پیکربندی امن

Microsoft Windows Server 2012

مرکز مدیریت راهبردی افتا

SCOS-WIN-SER-2012-V1.0

اسفند ۹۵

فهرست

پیش‌گفتار

مرکز مدیریت راهبردی افتا[1] به منظور ساماندهی امنیت تجهیزات در حوزه فاوا[2]، پروژه «پیکربندی امن محصولات IT در کشور» را آغاز نموده است. یکی از گام‌های اساسی در این پروژه ارائه چک‌لیست و راهنمای پیکربندی امن برای محصولات IT می‌باشد. ارائه چک‌لیست برای محصولات داخلی بر عهده تولیدکننده محصول می‌باشد. تولید کننده ملزم است، چک‌لیست خود را در غالب ارائه شده از سمت مرکز افتا ارائه دهد. چک‌لیست‌های ارائه شده، توسط مرکز افتا مورد ارزیابی قرار گرفته و منتشر می‌گردد. سازمان‌های دولتی ملزم به استفاده از چک لیست‌های مذکور برای محصولات در حال استفاده خود هستند. همچنین سازمان‌های دولتی موظفند قبل از استفاده از محصولات IT، آن‌را مطابق چک‌لیست امنیتی مورد تایید مرکز افتا پیکربندی نمایند.

توجه به این نکته حائز اهمیت می‌باشد که چک‌لیست‌های ارائه شده، یک امنیت سطح پایه برای محصول ایجاد می‌نماید و سازمان‌ها ملزم هستند که برای رسیدن به سطح امنیت مورد نیاز خود، پس از اجرای مدیریت ریسک[3]، الزامات دیگری را نیز به این تنظیمات اضافه و مستند نمایند.

---

[1] امنیت فضای تولید و تبادل اطلاعات

[2] فناوری اطلاعات و ارتباطات

[3] Risk management

مقدمه

این سند راهنمایی برای پیکربندی امن Microsoft Windows Server 2012 است. در این سند مقادیر و تنظیمات امن برای سیاست‌های پیکربندی محصول مذکور ارائه شده است. مخاطب با استفاده از این سند توانایی پیاده‌سازی تنظیمات ارائه شده را خواهد داشت.

این سند توسط شرکت "امن گستر پیام پرداز" و به درخواست و تحت نظارت مرکز مدیریت راهبردی افتا تهیه گردیده است و از تلاش کارشناسان آن شرکت صمیمانه قدردانی می‌گردد. مرکز مدیریت راهبردی افتا ضمن استقبال از نظرات کارشناسان و متخصصان این حوزه برای غنای بیشتر این سند و دیگر اسناد مقاوم سازی، آمادگی دریافت پیشنهادات سازنده از طریق آدرس پست الکترونیکی Hardening@aftasec.ir را اعلام می‌دارد.

در ادامه، تنظیمات مورد نیاز برای پیکربندی امن Microsoft Windows Server 2012 آمده است. در این سند هر تنظیم با یک نام لاتین و شماره مختص آن آورده شده است. برای هر الزام دو بخش شرح اجمالی و نحوه پیاده‌سازی ارائه شده است. در بخش شرح اجمالی، توضیحی مختصر از ماهیت الزام بیان گردیده و در بخش نحوه پیاده‌سازی نیز، راهنمایی برای پیاده‌سازی الزام توسط مدیر سامانه ارائه شده است.

تنظیمات

SCOS-1-1: کاربر با سطح دسترسی Administrative، باید برای فعالیت های مدیریتی و کارهای عملیاتی عادی خود دارای حساب های کاربری جداگانه باشد.

شرح اجمالی:

استفاده از یک حساب کاربری با دسترسی سطح بالا برای فعالیت های عادی میتواند سیستم را در طول برقراری یک نشست (Session) آسیب پذیر نماید و موجب فراهم شدن دسترسی ویژه برای بدافزارها گردد.

نحوه پیاده‌سازی:

هر کاربر با سطح دسترسی Administrative باید یک حساب کاربری برای کارهای عادی و یک حساب کاربری مجزا برای فعالیت های مدیریتی داشته باشد.

SCOS-1-2: طبق سیاست های امنیتی کاربر با حساب کاربری Administrative نباید از برنامه هایی مانند مرورگرهای وب و ایمیل که به اینترنت دسترسی دارند استفاده نماید.

شرح اجمالی:

هنگامی که کاربر با دسترسی اجرایی از یک برنامه که دسترسی به اینترنت دارد استفاده کند ممکن است سیستم را به خطر بیاندازد. اگر آسیب پذیری‌ای در برنامه وجود داشته باشد، سیستم را به خطر می‌اندازد . مرورگر های وب و ایمیل از راه های بسیار رایج برای حمله به استفاده کنندگان است که میتواند بسیار مخرب باشد پس نباید در هنگام دسترسی مدیریتی و اصلی از آنها استفاده کرد و اگر مدیر نیاز به استفاده از اینترنت داشته باشد با سطح دسترسی خود را تغییر بدهد .

این سیاست باید برای مدیریت سرویس های محلی استثناهای خاص تعریف کند. این استثنائات میتواند شامل مواردی از جمله ابزار https base که برای مدیریت سیستم ها ، سرویس ها و دستگاه های متصل که بصورت محلی (local) هستند استفاده شود.

نحوه پیاده‌سازی:

اجرای سیاست امنیتی برای ممنوع کردن استفاده از برنامه هایی که به اینترنت دسترسی دارند مانند مرورگرهای وب و ایمیل توسط کاربری با سطح دسترسی مدیر اجرایی و مطمئن شدن از اجرای دقیق آن سیاست.

SCOS-1-3: قابلیت رمزنگاری برگشت پذیر کلمات عبور باید غیرفعال گردد.

شرح اجمالی:

ذخیره کلمات عبور با استفاده از رمزنگاری برگشت پذیر، عملا مشابه با ذخیره آنها بصورت متن آشکار (clear-text) می باشد و به همین دلیل نباید این ویژگی فعال باشد.

نحوه پیاده‌سازی:

به مسیر زیر رفته و مقدار "Store password using reversible encryption" را به "Disabled" تغییر دهید:

Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

---

SCOS-1-4: درخواست دسترسی از راه دور (Remote Assistance) نباید اجازه داده شود.

شرح اجمالی:

دسترسی از راه دور اجازه مشاهده و تحت کنترل گرفتن یک نشست(Session) که توسط یک کاربر برقرا شده است را به دیگر کاربران میدهد.

نحوه پیاده‌سازی:

به مسیر زیر رفته و مقدار "Configure Solicited Remote Assistance" را به "Disabled" تغییر میدهیم:

Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Remote Assistance

---

SCOS-1-5: اجرای خودکار (Autoplay) برای دستگاه های non-volume باید خاموش (غیر فعال) باشد

شرح اجمالی:

اجرا خودکار ممکن است اجازه دهد که کد های مخرب بر روی سیستم اجرا شود . از آنجا که پخش خودکار باعث میشود به محض قرار گرفتن یک ورودی در دستگاه مانند نتایج یک برنامه، فایلهای تنظیمی یا موزیک و ... آن ها خوانده شود پس این تنظیمات باید برای دستگاه های non-volume مانند (MTP devices) غیر فعال باشد چون ممکن است باعث اجرای یک سری کد مخرب در سیستم شود.

نحوه پیاده‌سازی:

به مسیر زیر رفته و مقدار "Disallow Autoplay for non-volume devices" را به"Enabled" تغییر میدهیم:

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies

---

SCOS-1-6: رفتار (وضع) پیشفرض یک autorun باید برای جلوگیری از دستورات autorun تنظیم (پیکربندی) شود

شرح اجمالی:

دستورات autorun اجازه میدهد کدهای مخرب بر روی سیستم اجرا شوند. باید این تنظیمات برای جلوگیری از اجرای دستورات autorun پیکربندی شوند.

نحوه پیاده‌سازی:

به مسیر زیر رفته و مقدار "Set the default behavior for AutoRun" را به

"Enabled: Do not execute any autorun commands" تغییر میدهیم:

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies

---

SCOS-1-7: اجرای خودکار (Autoplay) باید بر روی درایورها غیر فعال باشند

شرح اجمالی:

اجرا خودکار ممکن است اجازه دهد که کد های مخرب بر روی سیستم اجرا شود . از آنجا که پخش خودکار باعث میشود به محض قرار گرفتن یک ورودی در دستگاه مانند نتایج یک برنامه، فایلهای تنظیمی یا موزیک و ... آن ها خوانده شود و بطور پیشفرض اجرای خودکار برروی درایورهای قابل پاک شدن مانند فلاپی (ولی نه CD-ROM) غیر فعال است پس این تنظیمات باید بر روی همه درایورها غیر فعال باشد چون ممکن است باعث اجرای یک سری کد مخرب در سیستم شود.

نحوه پیاده‌سازی:

به مسیر زیر رفته و مقدار "Turn off AutoPlay" را به"Enabled:All Drives" تغییر میدهیم:

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies

---

SCOS-1-8: نصب کننده ویندوز (Windows Installer) که همیشه با دسترسی بالا و ویژه نصب شود باید غیر فعال شود.

شرح اجمالی:

برای کاربران استاندارد(معمولی) نباید دسترسی ویژه فعال شود. نصب کننده ویندوز اگر مجوز ویژه داشته باشد در هنگام نصب برنامه ها میتواند یک آسیب پذیری پیش بیاید و به افراد و برنامه های غیر مجاز و مخرب اجازه کنترل کامل بر سیستم را میدهد .

نحوه پیاده‌سازی:

به مسیر زیر رفته و مقدار "Always install with elevated privileges" را به"Disabled" تغییر میدهیم:

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Installer

---

SCOS-1-9: مدیریت کنترل از راه دور ویندوز (WinRM) سمت کلاینت نباید از حراز هویت پایه ای و معمولی استفاده کند.

شرح اجمالی: احراز هویت پایه ای از رمز عبور به صورت متن آشکار استفاده میکند که میتواند برای نفوذ به سیستم از آن استفاده شود.

نحوه پیاده‌سازی:

به مسیر زیر رفته و مقدار "Allow Basic authentication" را به"Disabled" تغییر میدهیم:

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Client

---

SCOS-1-10: سرویس مدیریت کنترل از راه دور ویندوز (WinRM) نباید از حراز هویت پایه ای و معمولی استفاده کند.

شرح اجمالی:

احراز هویت پایه ای از رمز عبور به صورت متن آشکار استفاده میکند که میتواند برای نفوذ به سیستم از آن استفاده شود.

نحوه پیاده‌سازی:

به مسیر زیر رفته و مقدار "Allow Basic authentication" را به"Disabled" تغییر میدهیم:

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service -> "Allow Basic authentication" to "Disabled".

SCOS-1-11: سیستم باید یک سرویس پک پشتیبانی داشته باشد.

شرح اجمالی:

سیستم اگر آخرین نسخه سرویس پک پشتیبانی را نداشته باشد یا بروزرسانی های امنیتی برای آسیب پذیری های جدید را دریافت نکند، سیستم را مستعد نفوذ میکند، سیستم باید یک سرویس پک پشتیبانی داشته باشد به همراه بروزرسانی های امنیتی جدید.

نحوه پیاده‌سازی: بروزرسانی سیستم برای استفاده ار نسخه پشتیبان و سرویس پک نهایی.

SCOS-1-12: یک آنتی ویروس تایید شده mci باید نصب و استفاده شود.

شرح اجمالی:

برنامه های اسکن ویروس (آنتی ویروس) اولین قدم در راه مقابله با ویروس های شناخته شده و کدهای مخرب است که این تهدیدات میتوانند اطلاعات را از بین ببرند و کامپیوتر را از کار بیندازند. استفاده از یک برنامه اسکن توانایی جلوگیری از کدهای مخرب را قبل از یک آسیب جدی بالا میبرد.

نحوه پیاده‌سازی:

نصب یک نرم افزار اسکن ویروس (آنتی ویروس) تایید شده توسط mci

SCOS-1-13: فایلهای سیگنیچر آنتی ویروس ها باید بروز نگهداری شوند.

شرح اجمالی:

برنامه های اسکن ویروس اولین قدم در راه مقابله با ویروس های شناخته شده و کدهای مخرب است که این تهدیدات میتوانند اطلاعات را از بین ببرند و کامپیوتر را از کار بیندازند. استفاده از یک برنامه اسکن توانایی جلوگیری از کدهای مخرب را قبل از یک آسیب جدی بالا میبرد. بروزرسانی فایلهای اسکنرهای ویروس (آنتی ویروس) به محافظت از سیستم در برابر بدافزار های جدید که توسط صاحب نرم افزار که بصورت منظم شناسایی میشود کمک کند.

