18.5.4.2 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" "EnableMulticast" "0" $REG_DWORD
}
```

Estas dos funciones están diseñadas para configurar parámetros específicos en el registro del sistema. La primera función, NetBIOSNodeType, establece un parámetro de registro llamado NodeType en HKLM:\SYSTEM\CurrentControlSet\Services\NetBT\Parameters a un valor de 2. Esto configurará el tipo de nodo NetBIOS en el equipo como un nodo P. La segunda función, EnableMulticast, establece un parámetro de registro llamado EnableMulticast en HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient a un valor de 0. Esto habilitará la resolución de nombres multicast.

· EnableFontProviders, #18.5.5.1

```
function EnableFontProviders {
    #18.5.5.1 => Computer Configuration\Policies\Administrative Templates\Network\Fonts\Enable Font Providers
    Write-Info "18.5.5.1 (L2) Ensure 'Enable Font Providers' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "EnableFontProviders" "0" $REG_DWORD
}
```

Esta función habilita los proveedores de fuentes. Esta función realiza la configuración de la directiva de grupo de Windows para habilitar o deshabilitar los proveedores de fuentes. Esto controla si los usuarios pueden descargar, instalar y usar fuentes de terceros. Esta función configurará el valor de registro en el equipo para garantizar que los proveedores de fuentes estén deshabilitados.

· AllowInsecureGuestAuth, #18.5.8.1

```
function AllowInsecureGuestAuth {
    #18.5.8.1 => Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation\Enable insecure guest logons
    Write-Info "18.5.8.1 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation" "AllowInsecureGuestAuth" "0" $REG_DWORD
}
```

AllowInsecureGuestAuth es una función de Powershell que deshabilita la autenticación de invitados insegura en un equipo. Esta función establece el valor del registro HKLM: \ SOFTWARE \ Policies \ Microsoft \ Windows \ LanmanWorkstation \ AllowInsecureGuestAuth a 0, lo que indica que está deshabilitado. Esto reduce el riesgo de seguridad al evitar que los usuarios de invitado se conecten al equipo sin autenticación.

· LLTDIODisabled, #18.5.9.1

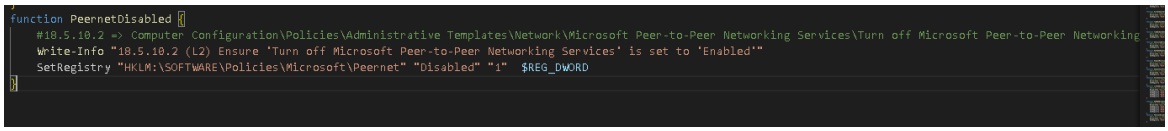
· RSPNDRDisabled, #18.5.9.2

```
function LLTDIODisabled {
    #18.5.9.1 => Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Mapper I/O (LLTDIO) driver
    Write-Info "18.5.9.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\LLTD" "AllowLLTDIOOnDomain" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\LLTD" "AllowLLTDIOOnPublicNet" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\LLTD" "EnableLLTDIO" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\LLTD" "ProhibitLLTDIOOnPrivateNet " "0" $REG_DWORD
}

function RSPNDRDisabled {
    #18.5.9.2 => Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Responder (RSPNDR) driver
    Write-Info "18.5.9.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\LLTD" "AllowRspndrOnDomain" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\LLTD" "AllowRspndrOnPublicNet" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\LLTD" "EnableRspndr" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\LLTD" "ProhibitRspndrOnPrivateNet" "0" $REG_DWORD
}
```

Estas dos funciones están diseñadas para configurar las directivas de administración de Windows para deshabilitar el controlador de descubrimiento de topología de capa de enlace (LLTDIO) y el controlador de respuesta (RSPNDR). Esto se logra estableciendo los valores de

registro en cero para los parámetros especificados. Esto evitará que los usuarios del sistema puedan utilizar estas características.

· PeernetDisabled, #18.5.10.2

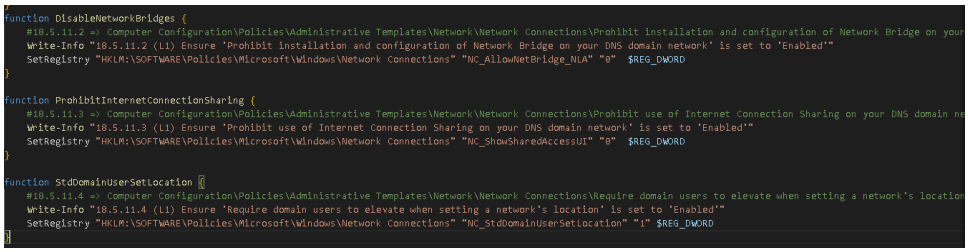


Esta función se utiliza para habilitar el servicio de Peer-to-Peer Networking Services en el equipo. Se escribe un mensaje de información para indicar que la configuración de Turn off Microsoft Peer-to-Peer Networking Services está habilitada. Luego, se establece la clave de registro HKLM:\SOFTWARE\Policies\Microsoft\Peernet para establecer el valor Disabled en 1. El valor se establece como REG_DWORD.

· DisableNetworkBridges, #18.5.11.2

· ProhibitInternetConnectionSharing, #18.5.11.3

· StdDomainUserSetLocation, #18.5.11.



Estas tres funciones son funciones de configuración de seguridad de red para un sistema operativo con Windows. La primera función, DisableNetworkBridges, configura el registro para prohibir la instalación y configuración de una conexión de puente de red en la red DNS. La segunda función, ProhibitInternetConnectionSharing, configura el registro para prohibir el uso de la compartición de conexión a Internet en la red DNS. La tercera función, StdDomainUserSetLocation, configura el registro para exigir que los usuarios de dominio ejecuten elevación cuando se establezca la ubicación de la red.

· HardenedPaths, #18.5.14.1

Esta función es una función de PowerShell para configurar la función de Rutas Protegidas de Windows. Esta función habilita la "Require Mutual Authentication" y "Require Integrity" para todas las comparticiones NETLOGON y SYSVOL. Esta función establece los valores de registro apropiados para asegurarse de que los recursos compartidos estén seguros.

· DisableIPv6DisabledComponents, #18.5.19.2.1

```
function DisableIPv6DisabledComponents {
    #18.5.19.2.1 => Navigate to the Registry path articulated in the Remediation section and confirm it is set as prescribed.
    Write-Info "18.5.19.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)')"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters" "DisabledComponents" "255"  $REG_DWORD
}
```

Esta función se utiliza para deshabilitar los componentes IPv6 en una computadora. La función establece la clave del registro HKLM:\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters para el valor "DisabledComponents" en "255" como un valor de tipo DWORD. Esto deshabilita los componentes IPv6 en la computadora.

- **DisableConfigurationWirelessSettings, #18.5.20.1**

- **ProhibitaccessWCNwizards, #18.5.20.2**

```
function DisableConfigurationWirelessSettings {
    #18.5.20.1 => Computer Configuration\Policies\Administrative Templates\Network\Windows Connect Now\Configuration of wireless settings using Windows Connect Now
    Write-Info "18.5.20.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars" "EnableRegistrars" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars" "DisableUPnPRegistrar" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars" "DisableInBand802DOT11Registrar" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars" "DisableFlashConfigRegistrar" "0" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars" "DisableWPDRegistrar" "0" $REG_DWORD
}

function ProhibitaccessWCNwizards {
    #18.5.20.2 => Computer Configuration\Policies\Administrative Templates\Network\Windows Connect Now\Prohibit access of the Windows Connect Now wizards
    Write-Info "18.5.20.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WCN\UI" "DisableWcnUI" "1"  $REG_DWORD
}
```

Estas dos funciones son utilizadas para configurar los ajustes de conexión inalámbrica usando Windows Connect Now. La función DisableConfigurationWirelessSettings deshabilita la configuración de ajustes inalámbricos usando Windows Connect Now al establecer los valores de registro en HKLM:\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars. La función ProhibitaccessWCNwizards habilita el acceso prohibido a los asistentes de Windows Connect Now al establecer el valor de registro en HKLM:\SOFTWARE\Policies\Microsoft\Windows\WCN\UI.

- **fMinimizeConnections, #18.5.21.1**

- **fBlockNonDomain, #18.5.21.2**