نحوه پیاده‌سازی:

پیکربندی آنتی ویروس بصورتیکه فایلهای سیگنیچر حداقل هر ۷ روز یکبار بروز رسانی شوند. بروز رسانی بیشتر (بصورت مکرر) نیز توصیه میشود.

SCOS-1-14: تنها مدیران مسئول عضو سرور باید حقوق مدیریت سسیستم را داشته باشند.

شرح اجمالی:

حساب کاربری که دارای وظایف administrator نیست نباید حقوق administrator داشته باشد. حقوقی که میتوانند اجازه دور زدن (bypass) حساب کاربری را یا اصلاح محدودیت های امنیتی بر روی سیستم را بدهند و این خود میتواند برای یک حمله (Attack) ایجاد یک آسیب پذیری کند.

مدیران سیستم باید با حساب کاربری ای که حداقل سطح اعتبار سنجی و احراز هویت را دارد وارد سیستم شوند.

برای عضو شدن به سرور های عضو دامنه باید گروه مدیران دامنه با گروه مدیران با سطح دسترسی administrator که عضو سرورهای دامنه هستند جایگزین شوند.

محدود کردن حساب های کاربری ویژه (administrator) از حساب های عادی میتواند خطر افزایش سطح دسترسی را کاهش دهد. البته سیستم هایی که از اکتیو دایرکتوری (active directory) استفاده میکنند معاف از این محدودیت ها هستند.

کاربران عادی نیز نباید عضو گروه مدیرانی با دسترسی administrator باشند.

نحوه پیاده‌سازی:

پیکربندی سیستم به گونه ای که تنها گروه افراد با دسترسی administrator و حساب های کاربری که عهده دار مسئولیت در سیستم هستند باید عضو گروه مدیران با سطح دسترسی بالا (administrato) باشند.

برای عضو شدن به سرور های عضو دامنه باید گروه مدیران عضو دامنه با گروه مدیران با سطح دسترسی administrator که عضو سرورهای دامنه هستند جایگزین شوند. سیستم هایی که از اکتیو دایرکتوری (active directory) استفاده میکنند معاف از این محدودیت ها هستند.

تمام حساب های کاربری عادی باید حذف شوند.

SCOS-1-15 : حافظه های محلی (local) باید از فرمت NTFS استفاده کنند.

شرح اجمالی:

توانای تنظیم مجوزهای دسترسی و حسابرسی برای برقراری امنیت و کنترل دسترسی مناسب به سیستم ضروری است. برای پشتیبانی از این باید حافظه ها از فرمت NTFS استفاده کنند .

نحوه پیاده‌سازی: فرمت کردن تمام پارتیشن ها و درایورها با NTFS

SCOS-1-16:حساب های کاربری نیاز به رمز عبور دارند.

شرح اجمالی:

عدم حفاظت از رمز عبور هر کس را قادر میسازد که به اطلاعات سیسستم دسترسی داشته باشد،که میتواند یک راه نفوذ مانند backdoor برای نفوذ کننده ایجاد کند که به منابع سیستم دست یابد. باید تمام حساب کاربری های سیستم دارای کلمه عبور باشند.

نحوه پیاده‌سازی:

اطمینان از اینکه تمام حساب های کاربری برای دسترسی یه اطلاعات از کلمه عبور استفاده کنند.

رمز عبور مورد نظر را میتوان با خط فرمان (command) زیر تنظیم کرد:

"Net user <account_name> /passwordreq:yes"

SCOS-1-17 : سرورهای ftp باید برای جلوگیری از دسترسی به درایوهای سیستم پیکربندی شوند.

شرح اجمالی:

سرویس های ftp اجازه میدهند تا کاربران بتوانند از راه دور برای دسترسی به فایل های اشتراک گذاری شده و همچنین دایرکتوری های که میتوانند دسترسی به منابع سیستم را فراهم کنند دسترسی داشته باشند و همچنین امکان نفوذ به سیستم را فراهم میکند، بخصوص اگر کاربر بتواند به دایرکتوری های root از درایو های bootدسترسی پیدا کند.

نحوه پیاده‌سازی:

پیکربندی سیستم بگونه ای که از دسترسی سرویس ftp به درایوهای سیستمی جلوگیری شود .

SCOS-1-18 : حساب کاربری کاربران عادی تنها باید مجوز خواندن کلید win logon registry را داشته باشند.

شرح اجمالی:

مجوز کلید win logon registry باید تنها به کاربران با دسترسی ویژه اجازه تغییر مقادیر registry را بدهد. اگر یک کاربر چنین توانایی را داشته باشد میتواند برنامه ها را با دسترسی ویژه اجرا کند هنگامی که کاربران با دسترسی ویژه وارد سیستم هستند.

نحوه پیاده‌سازی:

اطمینان از اینکه به کاربران عادی و گروه های عادی تنها مجوز و دسترسی خواندن registry keys اختصاص داده شود.

تنظیمات پیشفرض بصورت زیر است:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Win logon

---

SCOS-1-19 : حساب کاربری کاربران عادی باید تنها مجوز خواندن Active Setup\Installed Components registry key را داشته باشد.

شرح اجمالی:

مجوز فعال سازی Setup\Installed Components registry keyباید تنها به کاربران با سطح دسترسی ویژه اجازه اضافه کردن و تغییر دادن مقادیر registry را بدهد. . اگر یک کاربر چنین توانایی را داشته باشد میتواند برنامه ها را با دسترسی ویژه اجرا کند هنگامی که کاربران با دسترسی ویژه وارد سیستم هستند.

نحوه پیاده‌سازی:

اطمینان از اینکه به کاربران عادی و گروه های عادی تنها مجوز و دسترسی خواندن registry keys اختصاص داده شود.

تنظیمات پیشفرض بصورت زیر است:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

64-bit systems:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components

---

SCOS-1-20 : دسترسی های ناشناس (غیر مجاز) به registryباید محدود شود.

شرح اجمالی: registry یک جز اساسی و اصلی برای توابع ، امنیت و پایداری و ثبات ویندوز است.برخی از فرایند ها نیاز به دسترسی های ناشناس به registry دارند.این دسترسی ها باید محدود باشند تا سیستم محافظت شود.

نحوه پیاده‌سازی:

اطمینان حاصل کردن از اینکه سیستم برای جلوگیری از بدست آوردن دسترسی کاربران ناشناس به registry پیکربندی شده باشد. حفظ مجوز های پیفرض کلید registry بر اساس مسیر زیر:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\

Administrators - Full

Backup Operators - Read (QENR)

Local Service – Read

SCOS-1-21 : حساب های کاربری داخلی (local) با پسورد های خالی برای جلوگیری از دسترسی داشتن به شبکه باید محدود بشنود.

شرح اجمالی: یک حساب کاربری بدون کلمه عبور اجازه دارد دسترسی غیر مجاز به سیستم داشته باشند که تنها نیاز به نام کاربری داشته باشد. سیاست های امنیتی که برای کلمه عبور وجود دارد باید از وجود حساب کاربری بدون کلمه عبور در سیستم جلوگیری کند. با این حال، اگر حسابهای کاربری محلی (local) بدون کلمه عبور در سیستم وجود دارد ، این تنظیمات باید برای جلوگیری از دسترسی به شبکه هستند، محدود کردن حساب کاربری که تنها بتواند به کنسول محلی ورود کند فعال شوند.

نحوه پیاده‌سازی:

پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Configure the policy value for Computer Configuration -> Windows Settings ->

Security Settings -> Local Policies -> Security Options -> "Accounts: Limit local account use

Of blank passwords to console logon only" to "Enable".

SCOS-1-22 : تفسیر (ترجمه) های SID/Name ناشناخته نباید مجاز باشد.

شرح اجمالی: مجوز تفسیر SID/Name ناشناخته میتواند اطلاعات حساس و حیاتی را برای دسترسی به سیستم فراهم نماید. فقط کاربران مجاز باید قادر به انجام چنین کاری (translation) را داشته باشند

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Allow anonymous SID/Name translation" to "Disabled".

SCOS-1-23 : وجود تعداد ناشناسی از حساب های کاربری پوشه SAM (پوشه حاوی اطلاعات کلمه عبور و نام کاربری در ویندوز) باید غیر مجاز باشد.

شرح اجمالی: وجود تعداد ناشناسی از حساب های کاربری پوشه SAM اجازه ورود غیر مجاز کاربران را به سیستم و دسترسی به لیست تمام حساب های کاربری میدهد، بدین ترتیب یک لیست از نقاط اصلی سیستم فراهم میشود که زمینه حمله به سیستم را فراهم میکند.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings ->

Security Settings -> Local Policies -> Security Options -> "Network access: Do not allow

Anonymous enumeration of SAM accounts" to "Enabled".

SCOS-1-24 : تعداد فرآیندهای ناشناس برای اشتراک گذاری باید محدود شود.

شرح اجمالی: ورود ناشناس کاربران به سیستم و دسترسی آنها به لیستی از نامهای حسابهای کاربری و شمردن تمام منابعی که به اشتراک گذاشته شده میتواند یک نقشه از نقاط حساس سیستم برای حمله به آنرا فراهم نماید.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings ->

Security Settings -> Local Policies -> Security Options -> "Network access: Do not allow Anonymous enumeration of SAM accounts and shares" to "Enabled".

SCOS-1-25 :فرایندهای موازی (pipes) که میتوانند دسترسی ناشناخته به سیستم داشته باشد باید بصورتی پیکربندی شوند که حاوی هیچ مقداری بر روی سرور نباشند.

شرح اجمالی: فرایندهای موازی (همسان) pipes که میتوانند دسترسی های ناشناخته به سیستم داشته باشند بصورت پنهانی و بالقوه دسترسی اعتبارسنجی نشده به سیستم فراهم میکنند. فرایند های موازی فرایند ارتباطی سیستم داخلی هستند.آنها توسط شماره IDها شناسایی میشوند و بین سیستم های مختلف متفاوت هستند.برای اینکه این پردازش ها آسانتر باشد این فرایندهای موازی یکسری نام که بین سیستم های مختلف متفاوت نیستند را میدهند.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings ->

Security Settings -> Local Policies -> Security Options -> "Network access: Named pipes That can be accessed anonymously" to be defined but containing no entries (blank).

SCOS-1-26 : دسترسی غیر مجاز از راه دور به registry paths در دسترس نباید پیکربندی شده باشد.

شرح اجمالی: registry یک جز اساسی و اصلی برای توابع ، امنیت و پایداری و ثبات ویندوز است. برخی از فرایند ها نیاز به دسترسی های از راه دور به registry دارند. تنظیماتی که مثلا registry paths از یک کامپیوتر

از راه دور در دسترس هستند. این registry paths باید محدود شوند، مثلا آنها بتوانندددسترسی اشخاص ناشناس به registry را بدهند.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Remotely accessible registry paths" with the following entries:

System\CurrentControlSet\Control\ProductOptions

System\CurrentControlSet\Control\Server Application

Software\Microsoft\Windows NT\CurrentVersion.

SCOS-1-27 : دسترسی غیر مجاز از راه دور به registry paths و sub-paths که در دسترس هستند نباید پیکربندی شده باشد.

شرح اجمالی: registry یک جز اساسی و اصلی برای توابع ، امنیت و پایداری و ثبات ویندوز است. برخی از فرایند ها نیاز به دسترسی های از راه دور به registry دارند. تنظیماتی که مثلا registry paths و sub-paths از یک کامپیوتر از راه دور در دسترس هستند. این registry paths باید محدود شوند، مثلا آنها بتوانند دسترسی اشخاص ناشناس به registry را بدهند.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Remotely accessible registry paths and sub-paths" with the following entries:

Software\Microsoft\OLAP Server

Software\Microsoft\Windows NT\CurrentVersion\Perflib

Software\Microsoft\Windows NT\CurrentVersion\Print

Software\Microsoft\Windows NT\CurrentVersion\Windows

System\CurrentControlSet\Control\ContentIndex

System\CurrentControlSet\Control\Print\Printers

System\CurrentControlSet\Control\Terminal Server

System\CurrentControlSet\Control\Terminal Server\UserConfig

System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration

System\CurrentControlSet\Services\Eventlog

System\CurrentControlSet\Services\Sysmonlog.

SCOS-1-28 : دسترسی ناشناخته به فرآیندهای موازی و موارد اشتراک گذاری شده باید محدود شوند.

شرح اجمالی: دسترسی های ناشناخته به فرآیند های موازی و موارد اشترک گذاری شده اجازه میدهد که بصورت پنهانی و بالقوه دسترسی بدون اعتبارسنجی به سیستم فراهم شود. این تنظیمات دسترسی به مواردی که در " Network access: Named Pipes that can be accessed anonymously" و " Network access: Shares that can be accessed anonymously" تعریف شده اند را محدود میکند که هردو باید تحت الزامات دیگر خالی باشند.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Restrict anonymous access to Named Pipes and Shares" to "Enabled".