```
function fMinimizeConnections {
    #18.5.21.1 => Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Minimize the number of simultaneous connections to the Int
    Write-Info "18.5.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy" "fMinimizeConnections" "1" $REG_DWORD
}

function fBlockNonDomain {
    #18.5.21.2 => Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Prohibit connection to non-domain networks when connected
    Write-Info "18.5.21.2 (L2) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy" "fBlockNonDomain" "1" $REG_DWORD
}
```

Estas dos funciones configuran los parámetros de seguridad de la conexión de red del equipo. La función fMinimizeConnections se encarga de minimizar el número de conexiones simultáneas a Internet o a un dominio de Windows. La función fBlockNonDomain, por otro lado, se encarga de bloquear las conexiones a redes no relacionadas con el dominio cuando el equipo está conectado a una red autenticada por el dominio. Estas dos funciones modifican el registro del equipo para aplicar los cambios.

- **NoCloudApplicationNotification, #18.7.1.1**

```
}
function NoCloudApplicationNotification {
    #18.7.1.1 => Computer Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Turn off notifications network usage
    Write-Info "18.7.1.1 (L2) Ensure 'Turn off notifications network usage' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNotifications" "NoCloudApplicationNotification" "1" $REG_DWORD
}
```

Esta función establece la configuración de registro para desactivar las notificaciones de uso de la red. Esto significa que los usuarios no recibirán notificaciones sobre el uso de la red o los servicios asociados. Esto se logra estableciendo el valor de la clave "NoCloudApplicationNotification" en el registro HKLM:\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNotifications a 1.

· PROCESSCREATIONINCLUDECMDLINE, #18.8.3.1

```
function ProcessCreationIncludeCmdLine {
    #18.8.3.1 => Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events
    Write-Info "18.8.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit" "ProcessCreationIncludeCmdLine_Enabled" "0" $REG_DWORD
}
```

Esta función establece una directiva de seguridad en el registro del sistema para deshabilitar que la línea de comandos se incluya en los eventos de creación de procesos. Esto ayuda a prevenir ataques de ingeniería inversa, ya que los atacantes no pueden ver la línea de comandos completa utilizada para iniciar un proceso específico.

· ENCRYPTIONORACLEREMEDIATION, #18.8.4.1

· ALLOWPROTECTEDCREDS, #18.8.4.2

```
function EncryptionOracleRemediation {
    #18.8.4.1 => Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\Encryption Oracle Remediation
    Write-Info "18.8.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters" "AllowEncryptionOracle" "0" $REG_DWORD
}

function AllowProtectedCreds {
    #18.8.4.2 => Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\Remote host allows delegation of non-exportable credentials
    Write-Info "18.8.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation" "AllowProtectedCreds" "1" $REG_DWORD
}
```

Encryption Oracle Remediation es una función que se utiliza para asegurar que los clientes estén actualizados. Esto se configura mediante el registro de Windows en el que se establece la clave "AllowEncryptionOracle" en "0". AllowProtectedCreds es una función que se utiliza para habilitar la delegación de credenciales no exportables en el host remoto. Esto se configura mediante el registro de Windows en el que se establece la clave "AllowProtectedCreds" en "1".

· ENABLEVIRTUALIZATIONBASEDSECURITY, #18.8.5.1

· REQUIREPLATFORMSECURITYFEATURES, #18.8.5.2

· HYPERVISORENFORCEDCODEINTEGRITY, #18.8.5.3

· HVCIMATREQUIRED, #18.8.5.4

· LSACFGFLAGS, #18.8.5.5

```
function EnableVirtualizationBasedSecurity {
    #18.8.5.1 => Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security
    Write-Info "18.8.5.1 (NG) Ensure 'Turn On Virtualization Based Security' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" "EnableVirtualizationBasedSecurity" "1" $REG_DWORD
}

function RequirePlatformSecurityFeatures {
    #18.8.5.2 => Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Select Platform Security Level
    Write-Info "18.8.5.2 (NG) Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot and DMA Protection'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" "RequirePlatformSecurityFeatures" "3" $REG_DWORD
}

function HypervisorEnforcedCodeIntegrity {
    #18.8.5.3 => Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Virtualization Based Protection of
    Write-Info "18.8.5.3 (NG) Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock'" ""
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" "HypervisorEnforcedCodeIntegrity" "1" $REG_DWORD
}