SCOS-1-29 : شبکه مشترک (اشتزاک گذاری شده) که میتواند دسترسی ناشناخته را فراهم کند نباید مجاز باشد.

شرح اجمالی: دسترسی ناشناخته به شبکه مشترک یک دسترسی غیرمجاز به سیستم را توسط کاربران شبکه فراهم کند.که این دسترسی میتواند اطلاعات حساس را افشاء کند یا اینکه آنها را دستکاری (آلوده) کند.

نحوه پیاده‌سازی: اطمینان حاصل شدن از اینکه مقدار این خط مشی طبق مسیر زیر است انجام شده است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Shares that can be accessed anonymously" contains no entries (blank).

SCOS-1-30 : سیستم باید از ذخیره سازی رمزهای hash شده در LAN Manager جلوگیری کند.

شرح اجمالی: LAN Manager hash از یک الگوریتم رمزنگاری ضعیف استفاده می‌کند و چندین ابزار وجود دارد که از این hash برای رمزگذاری و بازیابی رمز حسابهای کاربری استفده میکنند. این تنظیمات خواه ناخواه، hash کلمه‌های عبور LAN Manager را در پوشه SAM ذخیره میکند و در زمانهای بعدی باید تغییر یابد.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network security: Do not store LAN Manager hash value on next password change" to "Enabled".

SCOS-1-31 : سطح اعتبار سنجی LanMan باید تنها مبتنی بر فرستادن پاسخ NTLMv2 تنظیم شود و LMو NTLM را رد کند.

شرح اجمالی: پروتکل اعتبار سنجی Kerberos v5 بطور پیشفرض برای اعتبارسنجی کاربران برای ورود به حساب دامنه میباشد.NTLM ، که امنیت کمتری دارد، در نسخه های بعدی ویندوز برای سازگاری با client و server که در حال اجرای نسخه های قبلی ویندوز و برنامه های کاربردی که از آن استفاده میکنند میباشند نیز نگه داری و ارائه میشود. همچنین آنرا برای اعتبارسنجی ورود به کامپیوترهای مستقل که از نسخه های بعدی استفاده میکنند نیز ارائه میدهند.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network security: LAN Manager Authentication level" to "Send NTLMv2 response only. Refuse LM & NTLM".

SCOS-1-32 : گزینه Recovery Console باید طوری تنظیم شود که از ورود خودکار به سیستم جلوگیری کند.

شرح اجمالی: اگر این گزینه فعال باشد، Recovery Console دیگر نیاز به کلمه عبور ندارد و بصورت خودکار میشود به سیستم ورود پیدا کرد. این میتواند بدون اعتبارسنجی اجازه دسترسی administrative به سیستم را بدهد.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Recovery console: Allow automatic administrative logon" to "Disabled".

SCOS-1-33 : حسابهای کاربری ناشناس نباید حق عمل بعنوان بخشی از سیستم عامل را داشته باشند.

شرح اجمالی: اعطای حقوق(دسترسی) های نامناسب به کاربران میتواند دسترسی های سیستمی و دسترسی های administrative و همچینن دیگر قابلیت های سطح بالا به کاربر بدهد. حسابهای کاربری با حقوق "عمل بعنوان بخشی از سیستم عامل هستند "را میتوانیم فرض کنیم که هر کاربر مشخص شود و به منابع ای دسترسی بگیرد که کاربران با اعتبارسنجی و مجوز به آنها دسترسی دارند. هر حساب کاربری با این حق میتواند کنترل کامل بر سیستم داشته باشد.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Act as part of the operating system" to be defined but containing no entries (blank).

SCOS-1-34 : حسابهای کاربری ناشناس نباید حق ایجاد token object را داشته باشند

شرح اجمالی: اعطای حقوق(دسترسی) های نامناسب به کاربران میتواند دسترسی های سیستمی و دسترسی های administrative و همچینن دیگر قابلیت های سطح بالا به کاربر بدهد. حق "ساختن یک token object " اجازه میدهد یک فرآیند یک دسترسی token ایجاد کند. این میتواند باعث شود که سطح دسترسی و مجوزها ارتقا یابد و به سیستم نفوذ کند .

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings ->Security Settings -> Local Policies -> User Rights Assignment -> "Create a token object" to

be defined but containing no entries (blank)

SCOS-1-35 : حسابهای کاربری ناشناس نباید اجازه debug برنامه را داشته باشند.

شرح اجمالی: اعطای حقوق(دسترسی) های نامناسب به کاربران میتواند دسترسی های سیستمی و دسترسی های administrative و همچینن دیگر قابلیت های سطح بالا به کاربر بدهد. حسابهای کاربری با حق " Debug programs " میتوانند به هر فرآیند یا kernel یک debugger وصل کنند و دسترسی کامل به اطلاعات حساس و اجزای بحرانی سیستم عامل فراهم کنند. این حق به مدیران با دسترسی administrative بصورت پیشفرض داده شده است.

نحوه پیاده‌سازی: پیکربندی کردن مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Debug programs" to only

Include the following accounts or groups:

Administrators

Administrative Templates -> Windows Components -> Windows Defender -> "Configure Microsoft Active Protection Service Reporting " to "Disabled".

SCOS-2-1: سیاست امنیتی الزام میکند که حساب های کاربری با دسترسی administrative نباید از برنامه هایی که به اینترنت دسترسی دارند مانند web browsers و یا برنامه هایی همچون ایمیل که نیاز به اینترنت خارج از سازمان دارند استفاده کنند.

شرح اجمالی: استفاده کردن از برنامه هایی که به اینترنت دسترسی دارند و یا دارای منابع اصلی و بالقوه اینترنت هستند از دسترسی(administrative) برای اینکه یک سیستم را در معرض خطر قرار بدهد، استفاده میکند. اگر یک برنامه دارای نقص در ساختارش باشد میشود هنگامی که یک کاربر با سطح دسترسی ویژه در حال اجرای آن است سیستم را با استفاده از اکسپلویت مورد نظر برای آن نقص در معرض خطر و نفوذ قرار داد. مرورگر های وب و ایمیل از راه های بسیار رایج برای حمله به استفاده کنندگان است که میتواند بسیار مخرب باشد پس نباید در هنگام دسترسی مدیریتی و اصلی از آنها استفاده کرد و اگر مدیر نیاز به استفاده از اینترنت داشته باشد با سطح دسترسی خود را تغییر بدهد .

این سیاست باید برای مدیریت سرویس های محلی استثناهای خاص تعریف کند. این استثنائات میتواند شامل مواردی از جمله ابزار https base که برای مدیریت سیستم ها ، سرویس ها و دستگاه های متصل که بصورت محلی (local) هستند استفاده شود.

نحوه پیاده‌سازی: اجرای سیاست امنیتی برای ممنوع کردن استفاده از برنامه هایی که به اینترنت دسترسی دارند مانند مرورگرهای وب و ایمیل توسط کاربری با سطح دسترسی مدیر اجرایی و مطمئن شدن از اجرای دقیق آن سیاست.

SCOS-2-2: سیاست امنیتی لازم میدارد که طول کلمه عبور حسابهای کاربری برنامه ها باید حداقل ۱۲ کاراکتر باشد.

شرح اجمالی: طول کلمه عبورهای سرویسها/برنامه ها باید به اندازه کافی باشد که به راحتی شکسته(crack) نشود. سرویسها/برنامه هایی که بصورت دستی مدیریت میشوند باید طول کلمه عبور آنها حداقل ۱۲ کاراکتر باشد.

نحوه پیاده‌سازی: اجرای سیاست امنیتی که طول کلمه عبورهای حساب های کاربری که برای سرویسها/برنامه هایی است که بصورت دستی مدیریت میشوند باید بیشتر از ۱۲ کاراکتر باشد و مطمئن شدن از جرای این دستورالعمل.

SCOS-2-3: مجوز وجود حساب های کاربری مشترک (به اشتراک گذاشته شده) بر روی سیستم نباید داده شود.

شرح اجمالی: حساب کاربری مشترک(حساب کاربری ای که دو یا تعداد بیشتری از افراد با تعیین هویت یکسان به سیستم ورود پیدا کنند) نمیتواند به اندازه کافی تعیین هویت (شناسایی) و اعتبار سنجی شود. هیچ راهی برای عدم انکار و مسئولیت پذیری فردی برای دسترسی سیستمی و استفاده از منابع وجود ندارد.

نحوه پیاده‌سازی: پاک کردن هر حساب کاربری مشترک موجود در سیستم.

SCOS-2-4: مدت زمان قفل بودن باید به گونه ای پیکربندی شود که برای باز کردن یک حساب کاربری نیاز به administrator باشد.

شرح اجمالی: هنگامی که ویژگی قفل بودن حساب کاربری فعال باشد از حمله brute-force برروی سیستم جلوگیری میکند. این پارامتر مشخص میکند که یک حساب کاربری پس از تعداد مشخصی تلاش برای ورود به آن قفل باقی بماند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes, "Account is locked out until administrator unlocks it"

SCOS-2-5: تعداد مجاز تلاش برای ورودهای نادرست (bad logon) باید حداقل الزامات را برآورده کند.

شرح اجمالی: هنگامی که ویژگی قفل بودن حساب کاربری فعال باشد از حمله brute-force برروی سیستم جلوگیری میکند. هرچقدر این مقدار بیشتر باشد اثرگذاری ویژگی lockout که از سیستم محلی محافظت میکند کمتر میشود. تعداد لاگین های ناموفق باید به گونه ای منطقی باشد که احتمال حمله موفق به سیستم داخلی (local) به حداقل برسد، درحالیکه اشتباهات سهوی میتواند در طول لاگین یک کاربر معمولی وجود داشته باشد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout threshold" to "5" or less invalid logon attempts (excluding "0" which is unacceptable).

SCOS-2-6: مدت زمان قبل از bad logon counter باید به حداقل مقدار ممکن تنظیم گردد.

شرح اجمالی: هنگامی که ویژگی قفل بودن حساب کاربری فعال باشد از حمله brute-force برروی سیستم جلوگیری میکند. این پارامتر مشخص مدت زمانیست که باید بعد تلاش های ناموفق برای ورود به سیستم بگذرد قبل از آنکه شمارنده مجددا به مقدار صفر تنظیم شود. اگر کوچک تر از این مقدار باشد ویژگی قفل شدن حساب کاربری تاثیر کمتری برا محافظت از سیستم های داخلی دارد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Reset account lockout counter after" to at least "60" minutes

SCOS-2-7: منحصر به فرد بودن (یکتایی) کلمه عبور باید حداقل الزامات را برآورده کند.

شرح اجمالی: یک سیستم نسبت به دسترسی های غیرمجاز بیشتر آسیب پذیر میشود وقتی که کاربران سیستم چندین بار کلمه عبوری مشابه را بازیابی(تنظیم) میکنند، بدون اینکه نیاز به تغییر آنها به یک کلمه عبور منحصر به فرد بر اساس یک بازه زمانی منظم باشد، این کاربران را قادر میسازد تا تغییر کلمه عبور که جز الزامات و قوانین میباشد را رعایت نکنند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Account Policies -> Password Policy -> "Enforce password history" to "5" (or more) passwords remembered.

SCOS-2-8: حداکثر مدت (دوره)ای که کلمه عبور میتواند بدون تغییر بماند باید حداقل الزامات را برآورده کند.

شرح اجمالی: اگر یک کلمه عبور مدت زیادی مورد استفاده قرار گیرد این فرصت رو به برخی افراد میدهد که درباره آن کلمه عبور دانشی غیرمجاز بدست آورند. برنامه ریزی منظم برای تغییر کلمه عبور مانع از فهمیده شدن (crack) کلمه عبور و همچنین دسترسی به سیستم توسط کاربران ناشناخته(غیرمجاز) سیستم میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Account Policies -> Password Policy -> "Maximum password age" to "120" days or less (excluding "0" which is unacceptable).

SCOS-2-9: حداقل مدت (دوره)ای که کلمه عبور میتواند بدون تغییر بماند باید حداقل الزامات را برآورده کند.

شرح اجمالی: مجوزهای کلمه عبور برای تغییر فوری آن در همان روز این اجازه را به کاربر میدهد تا کلمه عبور دوره ای از طریق پایگاه داده آنها تنظیم کند .این کاربران را قادر میسازد تا تغییر کلمه عبور که جز الزامات و قوانین میباشد را رعایت نکنند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Account Policies -> Password Policy -> "Minimum password age" to at least "1" day.

SCOS-2-10: کلمه عبور حداقل باید ۱۲ کاراکتر باشد.

شرح اجمالی: سیستم های اطلاعاتی که با طرح کلمه عبور قوی محافظت نمیشوند (از جمله کلمه عبورهایی با کمترین طول) این فرصت را برای هرکس فراهم میکنند که کلمه عبور را بفهمد(crack کند)، بدین ترتیب به سیستم دسترسی پیدا کرده و به دستگاه، اطلاعات یا شبکه محلی(local) نفوذ میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Account Policies -> Password Policy -> "Minimum password length" to "12" characters

---

SCOS-2-11: سیستم باید به گونه ای پیکربندی شود که Account Logon - Credential Validation successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدارک اعتبارسنجی وقایع مربوط به آزمون اعتبارسنجی برای اعتبار حساب کاربری هر کاربر برای ورود را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings ->Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Logon -> "Audit Credential Validation" with "Success" selected.

SCOS-2-12: سیستم باید به گونه ای پیکربندی شود که Account Logon - Credential Validation failures. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدارک اعتبارسنجی وقایع مربوط به آزمون اعتبارسنجی برای اعتبار حساب کاربری هر کاربر برای ورود را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Logon -> "Audit Credential Validation" with "Failure" selected.

SCOS-2-13: سیستم باید به گونه ای پیکربندی شود که Account Logon - Computer Account Management successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ

(سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدیریت حساب های کاربری کامپیوتر اتفاقاتی مانند ایجاد ، تغییر ، حذف کردن، تغییر نام دادن ، غیرفعال کردن یا فعال کردن حسابهای کاربری کامپیوتر را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Management -> "Audit Computer Account Management" with "Success" selected.

SCOS-2-14: سیستم باید به گونه ای پیکربندی شود که Account Logon - Computer Account Management failures. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدیریت حساب های کاربری کامپیوتر اتفاقاتی مانند ایجاد ، تغییر ، حذف کردن، تغییر نام دادن ، غیرفعال کردن یا فعال کردن حسابهای کاربری کامپیوتر را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Management -> "Audit Computer Account Management" with "Failure" selected.

SCOS-2-15: سیستم باید به گونه ای پیکربندی شود که Account Management - Other Account Management Events successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدیریت رویدادهای حساب های کاربری دیگر نیز اتفاقاتی مانند دسترسی با کلمه عبورهای رمز(hash) شده و یا سیاست چک کردن کلمه عبور بنام API را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Management -> "Audit Other Account Management Events" with "Success" selected.

SCOS-2-16: سیستم باید به گونه ای پیکربندی شود که Account Management - Other Account Management Events failures را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدیریت رویدادهای حساب های کاربری دیگر نیز اتفاقاتی مانند دسترسی با کلمه عبورهای رمز(hash) شده و یا سیاست چک کردن کلمه عبور بنام API را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Management -> "Audit Other Account Management Events" with "Failure" selected

---

SCOS-2-17: سیستم باید به گونه ای پیکربندی شود که Account Management - Security Group Management successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدیریت گروه امنیتی تمام اتفاقات از جمله ایجاد ، حذف ، یا تغییر گروه های امنیتی، شامل تغییر اعضای گروه را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Management -> "Audit Security Group Management" with "Success" selected.

SCOS-2-18: سیستم باید به گونه ای پیکربندی شود که Account Management - Security Group Management failures را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدیریت گروه امنیتی تمام اتفاقات از جمله ایجاد ، حذف ، یا تغییر گروه های امنیتی، شامل تغییر اعضای گروه را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Management -> "Audit Security Group Management" with "Failure" selected.

SCOS-2-19: سیستم باید به گونه ای پیکربندی شود که Account Management - User Account Management successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدیریت حساب های کاربران تمام اتفاقات از جمله ایجاد، تغییر، حذف ، تغییر نام، فعال کردن و غیر فعال کردن حساب های کاربری را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Management -> "Audit User Account Management" with "Success" selected.

SCOS-2-20: سیستم باید به گونه ای پیکربندی شود که Account Management - User Account Management failures.ناموفق را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ

(سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

مدیریت حساب های کاربران تمام اتفاقات از جمله ایجاد، تغییر، حذف ، تغییر نام، فعال کردن و غیر فعال کردن حساب های کاربری را ضبط میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Account Management -> "Audit User Account Management" with " failure" selected.

SCOS-2-21: سیستم باید به گونه ای پیکربندی شود که Detailed Tracking - Process Creation successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

روند ایجاد فرآیند اتفاقات مربوط به ایجاد یک فرآیند و منبع را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Detailed Tracking -> "Audit Process Creation" with "Success" selected.

SCOS-2-22: سیستم باید به گونه ای پیکربندی شود که Logon/Logoff – Logoff successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص

حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

فرایند خروج ، خروج کاربران را ثبت میکند. اگر این یک خروج تعاملی باشد آن در سیستم محلی(local) ثبت میشود، اگر آن بصورت شبکه مشترک باشد آن بر روی سیستم در دسترس(دیده شده) ثبت میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Logon/Logoff -> "Audit Logoff" with "Success" selected.

SCOS-2-23: سیستم باید به گونه ای پیکربندی شود که Logon/Logoff – Logoff successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

فرایند ورود ، ورود کاربران را ثبت میکند. اگر این یک ورود تعاملی باشد آن در سیستم محلی(local) ثبت میشود، اگر آن بصورت شبکه مشترک باشد آن بر روی سیستم در دسترس(دیده شده) ثبت میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Logon/Logoff -> "Audit Logoff" with "Success" selected.

SCOS-2-24: سیستم باید به گونه ای پیکربندی شود که Logon/Logoff – Logoff failures را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

فرایند ورود ، ورود کاربران را ثبت میکند. اگر این یک ورود تعاملی باشد آن در سیستم محلی(local) ثبت میشود، اگر آن بصورت شبکه مشترک باشد آن بر روی سیستم در دسترس(دیده شده) ثبت میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Logon/Logoff -> "Audit Logon" with "Failure" selected.

SCOS-2-25: سیستم باید به گونه ای پیکربندی شود که Logon/Logoff - Special Logon را audit کند successes.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

فرآیند ورود مخصوص ورودهای ویژه که دارای سطح دسترسی administrative هستند و میتوانند فرآیند های سیستم را افزایش دهند ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Logon/Logoff -> "Audit Special Logon" with "Success" selected.

SCOS-2-26 : سیستم باید به گونه ای پیکربندی شود که Object Access - Central Access Policy successes. Staging را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

ممیزی(منظور همان ثبت لاگ هاست) Central Access Policy Staging (چارچوب سیاست دسترسی مرکزی) زیرمجموعه Object Access است که برای فعال کردن ثبت اتفاقات مربوط به تفاوت مجوزها بین سیاست دسترسی مرکزی و سیاست های پیشنهادی استفاده میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings ->Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Object Access -> "Audit Central Access Policy Staging" with "Success" selected.

SCOS-2-27: سیستم باید به گونه ای پیکربندی شود که Object Access - Central Access Policy failures. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

ممیزی(منظور همان ثبت لاگ هاست) Central Access Policy Staging (چارچوب سیاست دسترسی مرکزی) زیرمجموعه Object Access است که برای فعال کردن ثبت اتفاقات مربوط به تفاوت مجوزها بین سیاست دسترسی مرکزی و سیاست های پیشنهادی استفاده میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Object Access -> "Audit Central Access Policy Staging" with "Failure" selected.

SCOS-2-28: سیستم باید به گونه ای پیکربندی شود که Object Access - File System failures. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

ممیزی(منظور همان ثبت لاگ هاست) File System زیرمجموعه Object Access است که برای فعال کردن ثبت اتفاقات مربوط به دسترسی و تغییر فایلها و دایرکتوری ها استفاده میشود. ممیزی(همان لاگ انداختن) باید برای فایلهای سیستمی خاص نیز فعال باشد که آنها هم حسابرسی(لاگهای آنها بررسی) شوند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Object Access -> "Audit File System" with "Failure" selected.

SCOS-2-29: سیستم باید به گونه ای پیکربندی شود که Object Access - Handle Manipulation failures. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است. Handle Manipulation (

رسیدگی به دستکاری ها) زیرمجموعه Object Access است که برای درست فعال کردن ثبت اتفاقات مربوط به دسترسی و تغییر فایلها و دایرکتوری ها مورد نیاز است. ممیزی(همان لاگ انداختن) باید برای فایلهای سیستمی خاص نیز فعال باشد که آنها هم حسابرسی(لاگهای آنها بررسی) شوند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Object Access -> "Audit Handle Manipulation" with "Failure" selected.

SCOS-2-30: سیستم باید به گونه ای پیکربندی شود که Object Access – Registry failures. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.ممیزی(منظور همان ثبت لاگ هاست) Registry زیرمجموعه Object Access است که برای فعال کردن ثبت اتفاقات مربوط به دسترسی و تغییر Registry استفاده میشود. ممیزی(همان لاگ انداختن) باید برای Registry خاص نیز فعال باشد که آنها هم حسابرسی(لاگهای آنها بررسی) شوند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Object Access -> "Audit Registry" with "Failure" selected.

SCOS-2-31: سیستم باید به گونه ای پیکربندی شود که Object Access - Removable Storage successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص

حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Removable Storage زیر مجموعه Object Access است که وقایع مربوط به تلاش برای دسترسی به اشیاء فایل سیستمها برروی دستگاههای ذخیره سازی(حافظه) قابل جابجایی را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Object Access -> "Audit Removable Storage" with "Success" selected.

SCOS-2-32: سیستم باید به گونه ای پیکربندی شود که Object Access - Removable Storage failures. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Removable Storage زیر مجموعه Object Access است که وقایع مربوط به تلاش برای دسترسی به اشیاء فایل سیستمها برروی دستگاههای ذخیره سازی(حافظه) قابل جابجایی را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Object Access -> "Audit Removable Storage" with " failures" selected.

SCOS-2-33: سیستم باید به گونه ای پیکربندی شود که Policy Change - Audit Policy Change successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Audit Policy Change اتفاقات مربوط به تغییر در سیاست ممیزی (بررسی لاگ ها) را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Policy Change -> "Audit Audit Policy Change" with "Success" selected.

SCOS-2-34: سیستم باید به گونه ای پیکربندی شود که Policy Change - Audit Policy Change failures. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Audit Policy Change اتفاقات مربوط به تغییر در سیاست ممیزی (بررسی لاگ ها) را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Policy Change -> "Audit Audit Policy Change" with " Failure" selected.

SCOS-2-35: سیستم باید به گونه ای پیکربندی شود که Policy Change - Authentication Policy Change successes.را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Authentication Policy Change اتفاقات مربوط به تغییر در سیاست احراز هویت ، شامل خط مشی Kerberos و تغییرات Trust را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Policy Change -> "Audit Authentication Policy Change" with "Success" selected.

SCOS-2-36: سیستم باید به گونه ای پیکربندی شود که Privilege Use - Sensitive Privilege Use successes.را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Sensitive Privilege Use تمام اتفاقات مربوط به استفاده از دسترسی های سطح بالای حساس مانند عملکرد "بعنوان بخشی از سیستم عامل" یا "عیب یاب برنامه" را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Privilege Use -> "Audit Sensitive Privilege Use" with "Success" selected.

SCOS-2-37: سیستم باید به گونه ای پیکربندی شود که Privilege Use - Sensitive Privilege Use successes.را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Sensitive Privilege Use تمام اتفاقات مربوط به استفاده از دسترسی های سطح بالای حساس مانند عملکرد "بعنوان بخشی از سیستم عامل" یا "عیب یاب برنامه" را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Privilege Use -> "Audit Sensitive Privilege Use" with " Failure" selected.

SCOS-2-38: سیستم باید به گونه ای پیکربندی شود که System - IPsec Driver successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

IPsec Driver وقایع مربوط به IPSec Driver مانند دور انداختن بسته ها را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> System -> "Audit IPsec Driver" with "Success" selected.

SCOS-2-39: سیستم باید به گونه ای پیکربندی شود که .System - IPsec Driver failures را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

IPsec Driver وقایع مربوط به IPSec Driver مانند دور انداختن بسته ها را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> System -> "Audit IPsec Driver" with "Failure" selected.

SCOS-2-40: سیستم باید به گونه ای پیکربندی شود که System - Security State Change successesرا audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Security State Change اتفاقات مربوط به تغییر در حالت امنیتی مانند شروع(startup) و خاموش کردن(shutdown) را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> System -> "Audit Security State Change" with "Success" selected.

SCOS-2-41: سیستم باید به گونه ای پیکربندی شود که System - Security State Change ailures را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Security State Change اتفاقات مربوط به تغییر در حالت امنیتی مانند شروع(startup) و خاموش کردن(shutdown) را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> System -> "Audit Security State Change" with "Failure" selected.