function HVCIMATRequired {
    #18.8.5.4 => Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Require UEFI Memory Attributes Tabl
    Write-Info "18.8.5.4 (NG) Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" "HVCIMATRequired" "1" $REG_DWORD
}

function LsaCfgFlags {
    #18.8.5.5 => Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Credential Guard Configuration
    Write-Info "18.8.5.5 (NG) Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" "LsaCfgFlags" "1" $REG_DWORD
}
```

Estas cinco funciones se usan para habilitar la seguridad basada en la virtualización en un sistema Windows. Establecen diferentes opciones de configuración en el Registro de Windows para permitir al sistema usar la seguridad basada en la virtualización. Esto puede incluir la protección contra el arranque no seguro, la protección de la integridad de código basada en el hipervisor, la protección del acceso de memoria basada en el hipervisor y la configuración de Credential Guard.

· CONFIGURESYSTEMGUARDLAUNCH, #18.8.6.7

```
function ConfigureSystemGuardLaunch {
    #18.8.6.7 => Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Secure Launch Configuration
    Write-Info "18.8.5.7 (NG) Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard" "ConfigureSystemGuardLaunch" "1" $REG_DWORD
}
```

Esta función configura una característica de seguridad llamada "Secure Launch Configuration" en Windows Device Guard. Esta característica se utiliza para mejorar la seguridad del sistema al verificar que todos los programas que se ejecutan en el sistema están firmados y autorizados por la empresa. Esta función establece una clave de registro para habilitar la configuración de Secure Launch.

· DRIVERLOADPOLICY, #18.8.14.1

```
function DriverLoadPolicy {
    #18.8.14.1 => Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware\Boot-Start Driver Initialization Policy
    Write-Info "18.8.14.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'"
    SetRegistry "HKLM:\SYSTEM\CurrentControlSet\Policies\EarlyLaunch" "DriverLoadPolicy" "1" $REG_DWORD
}
```

Esta función configura la directiva de inicialización de controladores de inicio de Windows. Establece el valor de registro "DriverLoadPolicy" en "1" en la clave HKLM:\SYSTEM\CurrentControlSet\Policies\EarlyLaunch. Esta directiva le permite a Windows controlar cómo se cargan los controladores de inicio. Configurar esta directiva en "Habilitado: bueno, desconocido y malo pero crítico" permite a Windows cargar controladores de inicio críticos, aunque no sean firmados digitalmente por Microsoft.

- **NoBackgroundPolicy, #18.8.21.2**
- **NoGPOListChanges, #18.8.21.3**
- **EnableCdp, #18.8.21.4**
- **DisableBkGndGroupPolicy, #18.8.21.5**

```
function NoBackgroundPolicy {
    #18.8.21.2 => Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing
    Write-Info "18.8.21.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}" "NoBackgroundPolicy" "0" $REG_DWORD
}

function NoGPOListChanges {
    #18.8.21.3 => Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing
    Write-Info "18.8.21.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}" "NoGPOListChanges" "1" $REG_DWORD
}

function EnableCdp {
    #18.8.21.4 => Computer Configuration\Policies\Administrative Templates\System\Group Policy\Continue experiences on this device
    Write-Info "18.8.21.4 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "EnableCdp" "0" $REG_DWORD
}

function DisableBkGndGroupPolicy {
    #18.8.21.5 => Computer Configuration\Policies\Administrative Templates\System\Group Policy\Turn off background refresh of Group Policy
    Write-Info "18.8.21.5 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' "
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" "DisableBkGndGroupPolicy" "0" $REG_DWORD
}
```

Estas funciones son parte de un script de PowerShell que configura la política de grupo en una computadora. La función NoBackgroundPolicy establece una política en el registro para "No aplicar durante el procesamiento de fondo periódico". La función NoGPOListChanges establece una política en el registro para "Procesar incluso si los objetos de política de grupo no han cambiado". La función EnableCdp establece una política en el registro para "Continuar con las experiencias en este dispositivo". Por último, la función DisableBkGndGroupPolicy establece una política en el registro para "Desactivar la actualización de fondo de la política de grupo".

- **DisableWebPnPDownload, #18.8.22.1.1**
- **PreventHandwritingDataSharing, #18.8.22.1.2**
- **PreventHandwritingErrorReports, #18.8.22.1.3**
- **ExitOnMSICW, #18.8.22.1.4**
- **NoWebServices, #18.8.22.1.5**
- **DisableHTTPPrinting, #18.8.22.1.6**
- **NoRegistration, #18.8.22.1.7**
- **DisableContentFileUpdates, #18.8.22.1.8**
- **NoOnlinePrintsWizard, #18.8.22.1.9**
- **NoPublishingWizard, #18.8.22.1.10**
- **CEIP, #18.8.22.1.11**