SCOS-2-42: سیستم باید به گونه ای پیکربندی شود که System - Security System Extension successes.را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Security System Extension وقایع مربوط به فرمت کدهایی که توسط زیرسیستم ها بارگذاری میشوند را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> System -> "Audit Security System Extension" with "Success" selected.

SCOS-2-43: سیستم باید به گونه ای پیکربندی شود که System - Security System Extension failures. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

Security System Extension وقایع مربوط به فرمت کدهایی که توسط زیرسیستم ها بارگذاری میشوند را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> System -> "Audit Security System Extension" with "Failure" selected.

SCOS-2-44: سیستم باید به گونه ای پیکربندی شود که System - System Integrity successes. را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

System Integrity اتفاقات مربوط به نقص موجودیت زیر سیستمهای امنیتی را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> System -> "Audit System Integrity" with "Success" selected

---

SCOS-2-45: سیستم باید به گونه ای پیکربندی شود که System - System Integrity failures را audit کند.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

System Integrity اتفاقات مربوط به نقص موجودیت زیر سیستمهای امنیتی را ثبت میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> System -> "Audit System Integrity" with "Failure" selected

---

SCOS-2-46 : auditکردن دسترسی به Global object (شی سراسری) از فایلهای سیستمی باید برای ثبت عدم موفقیت ها پیکربندی (تنظیم) شود.

شرح اجمالی: اصلاح نامناسب فایلهای سیستمی میتواند تاثیرات قابل توجهی بر پیکربندی امنیت یک سیستم داشته باشد، همچنین میتواند سیستم را از کار اندازد. تلاش های ناموفق برای دسترسی به سیستم ممکن است گویای یک حمله به سیستم باشد. Audit کردن تلاشهای ناموفق برای دسترسی یک شاخص از این تلاش ها فراهم میکند و یک روش نیز برای مشخص (محدود) کردن بخشهای مسئول تهیه مینماید.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Global Object Access Auditing -> "File system" with the following:

Principal: Everyone

Type: Fail

Permissions: all categories selected

اگر این تنظیمات بر روی domain controller بود، در شبکه یا خطی مشی گروه ، هیچ شرایطی برای محدود کردن دامنه تنظیم نشود.

SCOS-2-47 : auditکردن دسترسی به Global object (شی سراسری) از فایلهای سیستمی باید برای ثبت عدم موفقیت ها پیکربندی (تنظیم) شود.

شرح اجمالی: اصلاح نامناسب فایلهای سیستمی میتواند تاثیرات قابل توجهی بر پیکربندی امنیت یک سیستم داشته باشد، همچنین میتواند سیستم را از کار اندازد. تلاش های ناموفق برای دسترسی به سیستم ممکن است گویای یک حمله به سیستم باشد. Audit (حسابرسی لاگ ها) کردن تلاشهای ناموفق برای دسترسی یک شاخص از این تلاش ها فراهم میکند و یک روش نیز برای مشخص(محدود) کردن بخشهای مسئول تهیه مینماید.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Global Object Access Auditing -> "Registry" with the following:

Principal: Everyone

Type: Fail

Permissions: all categories selected

SCOS-2-48: سرویس شبکه‌ی (peer-to-peer) در ویندوز باید خاموش باشد.

شرح اجمالی: برنامه های کاربردی peer-to-peer میتوانند اجازه دسترسی غیرمجاز به سیستم و افشا شدن اطلاعات حساس را بدهند. این تنظیمات باید برای سرویس شبکه همتا به همتا ماکروسافت خاموش باشد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Network -> Microsoft Peer-to-Peer Networking Services -> "Turn off Microsoft Peer-to-Peer Networking Services" to "Enabled".

SCOS-2-49: Network Bridges باید در ویندوز ممنوع باشند.

شرح اجمالی: به یک Network Bridges میشود دو یا چند بخش شبکه متصل کرد، که زمینه دسترسی غیرمجاز و افشای اطلاعات فراهم میشود. این تنظیمات از نصب و پیکربندی یک Network Bridges جلوگیری میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Network -> Network Connections -> "Prohibit installation and configuration of Network Bridge on your DNS domain network" to "Enabled".

SCOS-2-50 : پیکربندی دستگاه های بیسیم که از Windows Connect Now استفاده میکنند باید غیرفعال باشد.

شرح اجمالی: Windows Connect Now اجازه افشا و پیکربندی دستگاه هایی که بصورت بیسیم هستند را میدهد. دستگاه های بیسیم باید مدیریت شوند. اگر یک دستگاه ناشناس مشکوک به سیستم متصل شود یک خطر بالقوه برای اطلاعات حساس هست که ممکن است فاش بشوند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Network -> Windows Connect Now -> "Configuration of wireless settings using Windows Connect Now" to "Disabled".

SCOS-2-51 : Early Launch Antimalware, Boot-Start Driver Initialization Policy باید فعال شود و فقط به Good و Unknown پیکربندی شود.

شرح اجمالی: درمعرض خطر قرار گرفتن boot drivers میتواند بدافزارهای قبلی را برای برخی از مکانیزم های محافظتی که بعد از مقدار دهی اولیه بارگزاری شده اند معرفی کند.Early Launch Antimalware driver میتواند

درایورهای مجاز که توسط برنامه های محافظت دربرابر بدافزار طبقه بندی شده اند را محدود کنند. حداقل drivers بصورت bad نباید اجازه داده شوند

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Early Launch Antimalware -> "Boot-Start Driver Initialization Policy" to "Enabled" with "Good and Unknown" selected.

SCOS-2-52 : اجزا Group Policy باید بازنگری (فرآوری) شوند حتی اگر آنها هیچ تغییری نکرده باشند.

شرح اجمالی: فعال کردن این تنظیمات و سپس انتخاب گزینه

"Process even if the Group Policy objects have not changed" تضمین میکند که این سیاستها بازنگری شده اند حتی اگر هیچ تغییری نکرده باشند. در این صورت هر تغییر بدون اعتبارسنجی ای باید خود را با دامنه مبتنی بر تنظیمات Group Policy مطابقت دهد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Group Policy -> "Configure registry policy processing" to "Enabled" and select the option "Process even if the Group Policy objects have not changed".

SCOS-2-53: Group Policy باید هنگامی که یک کاربر ورود پیدا کرده است در پس زمینه (background) مجددا اجرا شود (تجدید شود).

شرح اجمالی: اگر این تنظیمات فعال باشند، سپس تنظیمات Group Policy درحالی که یک کاربر به سیستم ورود کرده است مجددا اجرا نشود، این میتواند منجر شود به اینکه یک کاربر آخرین تغییرات را به یک سیاست اعمال شده است را نداشته باشد و از این رو در یک محیط ناامن کار کند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Group Policy -> "Turn off background refresh of Group Policy" to "Disabled".

SCOS-2-54: Windows Customer Experience Improvement Program باید غیرفعال باشد.

شرح اجمالی: برخی از ویژگی ها میتوانند با ارائه کننده خدمات، برای ارسال کردن اطلاعات سیستم یا دانلود کردن اطلاعات یا اجزاء سازنده برای ویژگی ها ارتباط برقرار کنند. غیرفعال کردن این قابلیت میتواند از درز کردن اطلاعات حساس به خارج از سازمان و همچنین بروزرسانی های کنترل نشده برای سیستم جلوگیری کند.

این تنظیمات اطمینان حاصل میکند از اینکه Windows Customer Experience Improvement Program

غیرفعال است بنابراین اطلاعات به سازنده یا ارائه کننده خدمت نمیرسند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Internet Communication Management -> Internet Communication Settings -> "Turn off Windows Customer Experience Improvement Program" to "Enabled".

SCOS-2-55 : سیستم باید به نحوی پیکربندی شود که که از ارسال خودکار اطلاعات خطا جلوگیری کند.

شرح اجمالی: این تنظیمات گزارشات خطا به مایکروسافت را کنترل میکنند و اگر یک سایت گزارش خطا شرکت های بزرگ تعریف شده باشد، این با گزارش خطاها به کاربر داخلی تداخل ندارد. از آنجا که محتویات حافظه در این گزارش خطا گنجانده میشود، اطلاعات حساس ممکن است به مایکروسافت ارسال شوند. این ویژگی باید غیرفعال شود تا از افشای چنین اطلاعاتی جلوگیری شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings -> "Turn off Windows Error Reporting" to "Enabled".

SCOS-2-56: ویندوز باید از جستجوی درایورها توسط Windows Update جلوگیری کند.

شرح اجمالی: برخی از ویژگی ها میتوانند با ارائه کننده خدمات، برای ارسال کردن اطلاعات سیستم یا دانلود کردن اطلاعات یا اجزاء سازنده برای ویژگی ها ارتباط برقرار کنند. غیرفعال کردن این قابلیت میتواند از درز کردن اطلاعات حساس به خارج از سازمان و همچنین بروزرسانی های کنترل نشده برای سیستم جلوگیری کند.

این تنظیمات باعث میشود که ویندوز از جستجوی درایورهای دستگاه توسط Windows Update زمانی که هیچ درایور محلی (local) موجود نیست جلوگیری کند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings -> "Turn off Windows Update device driver searching" to "Enabled".

SCOS-2-57 : کاربران محلی بر روی کامپیوترهای متصل به دامنه نباید برشمرده شوند.

شرح اجمالی: نام کاربری بخشی از اعتبار ورود به سیستم است که میتواند برای بدست آوردن دسترسی استفاده شود. قابلیت شمارش کاربران تنها باید در اختیار کاربران مجاز قرار بگیرد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Logon -> "Enumerate local users on domain-joined computers" to "Disabled".

SCOS-2-58: سیستم باید به نحوی پیکربندی شود که از پیشنهاد دسترسی(کمک) از راه دور بصورت ناخواسته جلوگیری کند.

شرح اجمالی: دسترسی از راه دور میتواند امکان مشاهده و گرفتن کنترل نشست(session) محلی یک کاربر را برای دیگر کاربران فراهم نماید. دسترسی ناخواسته از راه دور یک دسترسی است که توسط یک کاربر از راه دور ارائه میشود. این میتواند اجازه دسترسی غیرمجاز به منابع سیستم را فراهم کند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Remote Assistance -> "Configure Offer Remote Assistance" to "Disabled".

SCOS-2-59: استفاده از بیومتریک(biometrics) باید غیرفعال باشد.

شرح اجمالی: بیومتریک (biometrics) اجازه دور زدن روشهای احراز هویت ضروری را فراهم میکند. بیومتریک تنها میتواند در فاکتورهای احراز هویت اضافه استفاده شود که در آن افزایش قدرت اعتبارسنجی احراز هویت ضروری و یا مطلوب است. فاکتورهای اضافی دیگر باید در محدوده سیاست های mci باشند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Biometrics -> "Allow the use of biometrics" to "Disabled".

SCOS-2-60 : دکمه ی نشان دادن کلمه عبور باید غیرفعال باشد.(همان دکمه ای که باعث میشود پسورد بصورت واضح نشان داده شود باید غیرفعال شود)

شرح اجمالی: کلمه عبور قابل رویت ممکن است توسط افراد نزدیک ما دیده شود و آن را در معرض خط و سوءاستفاده قرار دهد. دکمه نشان دادن کلمه عبور باعث میشود که کلمه عبور وارد شده بصورت واضح نشان داده شود و به همین دلیل نباید اجازه داده شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Credential User Interface -> "Do not display the password reveal button" to "Enabled".

SCOS-2-61: Explorer Data Execution Prevention باید فعال باشد.

شرح اجمالی: Data Execution Prevention (DEP) حفاظت بیشتری را از طریق چک کردن حافظه که به جلوگیری از اجرای کدهای مخرب کمک میکند فراهم میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> File Explorer -> "Turn off Data Execution Prevention for Explorer" to "Disabled".

SCOS-2-62 : باید از به اشتراک گذاری درایورهای محلی (local) توسط Remote Desktop Hosts Session ((Remote Desktop Services Role) جلوگیری شود.

شرح اجمالی: جلوگیری از به اشتراک گذاشتن درایورهای محلی بر دیگر کامپیوترهای کلاینت با Remote Session Hosts توسط کاربران که آنها هم دسترسی داشته باشند کمک به کاهش افشای احتمالی اطلاعات حساس میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Device and Resource Redirection -> "Do not allow drive redirection" to "Enabled".

SCOS-2-63: سرویس Remote Desktop باید بگونه ای پیکربندی شود که اتصالات رمز شده بین کلاینت ها در سطح مورد نیازی تنظیم شده باشد.

شرح اجمالی: اتصالات از راه دور باید برای جلوگیری از افشای اطلاعات حساس و داده ها رمز شوند . انتخاب سطح "High Level" میتواند اطمینان حاصل کند که رمز گذاری Remote Desktop Services در دو طرف ارتباط انجام میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Security -> "Set client connection encryption level" to "Enabled" and "High Level".