```powershell
function DisableWebPnPDownload {
    #18.8.22.1.1 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off downloadi
    Write-Info "18.8.22.1.1 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers" "DisableWebPnPDownload" "1" $REG_DWORD
}

function PreventHandwritingDataSharing {
    #18.8.22.1.2 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriti
    Write-Info "18.8.22.1.2 (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\TabletPC" "PreventHandwritingDataSharing" "1" $REG_DWORD
}

function PreventHandwritingErrorReports {
    #18.8.22.1.3 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriti
    Write-Info "18.8.22.1.3 (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\HandwritingErrorReports" "PreventHandwritingErrorReports" "1" $REG_DWORD
}

function ExitOnMSICW {
    #18.8.22.1.4 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet
    Write-Info "18.8.22.1.4 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' "
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Internet Connection Wizard" "ExitOnMSICW" "1" $REG_DWORD
}

function NoWebServices {
    #18.8.22.1.5 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet
    Write-Info "18.8.22.1.5 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" "NoWebServices" "1" $REG_DWORD
}

function DisableHTTPPrinting {
    #18.8.22.1.6 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing
    Write-Info "18.8.22.1.6 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers" "DisableHTTPPrinting" "1" $REG_DWORD
}

function NoRegistration {
    #18.8.22.1.7 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Registrat
    Write-Info "18.8.22.1.7 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Registration Wizard Control" "NoRegistration" "1" $REG_DWORD
}

function DisableContentFileUpdates {
    #18.8.22.1.8 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Search Co
    Write-Info "18.8.22.1.8 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\SearchCompanion" "DisableContentFileUpdates" "1" $REG_DWORD
}
```

```powershell
function NoOnlinePrintsWizard {
    #18.8.22.1.9 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Orde
    Write-Info "18.8.22.1.9 (L2) Ensure 'Turn off the Order Prints picture task' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" "NoOnlinePrintsWizard" "1" $REG_DWORD
}

function NoPublishingWizard {
    #18.8.22.1.10 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Pub
    Write-Info "18.8.22.1.10 (L2) Ensure 'Turn off the Publish to Web task for files and folders' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" "NoPublishingWizard" "1" $REG_DWORD
}

function CEIP {
    #18.8.22.1.11 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the Wind
    Write-Info "18.8.22.1.11 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Messenger\Client" "CEIP" "1" $REG_DWORD
}
```

Estas son funciones con el objetivo de garantizar la configuración segura de un equipo. Estas funciones establecen la configuración del Registro para deshabilitar la descarga de controladores de impresión a través de HTTP, la compartición de datos de personalización de escritura a mano, informes de errores de reconocimiento de escritura a mano, la asistencia de configuración de conexión a Internet si la URL se refiere a Microsoft.com, descargas Web para publicación en la Web y pedidos en línea, impresión a través de HTTP, registro si la URL se refiere a Microsoft.com, actualizaciones de archivos de contenido de Compañero de búsqueda, tarea de impresión en línea, tarea de publicación en la Web para archivos y carpetas, y Programa de mejora de la experiencia del cliente de Windows Messenger.

· CEIPENABLE, #18.8.22.1.2

```powershell
function CEIPEnable {
    #18.8.22.1.2 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows C
    Write-Info "18.8.22.1.12 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\SQMClient\Windows" "CEIPEnable" "1" $REG_DWORD
}
```

Esta función establece la configuración de la Política de Control de Experiencia de Usuario de Microsoft (CEIP). Esta función hace uso del cmdlet SetRegistry para configurar el valor CEIPEnable en el Registro de Windows como 1. Esto significa que la Política de Control de Experiencia de Usuario se ha habilitado. Esto permitirá que Microsoft recoja información sobre el uso de productos y servicios Microsoft para mejorar la experiencia del usuario.

· TurnoffWindowsErrorReporting, #18.8.22.1.13