SCOS-2-64: سرویس Remote Desktop باید بگونه ای پیکربندی شود که یک زمان مشخص برای قطع ارتباط تنظیم شود.

شرح اجمالی: این تنظیمات کنترل میکند که یک ارتباط چه مدت زمانی باید برقرار باشد اگر آن برخلاف انتظار قطع شده است(خاتمه یافته است). ارتباطاتی که مثلا از منابع سیستم استفاده میکنند باید سریع ترین زمان ممکن قطع شوند.(به محض اتمام فعالیت قطع شوند)

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Session Time Limits -> "Set time limit for disconnected sessions" to "Enabled", and "End a disconnected session" to "1 minute".

SCOS-2-65: عضویت Microsoft Active Protection Service باید غیرفعال باشد.

شرح اجمالی: برخی از ویژگی ها میتوانند با ارائه کننده خدمات، برای ارسال کردن اطلاعات سیستم یا دانلود کردن اطلاعات یا اجزاء سازنده برای ویژگی ها ارتباط برقرار کنند. غیرفعال کردن این قابلیت میتواند از درز کردن اطلاعات حساس به خارج از سازمان و همچنین بروزرسانی های کنترل نشده برای سیستم جلوگیری کند.

این تنظیمات عضویت Microsoft Active Protection Service را غیرفعال میکند و گزارش میدهد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Windows Defender -> "Configure Microsoft Active Protection Service Reporting " to "Disabled".

SCOS-2-66: باید از تغییر گزینه های نصب و راه اندازی توسط کاربران جلوگیری شود.

شرح اجمالی: گزینه های امنیتی برای برنامه های کاربردی معمولا به وسیله کاربران با دسترسی administrators کنترل میشود. باید از تغییر گزینه های نصب و راه اندازی توسط کاربران جلوگیری شود چونکه ممکن است تدابیر امنیتی دور زده شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Windows Installer -> "Allow user control over installs" to "Disabled".

SCOS-2-67 : باید از دسترسی Windows Media Digital Rights Management (DRM) به اینترنت جلوگیری شود.

شرح اجمالی: برخی از ویژگی ها میتوانند با ارائه کننده خدمات، برای ارسال کردن اطلاعات سیستم یا دانلود کردن اطلاعات یا اجزاء سازنده برای ویژگی ها ارتباط برقرار کنند. غیرفعال کردن این قابلیت میتواند از درز کردن اطلاعات حساس به خارج از سازمان و همچنین بروزرسانی های کنترل نشده برای سیستم جلوگیری کند.

این بررسی تایید میکند که Windows Media DRM به اینترنت دسترسی ندارد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Windows Media Digital Rights Management -> "Prevent Windows Media DRM Internet Access" to "Enabled".

SCOS-2-68 : باید از بررسی خودکار Windows Media Player برای بروزرسانی جلوگیری شود.

شرح اجمالی: در بروز رسانی های بدون کنترل برای سیستم مسائلی مطرح می‌شود. بروزرسانی خودکار توسط Windows Media Player باید غیرفعال شود تا از ثابت بودن پلتفرم اطمینان حاصل شود و از معرفی برنامه های شناخته نشده/ تست نشده بر روی سیستم جلوگیری شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Windows Media Player -> "Prevent Automatic Updates" to "Enabled".

SCOS-2-69: طرف کلاینت نباید اجازه رمزگشایی ترافیک را داشته باشد. (WinRM) مدیریت از راه دور ویندوز

شرح اجمالی: دسترسی از راه دور رمز نشده به سیستم میتواند اجازه افشا شدن و نفوذ به اطلاعات حساس سیستم را بدهد ارتباطات مدیریت از راه دور ویندوز (Windows remote management) باید برای جلوگیری از همین موضوع رمز گذاری شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Client -> "Allow unencrypted traffic" to "Disabled".

SCOS-2-70: سرویس The Windows Remote Management (WinRM) نباید اجازه دهد که ترافیک رمز نشود.

شرح اجمالی: دسترسی از راه دور رمز نشده به سیستم میتواند اجازه افشا شدن و نفوذ به اطلاعات حساس سیستم را بدهد ارتباطات مدیریت از راه دور ویندوز (Windows remote management) باید برای جلوگیری از همین موضوع رمز گذاری شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service -> "Allow unencrypted traffic" to "Disabled".

SCOS-2-71: Remote Desktop Session سمت میزبان (host) نیاز به ارتباطات امن RPC دارد.

شرح اجمالی: اگر سیستم اجازه استفاده از ارتباطات RCP را بدهد سیستم مستعد حمله man-in-the-middle میشود و همچنین داده های سیستم فاش میشود. Man-in-the-middle زمانی اتفاق میفتد که یک حمله کننده(جاسوس) بین کلاینت و سرور میشیند و بسته های که بین آنها منتقل میشود را بدون اجازه شنود کرده و قبل از رد و بدل شدن آنها را تغییر میدهد. معمولا حمله کننده(attacker) در این تلاش سعی میکند که در بسته ها تغییر ایجاد کند و همچنین سبب شود که کلاینت یا سرور اطلاعات حساس خود را آشکار کنند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Security -> "Require secure RPC communication" to "Enabled".

SCOS-2-72: نشان دادن slide shows بر روی صفحه نمایش قفل شده نباید مجاز باشد.(Windows 2012 R2)

شرح اجمالی: نمایش slide show برروی صفحه نمایش قفل شده میتواند اطلاعات حساس را برای پرسنل غیر مجاز نشان دهد. غیر فعال کردن این ویژگی میتواند دسترسی به اطلاعات را هنگامی که یک کاربر به سیستم ورود پیدا کرده است محدود کند.

نحوه پیاده‌سازی: این تنظیمات برای اولین نسخه Windows 2012 نیاز نبود اما برای Windows 2012 R2 مناسب است.

پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Control Panel -> Personalization -> "Prevent enabling lock screen slide show" to "Enabled".

SCOS-2-73: رویدادهای ایجاد فرآیند باید شامل داده های خط فرمان (Command line data) باشند. (Windows 2012 R2)

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است. این تنظیمات ثبت وقایع داده های اضافی را برای اتفاقات ایجاد فرآیند را قادر میسازد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Audit Process Creation -> "Include command line in process creation events" to "Enabled".

SCOS-2-74: بعد از اینکه سیستم دوباره راه اندازی میشود باید از کاربر خواسته شود دوباره اطلاعات خود را وارد کند.(یعنی از ورود خودکار جلوگیری شود.)

شرح اجمالی: Windows 2012 R2 می تواند به گونه ای پیکربندی شود که بطور خودکار بعد از restart مربوط به آپدیت ویندوز، کاربر را به سیستم وارد کند. (sign in back) .بعضی تمهیدات وجود دارند که سبب میشود این عمل بصورت امن صورت گیرد، با این وجود غیر فعال کردن این قابلیت مانع از caching اطلاعات حساس میشود و نیز اطمینان حاصل میکند که کاربر از restart مطلع است.

نحوه پیاده‌سازی: این تنظیمات برای اولین نسخه Windows 2012 نیاز نبود اما برای Windows 2012 R2 قابل اجرا است.

پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Windows Components -> Windows Logon Options -> "Sign-in last interactive user automatically after a system-initiated restart" to "Disabled".

SCOS-2-75: مجوز پوشه root درایو سیستم (معمولا C:\) باید با حداقل نیازمندیها مطابقت کند.

شرح اجمالی: تغییر در فایلهای سیستمی و مجوزهای دایرکتوری اجازه ی تغییرات غیرمجاز و ناشناخته بر روی سیستم عامل و همچنین نصب برنامه ها را میدهد.

مجوزهای پیشفرض برای زمانی که گزینه ی امنیتی

"Network access: Let everyone permissions apply to anonymous users" بر روی"Disabled" تنظیم شود کافی است(V-3377).

نحوه پیاده‌سازی: حفظ مجوزهای پیشفرض برای دایرکتوری ریشه(root) درایو سیستم و پیکربندی گزینه امنیتی:

"Network access: Let everyone permissions apply to anonymous users" به "Disabled" (V-3377).

مجوزهای پیشفرض :

C:\

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

SYSTEM - Full control - This folder, subfolders and files

Administrators - Full control - This folder, subfolders and files

Users - Read & execute - This folder, subfolders and files

Users - Create folders / append data - This folder and subfolders

Users - Create files / write data - Subfolders only

CREATOR OWNER - Full Control - Subfolders and files only

SCOS-2-76: مجوز برای دایرکتوری فایلهای برنامه باید با حداقل نیازها(ی امنیتی) مطابقت کند .

شرح اجمالی: تغییر در فایلهای سیستمی و مجوزهای دایرکتوری اجازه ی تغییرات غیرمجاز و ناشناخته بر روی سیستم عامل و همچنین نصب برنامه ها را میدهد.

مجوزهای پیشفرض برای زمانی که گزینه ی امنیتی Network access: Let everyone permissions apply to "anonymous users" بر روی"Disabled" تنظیم شود کافی است(V-3377).

نحوه پیاده‌سازی: حفظ مجوزهای پیشفرض برای دایرکتوری فایلهای برنامه و پیکربندی گزینه امنیتی:

"Network access: Let everyone permissions apply to anonymous users" به "Disabled" (V-3377).

مجوزهای پیشفرض :

\Program Files and \Program Files (x86)

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

TrustedInstaller - Full control - This folder and subfolders

SYSTEM - Modify - This folder only

SYSTEM - Full control - Subfolders and files only

Administrators - Modify - This folder only

Administrators - Full control - Subfolders and files only

Users - Read & execute - This folder, subfolders and files

CREATOR OWNER - Full control - Subfolders and files only

ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders and files

---

SCOS-2-77 : مکانیزم های سیستم باید بگونه ای پیاده سازی شوند که انقضای کلمه عبور بطور خودکار اجرا شود.

شرح اجمالی: کلمه عبور اگر منقضی نشود و یا دوباره مورد استفاده قرار گیرد احتمال افشا و Crack شدن آن افزایش میابد .

نحوه پیاده‌سازی: پیکربندی تمام کلمه عبورها برای اینکه منقضی شوند. اطمینان حاصل کردن از اینکه " Password never expires" برای هیچ حساب کاربری ای بررسی نمیشود. هر دستورالعملی غیر از این باید با IAO باشد.

SCOS-2-78 : سرور FTP باید به گونه ای پیکربندی شود که از ورودهای ناشناس جلوگیری کند.

شرح اجمالی: سرویس FTP (File Transfer Protocol) اجازه میدهد که کاربران از راه دور به فایلهای اشتراک گذاری شده و دایرکتوری ها دسترسی داشته باشند. مجوز ارتباط FTP بصورت ناشناخته audit کاربران را دشوار میکند.

استفاده از حساب کاربری با دسترسی سطح administrator خطر مسحوب میشود چونکه شماره شناسه و کلمه عبور برروی شبکه capture میشود و دسترسی در سطح administrator به کاربران غیرمجاز میدهد.

نحوه پیاده‌سازی: جلوگیری از اینکه که سرویس FTP نصب شده اجازه ورود کاربران ناشناخته را ندهد.

SCOS-2-79: حساب کاربری مهمان موجود(سیستمی) باید غیرفعال شود.

شرح اجمالی: اگر این ویژگی غیرفعال نشود سیستم در معرض افزایش تهدید آسیب پذیری قرار میگیرد. این حساب کاربری یک حساب کاربری شناخته شده است که برروی تمام سیستم های ویندوزی است و نمیتوان آنرا پاک کرد. به این حساب کاربری در طول نصب و راه اندازی اولیه سیستم عامل هیچ کلمه عبوری اختصاص داده نمیشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Accounts: Guest account status" to "Disabled".

SCOS-2-80: حساب کاربری administrator موجود (سیستمی) باید تغییر نام داده شود.

شرح اجمالی: حساب کاربری administrator موجود (سیستمی) یک حساب کاربری شناخته شده برای attack است.

تغییر نام دادن حساب کاربری به نام ناشناس حفاظت از این حساب کاربری و سیستم را بهبود میبخشد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Accounts: Rename administrator account" to a name other than "Administrator".

SCOS-2-81 : خطی مشی audit با استفاده از زیرشاخه ها باید فعال شود.

شرح اجمالی: نگهداری یک دنباله ممیزی از لاگ فعالیت های سیستم میتواند به تشخیص خطاهای پیکربندی ، عیب یابی اختلالات موجود در سرویسها ، تحلیل نفوذهایی(سوءاستفاده) که اتفاق افتاده است و همچنین تشخیص حملات کمک کند. ممیزی لاگ ها برای تهیه دنباله ای از مدارک در مورد سیستم یا شبکه ای که مورد نفوذ (سوءاستفاده) قرار گرفته است بسیار ضروری است. جمع آوری این اطلاعات برای تحلیل امنیت دارایی های اطلاعاتی و تشخیص نشانه های مشکوک و رفتارهای غیر منتظره بسیار ضروری است.