```
function TurnoffWindowsErrorReporting {
    #18.8.22.1.13 => Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows
    Write-Info "18.8.22.1.13 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting" "Disabled" "1" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting" "DoReport" "1" $REG_DWORD
}
```

Esta función se utiliza para desactivar el informe de errores de Windows. Establece dos entradas de registro para deshabilitar el informe de errores de Windows con el valor "1" para cada una. Esto significa que el informe de errores de Windows está desactivado.

· SupportDeviceAuthenticationUsingCertificate, #18.8.25.1

```
function SupportDeviceAuthenticationUsingCertificate {
    #18.8.25.1 => Computer Configuration\Policies\Administrative Templates\System\Kerberos\Support device authentication using certificate
    Write-Info "18.8.25.1 (L2) Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'"
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\kerberos\parameters" "DevicePKInitBehavior" "1" $REG_DWORD
    SetRegistry "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\kerberos\parameters" "DevicePKInitEnabled" "1" $REG_DWORD
}
```

Esta función establece la configuración de registro necesaria para habilitar la autenticación de dispositivos usando certificados. Esto significa que los dispositivos se autenticarán usando certificados en lugar de credenciales de usuario. Esta función establece dos claves de registro en el registro de Windows para habilitar el comportamiento de autenticación de dispositivos y habilitarlo.

· DeviceEnumerationPolicy, #18.8.26.1

```
unction DeviceEnumerationPolicy {
    #18.8.26.1 => Computer Configuration\Policies\Administrative Templates\System\Kernel DMA Protection\Enumeration policy for external devices incompatible with Kernel
    Write-Info "18.8.26.1 (L1) Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Kernel DMA Protection" "DeviceEnumerationPolicy" "1" $REG_DWORD
}
```

Esta función configura la directiva de administración de plantillas "Enumeración de políticas para dispositivos externos incompatibles con la protección de Kernel DMA" para bloquear todos los dispositivos externos incompatibles con la protección de Kernel DMA. Esta configuración ayuda a prevenir la ejecución de código malintencionado en el sistema. Establece un valor de registro para habilitar esta configuración.

· BlockUserInputMethodsForSignIn, #18.8.27.1

```
function BlockUserInputMethodsForSignIn {
    #18.8.27.1 => Computer Configuration\Policies\Administrative Templates\System\Locale Services\Disallow copying of user input methods to the system account for sign-
    Write-Info "18.8.27.1 (L2) Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Control Panel\International" "BlockUserInputMethodsForSignIn" "1" $REG_DWORD
}
```

Esta función configura una directiva de grupo para deshabilitar los métodos de entrada de usuario para la cuenta de sistema durante el inicio de sesión. Esto significa que los usuarios

no pueden utilizar sus métodos de entrada de usuario para iniciar sesión en la cuenta de sistema. Esta directiva impide que los usuarios copien sus métodos de entrada de usuario en la cuenta de sistema. Esto ayuda a mejorar la seguridad de la red al evitar que los usuarios accedan a la cuenta de sistema con un método de entrada de usuario comprometido.

- **BlockUserFromShowingAccountDetailsOnSignin, #18.8.28.1**
- **DontDisplayNetworkSelectionUI, #18.8.28.2**
- **DontEnumerateConnectedUsers, #18.8.28.3**
- **EnumerateLocalUsers, #18.8.28.4**
- **DisableLockScreenAppNotifications, #18.8.28.5**
- **BlockDomainPicturePassword, #18.8.28.6**
- **AllowDomainPINLogon, #18.8.28.7**