این تنظیمات به administrators اجازه میدهد توانایی audit (ممیزی) دقیق تر فعال شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to "Enabled".

SCOS-2-82: سیستم باید بگونه ای پیکربندی شود که یک کلید قوی برای نشست(session) نیاز داشته باشد.

شرح اجمالی: یک کامپیوتر متصل به کنترل کننده دامنه (DC) باید از طریق یک کانال امن ارتباط برقرار کند.نیاز است که کلید قوی برای نشست (session) از رمزگذاری ۱۲۸ بیتی بین سیستمها استفاده کند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Domain member: Require strong (Windows 2000 or Later) session key" to "Enabled".

SCOS-2-83: کلید امنیتی Ctrl+Alt+Del دنباله امنیتی باید فعال باشد.

شرح اجمالی: غیرفعال کردن کلید امنیتی Ctrl+Alt+Del میتواند باعث نفوذ به سیستم امنیتی شود. از آنجا که تنها ویندوز به کلید امنیتی Ctrl+Alt+Del پاسخ میدهد ، کاربر میتواند مطمئن شود که هر کلمه عبور وارد شده تنها به ویندوز فرستاده میشود. اگر نیاز دنباله حذف شود ، برنامه های مخرب میتوانند کلمه عبور ویندوزی کاربران را درخواست و دریافت کنند. غیرفعال کردن این دنباله از اعلان ورود کاربر نیز جلوگیری میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Interactive Logon: Do not require CTRL+ALT+DEL" to "Disabled".

SCOS-2-84: آستانه قفل شدن حساب کاربری باید بر روی سیستم با BitLocker روی ۱۰ تنظیم شود.

شرح اجمالی: هنگامی که ویژگی قفل بودن حساب کاربری فعال باشد از حمله brute-force برروی سیستم جلوگیری میکند.هرچقدر این مقدار بیشتر باشد اثرگذاری ویژگی lockout که از سیستم محلی محافظت میکند کمتر میشود.تعداد لاگین های ناموفق باید به گونه ای منطقی باشد که احتمال حمله موفق به سیستم داخلی (local) به حداقل برسد، درحالیکه اشتباهات سهوی میتواند در طول لاگین یک کاربر معمولی وجود داشته باشد.

نحوه پیاده‌سازی: اگر BitLocker برروی سیستم عامل فعال باشد ، پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Interactive logon: Machine account lockout threshold" to "10" invalid logon attempts

---

SCOS-2-85: اخطار قانونی مورد نیاز باید با به نحوی پیکربندی شود که قبل از نمایش کنسول ورود نمایش داده شود.

شرح اجمالی: عدم نمایش logon banner قبل از تلاش برای ورود اقدامات قانونی ناشی از دسترسی غیرمجاز به منابع سیستم را نفی میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Interactive Logon: Message text for users attempting to log on" بصورت زیر است:

شما به یک MCI Information System (IS) دسترسی دارید که تنها برای استفاده MCIی مجاز ارائه میشود.

برای استفاده از این IS (که شامل هر دستگاه متصل به این به این IS میشود)، شما باید با شرایط زیر موافق باشید:

MCI بطور معمول ارتباطات برروی این IS را رهگیری و مانیتور میکند برای اهدافی ازجمله : تست نفوذ، COMSEC monitoring، عملیات شبکه و دفاع ، سوءرفتار پرسنل(PM)، اجرای قانون(LE) و تحقیقات سازمان ضدجاسوسی (CI). اما تنها محدود به این موارد نمیشود.

هر لحظه ممکن است MCI برروی IS داده ها را بررسی و توقیف کند.

ارتباطات استفاده شده در MCI و یا داده های ذخیره شده برو IS خصوصی نیستند، یک هدف برای مانیتورینگ روتین، رهگیری ، جستجو، و ممکن است آشکار شوند و برای هر هدف دارای اعتبار MCI استفاده شوند.

این IS شامل معیارهای امنیتی (e.g., authentication and access controls) برای حفاظت از منافع MCI نه برای منفعت پرسنل و خطی مشی ها میشود.

SCOS-2-86: کلمه عبور رمز نشده نباید به بخش (شخص) سوم سرور SMB فرستاده شود.

شرح اجمالی: برخی از سرویس های SMB به غیر از مایکروسافت تنها احراز هویت کلمه عبور رمز نشده(متن آشکار) را پشتیبانی میکنند. ارسال کلمه عبور بصورت متن آشکار هنگام اعتبار دادن به یک سرور SMB برروی شبکه ، امنیت سرتاسر محیط را کاهش میدهد. بررسی Vendorسرور SMB نشان میدهد که راهی برای پشتیبانی از کلمه عبور رمز شده وجود دارد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Microsoft network client: Send unencrypted password to connect to third-party SMB servers" to "Disabled"

SCOS-2-87: سرور Windows SMB باید بسته SMB را در صورت امکان تایید کند.

شرح اجمالی:پروتکل SMB یک مبنا برای عملکرد شبکه فراهم میکند. امضای دیجیتال بسته های SMB به جلوگیری از حمله man-in-the-middle کمک میکند. اگر این سیاست فعال باشد، سرور SMB بسته SMB بر اساس درخواست کلاینت تایید میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Microsoft network server: Digitally sign communications (if client agrees)" to "Enabled".

SCOS-2-88: ورود خودکار باید غیرفعال باشد.

شرح اجمالی: اجازه دادن سیستم به ورود خودکار وقتی که ماشین بوت شده است میتواند به هر فرد بدون اعتباری دسترسی بدهد که کامپیوتر را مجددا راه بندازد. ورود خودکار با سطح دسترسی administrator میتواند به یک فرد بدون اعتبار دسترسی کامل بدهد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)" to "Disabled".

اطمینان از اینکه هیچ کلمه عبوری برا مقدار رجیستری "DefaultPassword" طبق اشاره ذیل ذخیره نشود:

Registry Hive: HKEY_LOCAL_MACHINE

Registry Path: \Software\Microsoft\Windows NT\CurrentVersion\Winlogon\

Value Name: DefaultPassword

(See "Updating the Windows Security Options File" in the STIG Overview document if MSS settings are not visible in the system's policy tools.)

SCOS-2-89 : سیستم باید به نحوی پیکربندی شود که از ذخیره سازی کلمه عبورها و گواهی نامه‌ها جلوگیری کند.

شرح اجمالی: این تنظیمات ذخیره سازی کلمه عبورها و گواهی نامه‌ها را بر روی سیستم محلی (local)کنترل میکند.

بعنوان نمونه گواهی نامه‌ها نباید برروی سیستم محلی ذخیره شود، چونکه موجب نفوذ به سیستم میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Do not allow storage of passwords and credentials for network authentication" to "Enabled".

SCOS-2-90 : سیستم باید به گونه ای پیکربندی شود که کاربران ناشناخته (anonymous)حقوق یکسان برای دسترسی به هر گروه را نداشته باشند.

شرح اجمالی: دسترسی های کاربران anonymous باید محدود شوند. اگر این تنظیمات فعال باشند کاربران anonymous میتوانند حقوق یکسان و مجوز دسترسی به گروه های سیستمی را داشته باشند.کاربران anonymous نباید این مجوز و حقوق را داشته باشند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Let everyone permissions apply to anonymous users" to "Disabled".

SCOS-2-91 : حالت تایید User Account Control برای سطح دسترسی های Administrator سیستمی باید فعال شود.

شرح اجمالی: User Account Control (UAC) یک مکانیزم امنیتی برای محدود کردن افزایش سطح دسترسی شامل حساب های کاربری با دسترسی administrative است، مگر اینکه مجاز باشد. این تنظیمات برای حساب های کاربری Administrator سیستمی پیکربندی میشوند بطوری که تحت حالت تایید Admin اجرا شوند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "User Account Control: Admin Approval Mode for the Built-in Administrator account" to "Enabled".

SCOS-2-92: User Account Control باید درخواست های کاربران عادی برای افزایش سطح دسترسی را رد کند.

شرح اجمالی: User Account Control (UAC) یک مکانیزم امنیتی برای محدود کردن افزایش سطح دسترسی شامل؛ حساب های کاربری با دسترسی administrative است ، مگر اینکه مجاز باشد و این تنظیمات افزایش دسترسی که توسط کاربران عادی درخواست شده است را کنترل میکند.

نحوه پیاده‌سازی: نیازمندیهای UAC برای نصب و راه اندازی هسته اصلی سرور NA است.

پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "User Account Control: Behavior of the elevation prompt for standard users" to "Automatically deny elevation requests".

SCOS-2-93 : User Account Control باید به نحوی پیکربندی شود که از نصب و راه اندازی برنامه ها و افزایش سریع سطح دسترسی جلوگیری کند.

شرح اجمالی: User Account Control (UAC) یک مکانیزم امنیتی برای محدود کردن افزایش سطح دسترسی شامل حساب های کاربری با دسترسی administrative است ، مگر اینکه مجاز باشد. این تنظیمات لازم میکند که ویندوز به درخواست های برنامه های نصب شده بر اساس اعتبار سنجی گواهی نامه برنامه پاسخ بدهد.

نحوه پیاده‌سازی: نیازمندیهای UAC برای نصب و راه اندازی هسته اصلی سرور NA است.

پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "User Account Control: Detect application installations and prompt for elevation" to "Enabled".

SCOS-2-94 : ویندوز باید سطح تمام برنامه های User Account Control را افزایش دهد نه اینکه تنها آنهایی را که تایید شده است.

شرح اجمالی: User Account Control (UAC) یک مکانیزم امنیتی برای محدود کردن افزایش سطح دسترسی شامل حساب های کاربری با دسترسی administrative است، مگر اینکه مجاز باشد. این تنظیمات پیکربندی میشوند که ویندوز سطح تمام برنامه ها را یا تنها آنهایی که تایید شده اند افزایش دهد.

نحوه پیاده‌سازی: نیازمندیهای UAC برای نصب و راه اندازی هسته اصلی سرور NA است.

پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "User Account Control: Only elevate executables that are signed and validated" to "Disabled".

SCOS-2-95 : User Account Control باید به یک میزکار (desktop) امن تغییر کند هنگامی که میخواهد دسترسی را افزایش دهد.

شرح اجمالی: User Account Control (UAC) یک مکانیزم امنیتی برای محدود کردن افزایش سطح دسترسی شامل حساب های کاربری با دسترسی administrative است، مگر اینکه مجاز باشد. این تنظیمات از افزایش سطح دسترسی تنها در یک میزکار (desktop) امن استفاده شود، اطیمنان حاصل میکند.

نحوه پیاده‌سازی: نیازمندیهای UAC برای نصب و راه اندازی هسته اصلی سرور NA است.

پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "User Account Control: Switch to the secure desktop when prompting for elevation" to "Enabled".

SCOS-2-96: User Account Control باید نوشتن ناموفق برروی رجیستری و فایلها را بر حسب موقعیت هرکاربر مجازی سازی کند.

شرح اجمالی: User Account Control (UAC) یک مکانیزم امنیتی برای محدود کردن افزایش سطح دسترسی شامل حساب های کاربری با دسترسی administrative است، مگر اینکه مجاز باشد. این تنظیمات برنامه های غیرمنطبق با UAC را به اجرا در فایلهای مجازی شده و ورودی های هر رجیستر در موقعیت مکانی هر کاربر پیکربندی میشود. به آنها اجازه داده میشود که اجرا شوند.

نحوه پیاده‌سازی: نیازمندیهای UAC برای نصب Server Core، NA است.

پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options -> "User Account Control: Virtualize file and registry write failures to per-user locations" to "Enabled".

SCOS-2-97 : سرویس FTP مایکروسافت نباید نصب شده باشد.

شرح اجمالی: سرویسهای غیرضروری سطح حمله به سیستم را افزایش میدهند. برخی از این سرویس ها ممکن است سطوح لازم برای احراز هویت یا رمزنگاری را پشتیبانی نکنند.

نحوه پیاده‌سازی: پاک کردن یا غیرفعال نمودن سرویس FTP مایروسافت (msftpsvc).

SCOS-2-98: سرویس Peer Networking Identity Manager اگر نصب است باید غیرفعال شود.

شرح اجمالی: سرویسهای غیرضروری سطح حمله به سیستم را افزایش میدهند. برخی از این سرویس ها ممکن است سطوح لازم برای احراز هویت یا رمزنگاری را پشتیبانی نکنند.