```
function BlockUserFromShowingAccountDetailsOnSignin {
    #18.8.28.1 => Computer Configuration\Policies\Administrative Templates\System\Logon\Block user from showing account details on sign-in
    Write-Info "18.8.28.1 (L1) Ensure 'Block user from showing account details on signin' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "BlockUserFromShowingAccountDetailsOnSignin" "1" $REG_DWORD
}

function DontDisplayNetworkSelectionUI {
    #18.8.28.2 => Computer Configuration\Policies\Administrative Templates\System\Logon\Do not display network selection UI
    Write-Info "18.8.28.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "DontDisplayNetworkSelectionUI" "1" $REG_DWORD
}

function DontEnumerateConnectedUsers {
    #18.8.28.3 => Computer Configuration\Policies\Administrative Templates\System\Logon\Do not enumerate connected users on domain-joined computers
    Write-Info "18.8.28.3 (L1) Ensure 'Do not enumerate connected users on domainjoined computers' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "DontEnumerateConnectedUsers" "1" $REG_DWORD
}

function EnumerateLocalUsers {
    #18.8.28.4 => Computer Configuration\Policies\Administrative Templates\System\Logon\Enumerate local users on domain-joined computers
    Write-Info "18.8.28.4 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' "
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "EnumerateLocalUsers" "0" $REG_DWORD
}

function DisableLockScreenAppNotifications {
    #18.8.28.5 => Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off app notifications on the lock screen
    Write-Info "18.8.28.5 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "DisableLockScreenAppNotifications" "1" $REG_DWORD
}

function BlockDomainPicturePassword {
    #18.8.28.6 => Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off picture password sign-in
    Write-Info "18.8.28.6 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "BlockDomainPicturePassword" "1" $REG_DWORD
}

function AllowDomainPINLogon {
    #18.8.28.7 => Computer Configuration\Policies\Administrative Templates\System\Logon\Turn on convenience PIN sign-in
    Write-Info "18.8.28.7 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "AllowDomainPINLogon" "0" $REG_DWORD
}
```

Estas funciones son configuraciones de seguridad relacionadas con la pantalla de inicio de sesión de Windows. BlockUserFromShowingAccountDetailsOnSignin bloquea a los usuarios para que no muestren los detalles de su cuenta al iniciar sesión. DontDisplayNetworkSelectionUI impide que el usuario vea una interfaz para seleccionar la red. DontEnumerateConnectedUsers impide que se enumeren los usuarios conectados a un dominio. EnumerateLocalUsers impide enumerar usuarios locales conectados a un dominio. DisableLockScreenAppNotifications impide que se muestren notificaciones de la aplicación en la pantalla de bloqueo. BlockDomainPicturePassword impide que los usuarios inicien sesión utilizando contraseñas de imagen. Finalmente, AllowDomainPINLogon deshabilita el inicio de sesión con PIN para un dominio.

· ALLOWCROSSDEVICECLIPBOARD, #18.8.31.1

· UPLOADUSERACTIVITIES, #18.8.31.2

```
function AllowCrossDeviceClipboard {
    #18.8.31.1 => Computer Configuration\Policies\Administrative Templates\System\OS Policies\Allow Clipboard synchronization across devices
    Write-Info "18.8.31.1 (L2) Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "AllowCrossDeviceClipboard" "0" $REG_DWORD
}

function UploadUserActivities {
    #18.8.31.2 => Computer Configuration\Policies\Administrative Templates\System\OS Policies\Allow upload of User Activities
    Write-Info "18.8.31.2 (L2) Ensure 'Allow upload of User Activities' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" "UploadUserActivities" "0" $REG_DWORD
}
```

Estas dos funciones se utilizan para deshabilitar la sincronización de portapapeles y la carga de actividades de usuario en el registro de Windows. AllowCrossDeviceClipboard configura la clave de registro HKLM:\SOFTWARE\Policies\Microsoft\Windows\System "AllowCrossDeviceClipboard" para tener un valor DWORD de 0. Esto deshabilita la sincronización de portapapeles entre dispositivos. UploadUserActivities configura la misma clave de registro para tener un valor DWORD de 0. Esto deshabilita la carga de actividades de usuario.

· ALLOWNETWORKBATTERYSTANDBY, #18.8.34.6.1

· ALLOWNETWORKACSTANDBY, #18.8.34.6.2

· REQUIREPASSWORDWAKES, #18.8.34.6.3

· REQUIREPASSWORDWAKESAC, #18.8.34.6.4

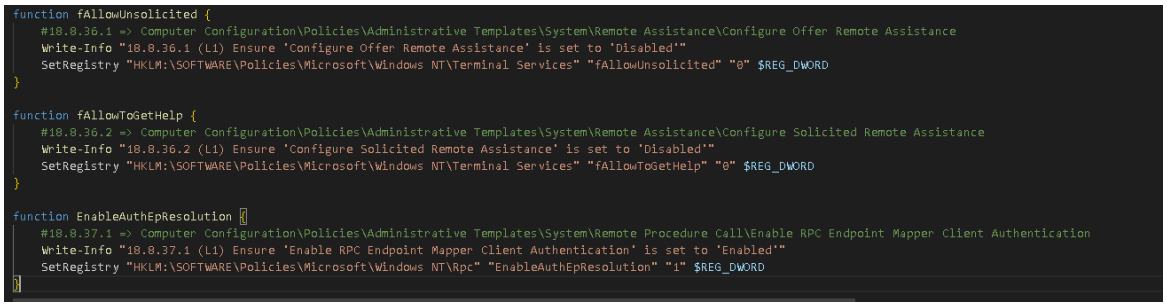
```
function AllowNetworkBatteryStandby {
    #18.8.34.6.1 => Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby
    Write-Info "18.8.34.6.1 (L2) Ensure 'Allow network connectivity during connectedstandby (on battery)' is set to 'Disabled' "
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e898b7-4186-b944-eafa664402d9" "DCSettingIndex" "0" $REG_DWORD
}

function AllowNetworkACStandby {
    #18.8.34.6.2 => Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby
    Write-Info "18.8.34.6.2 (L2) Ensure 'Allow network connectivity during connectedstandby (plugged in)' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e898b7-4186-b944-eafa664402d9" "ACSettingIndex" "0" $REG_DWORD
}

function RequirePasswordWakes {
    #18.8.34.6.3 => Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (on battery
    Write-Info "18.8.34.6.3 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb100d-47d6-a2d5-f7d2daa51f51" "DCSettingIndex" "1" $REG_DWORD
}

function RequirePasswordWakesAC {
    #18.8.34.6.4 => Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in
    Write-Info "18.8.34.6.4 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb100d-47d6-a2d5-f7d2daa51f51" "ACSettingIndex" "1" $REG_DWORD
}
```

Estas funciones están escritas en lenguaje PowerShell y permiten configurar el comportamiento de la energía del equipo. AllowNetworkBatteryStandby deshabilita la conectividad de red durante la conectividad de espera (cuando la batería está conectada). AllowNetworkACStandby deshabilita la conectividad de red durante la conectividad de espera (cuando el enchufe está conectado). RequirePasswordWakes habilita la contraseña cuando el equipo se despierta (cuando la batería está conectada). RequirePasswordWakesAC habilita la contraseña cuando el equipo se despierta (cuando el enchufe está conectado).

· FALLOWUNSOLICITED, #18.8.36.1

- **fAllowToGetHelp, #18.8.36.2**

- **EnableAuthEpResolution**



```
function fAllowUnsolicited {
    #18.8.36.1 => Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance
    Write-Info "18.8.36.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" "fAllowUnsolicited" "0" $REG_DWORD
}

function fAllowToGetHelp {
    #18.8.36.2 => Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance
    Write-Info "18.8.36.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" "fAllowToGetHelp" "0" $REG_DWORD
}

function EnableAuthEpResolution {
    #18.8.37.1 => Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication
    Write-Info "18.8.37.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'"
    SetRegistry "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Rpc" "EnableAuthEpResolution" "1" $REG_DWORD
}
```

Estas tres funciones se utilizan para configurar parámetros de seguridad para la asistencia remota en un equipo con Windows. La función fAllowUnsolicited configura el parámetro "Configure Offer Remote Assistance" con el valor "Deshabilitado", lo que significa que no se permiten ofrecimientos de asistencia remota no solicitados. La función fAllowToGetHelp configura el parámetro "Configure Solicited Remote Assistance" con el valor "Deshabilitado", lo que significa que no se permiten solicitudes de asistencia remota. La función EnableAuthEpResolution configura el parámetro "Enable RPC Endpoint Mapper Client Authentication" con el valor "Habilitado", lo que significa que se requiere autenticación para el acceso al punto de conexión del servicio de registro de procedimiento remoto.