نحوه پیاده‌سازی: پاک یا غیرفعال کردن سرویس Peer Networking Identity Manager (p2pimsvc)

SCOS-2-99 : محافظ صفحه نمایش باید در سیستم فعال باشند.

شرح اجمالی: سیستم های محافظت نشده مستعد استفاده های بدون اعتبار و مجوز هستند و وقتیکه بدون محافظ هستند باید قفل شوند. فعال کردن کلمه عبور برای محافظ صفحه نمایش با گرفتن یک زمان مشخص به محافظت از اعتبارنامه و داده های حساس دربرابر افشا شدن برای پرسنل غیرمجاز با دسترسی فیزیکی به کامپیوترکمک میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Control Panel -> Personalization -> "Enable screen saver" to "Enabled".

SCOS-2-100 : محافظ صفحه نمایش باید از کلمه عبور محافظت کند.

شرح اجمالی: سیستم های محافظت نشده مستعد استفاده های بدون اعتبار و مجوز هستند و وقتیکه بدون محافظ هستند باید قفل شوند. فعال کردن کلمه عبور برای محافظ صفحه نمایش با گرفتن یک زمان مشخص به

محافظت از اعتبارنامه و داده های حساس دربرابر افشا شدن برای پرسنل غیرمجاز با دسترسی فیزیکی به کامپیوترکمک میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> Control Panel -> Personalization -> "Enable screen saver" to "Enabled".

SCOS-2-101 : Windows Help Experience Improvement Program باید غیرفعال باشد.

شرح اجمالی: برخی از ویژگی ها میتوانند با ارائه کننده خدمات، برای ارسال کردن اطلاعات سیستم یا دانلود کردن اطلاعات یا اجزاء سازنده برای ویژگی ها ارتباط برقرار کنند. غیرفعال کردن این قابلیت میتواند از درز کردن اطلاعات حساس به خارج از سازمان و همچنین بروزرسانی های کنترل نشده برای سیستم جلوگیری کند.

این تنظیمات اطمینان حاصل میکند از اینکه Windows Help Experience Improvement Program

غیرفعال است بنابراین اطلاعات به سازنده یا ارائه کننده خدمت نمیرسند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Internet Communication Management -> Internet Communication Settings -> "Turn off Help Experience Improvement Program" to "Enabled".

SCOS-2-102: Windows Help Ratings feedback باید خاموش باشد.

شرح اجمالی: برخی از ویژگی ها میتوانند با ارائه کننده خدمات، برای ارسال کردن اطلاعات سیستم یا دانلود کردن اطلاعات یا اجزاء سازنده برای ویژگی ها ارتباط برقرار کنند. غیرفعال کردن این قابلیت میتواند از نشت اطلاعات حساس به خارج از سازمان و همچنین بروزرسانی های کنترل نشده برای سیستم جلوگیری کند.

این تنظیمات اطمینان حاصل میکند از اینکه کاربران نتوانند برای بررسی محتوا ratings feedback به Microsoft ارائه دهند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Administrative Templates -> System -> Internet Communication Management -> Internet Communication Settings -> "Turn off Help Ratings" to "Enabled".

SCOS-2-103 : ویژگی Access Credential Manager as a trusted caller user right برای حسابهای کاربری غیرمجاز (بدون اعتبار) نباید وجود داشته باشد.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حساب های کاربری با پالیسی کاربر"Access Credential Manager as a trusted caller" ممکن است توانایی بازیابی اعتبارنامه ها از حسابهای کاربری مدیر اعتبارنامه را دارد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Access Credential Manager as a trusted caller" to be defined but containing no entries (blank).

SCOS-2-104: نباید ویژگی Access this computer from the network user right برای حسابهای کاربری غیرمجاز سرورهای عضو دامنه وجود داشته باشد.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حساب های کاربری با پالیسی "Access this computer from the network" ممکن است برروی سیستم دسترسی به منابع داشته باشند، و باید براساس نیاز آنها را محدود کرد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Access this computer from the network" to only include the following accounts or groups:

Administrators

Authenticated Users

سیستم های اختصاص داده شده به مدیریت اکتیو دایرکتوری، تنها باید به افراد با دسترسی Administrators اجازه حذف گروه های معتبر را بدهد.

SCOS-2-105: نباید پالیسی Adjust memory quotas for a process برای حساب های کاربری غیرمجاز وجود داشته باشد.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با "Adjust memory quotas for a process" میتوانند حافظه (memory)ای که برای پردازش در دسترس میباشد را تنظیم کند(تغییر دهند) و همین میتواند برای حمله DOS استفاده شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings ->

Security Settings -> Local Policies -> User Rights Assignment -> "Adjust memory quotas for a process" to only include the following accounts or groups:

Administrators

Local Service

Network Service

SCOS-2-106: نباید ویژگی Allow log on locally برای کاربران غیرمجاز وجود داشته باشد.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با پالیسی "Allow log on locally" میتوانند ورود تعاملی به سیستم داشته باشند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Allow log on locally" to only include the following accounts or groups:

Administrators

SCOS-2-107 : نباید ویژگی Allow log on through Remote Desktop برای حسابهای کاربری غیرمعتبر وجود داشته باشد.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با داشتن پالیسی "Allow log on through Remote Desktop Services" میتوانند به سیستم از راه دور دسترسی داشته باشند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Allow log on through Remote Desktop Services" to only include the following accounts or groups:

Administrators

SCOS-2-108: حساب های کاربری بدون اعتبار نباید پالیسی Back up files and directories را داشته باشند.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با داشتن حق "Back up files and directories" میتوانند فایل ها و دایرکتوری ها را دور بزنند و به اطلاعات حساس دسترسی داشته باشند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Back up files and directories" to only include the following accounts or groups:

Administrators

SCOS-2-109 : حساب های کاربری بدون اعتبار نباید پالیسی Change the system time را داشته باشند.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با داشتن حق "Change the system time" میتوانند زمان سیستم را عوض کنند، و میتواند بر احراز هویت تاثیر گذارد و همچنین میتواند بر زمان لاگ انداختن سیستم موثر باشد و آنرا تغییر دهد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Change the system time" to only include the following accounts or groups:

Administrators

Local Service

SCOS-2-110 : حساب های کاربری بدون اعتبار نباید حق (ویژگی) Create a pagefile را داشته باشند.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با داشتن حق "Create a pagefile" میتوانند اندازه pagefile را تغییر دهند که میتواند بر کارایی سیستم تاثیر گذارند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Create a pagefile" to only include the following accounts or groups:

Administrators

SCOS-2-111: حساب های کاربری بدون اعتبار نباید حق(ویژگی) Create global object را داشته باشند.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با داشتن حق "Create global objects" میتوانند یک شی ایجاد کنند که برای همه ی نشست (session) ها در دسترس است که میتواند فرایند هایی که در sessionهای دیگر هست را تحت تاثیر قرار دهد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Create global objects" to only include the following accounts or groups:

Administrators

Service

Local Service

Network Service

SCOS-2-112 : حساب های کاربری بدون اعتبار نباید حق (ویژگی) Create permanent shared objects را داشته باشد.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با داشتن حق"Create permanent shared objects" میتوانند داده های حساس را به وسیله اشیاء اشتراک گذاری شده فاش کند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Create permanent shared objects" to be defined but containing no entries (blank).

SCOS-2-113 : حساب های کاربری بدون اعتبار نباید ویژگی Create symbolic linksرا داشته باشند.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با داشتن ویژگی "Create symbolic links" میتوانند یک اشاره گر به اشیاء دیگر ایجاد کند که میتواند سیستم را در معرض حمله قرار دهد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Create symbolic links" to only include the following accounts or groups:

Administrators

SCOS-2-114 : ویژگی Deny log on as a batch job باید روی اعضای سرور تنظیم شود تا از دسترسی حسابهای کاربری عضو دامنه با سطح بالا روی سیستم های دامنه جلوگیری شود.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند. ویژگی "Deny log on as a batch job" حسابهای کاربری که از ورود به سیستم بعنوان

batch jobها ، مانند Task Scheduler جلوگیری میکند را معرفی میکند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Deny log on as a batch job" to include the following:

Domain Systems Only:

Enterprise Admins Group

Domain Admins Group

SCOS-2-115: SCOS-2-114 : ویژگی Deny log on as a batch job باید روی اعضای سرور تنظیم شود تا از دسترسی حسابهای کاربری عضو دامنه با سطح بالا روی سیستم های دامنه جلوگیری شود. و هیچ گروه یا حساب کاربری دیگری نباید این حقوق را داشته باشد.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند. ویژگی "Deny log on as a service" حسابهای کاربری که از ورود به یک سرویس جلوگیری میکند را معرفی میکند.

پیکربندی نادرست میتواند سرویس را از شروع به کار بازدارد و در نتیجه به یک حمله DOS منجر شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Deny log on as a service" to include the following for domain-joined systems:

Enterprise Admins Group

Domain Admins Group

پیکربندی "Deny log on as a service" برای سیستم هایی که عضو دامنه نمیباشند هیچ مقداری ندارد.

SCOS-2-116: ویژگی Deny log on locally user برای کاربران محلی موجود روی سرورهای عضو دامنه باید به نحوی پیکربندی شوند که از دسترسی به حسابهای کاربری بسیار ویژه عضو دامنه برروی سیستم های عضو دامنه و همچنین از دسترسی بدون اعتبار به کل سیستم جلوگیری شود.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند. ویژگی "Deny log on locally" حسابهای کاربری که از ورود تعاملی به سیستم جلوگیری میکنند را معرفی میکند.

گروه مهمان برای جلوگیری از دسترسی های غیرمجاز مشخص شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Deny log on locally" to include the following:

Domain Systems Only:

Enterprise Admins Group

Domain Admins Group

Systems dedicated to the management of Active Directory are exempt from this.

All Systems:

Guests Group

SCOS-2-117 : حساب های کاربری غیرمجاز نباید اجازه فعال کردن کامپیوتر و حساب های کاربری تایید شده را بر روی سرورهای عضو دامنه داشته باشند.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

وجود حق "Enable computer and user accounts to be trusted for delegation" اجازه میدهد که تنظیمات "Trusted for Delegation" تغییر یابد. این میتواند به کاربران غیر معتبر اجازه دهد که هویت دیگر کاربران را جعل کنند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Enable computer and user accounts to be trusted for delegation" to be defined but containing no entries (blank).

SCOS-2-118 : حساب های کاربری غیرمجاز نباید ویژگی (Force shutdown from a remote) را داشته باشند.

شرح اجمالی: اعطای نامناسب حقوق به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

پالیسی "Force shutdown from a remote system" برای حسابهای کاربری این اجازه را به آنها میدهد که سیستم را از راه دور خاموش کنند و همین زمینه ساز حمله DOS میشود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Force shutdown from a remote system" to only include the following accounts or groups:

Administrators

SCOS-2-119 : حساب های کاربری غیرمجاز نباید ویژگی Generate security audits را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

پالیسی "Generate security audits" میتواند به کاربران مشخص شده توانایی ایجاد سوابق Audit(ممیزی) کردن لاگ ها را بدهد. که فقط باید حسابهای سرویس سیستم(system service) تعریف شده باشند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Generate security audits" to only include the following accounts or groups:

Local Service

Network Service

SCOS-2-120 : حساب های کاربری غیر مجاز نباید توانایی Impersonate a client after authentication را داشته باشند.(نتوانند هویت کاربران را بعد احراز هویت جعل کنند)

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

ویژگی "Impersonate a client after authentication" اجازه میدهد که یک برنامه به جعل هویت دیگر کاربران و حسابهای کاربری برای اجرای عملیات از طرف آنها بپردازد و یک attacker میتواند با استفاده از همین موضوع سطح دستری خود را افزایش دهد.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Impersonate a client after authentication" to only include the following accounts or groups:

Administrators

Service

SCOS-2-121 : حساب های کاربری غیر مجاز نباید پالیسی Increase a process working set را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حساب کاربری با داشتن ویژگی "Increase a process working set" میتواند اندازه روند فرآیند کار را تغییر دهد و بطور بالقوه باعث مسائل مربوط به عملکرد یا حمله DOS شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Increase a process working set" to only include the following accounts or groups:

Administrators

Local Service

Window Manager\Window Manager Group

SCOS-2-122 : ویژگی "Increase scheduling priority" برای حساب های کاربری غیر مجاز نباید فعال باشد.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حساب کاربری با داشتن ویژگی "Increase scheduling priority" میتواند (scheduling priority)اولویت زمانبندی را تغییر دهد که باعث مسائل مربوط به عملکرد یا حمله DOS شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Increase scheduling priority" to only include the following accounts or groups:

Administrators

SCOS-2-123 : حساب های کاربری غیر مجاز نباید پالیسی Load and unload device drivers داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

ویژگی "Load and unload device drivers" اجازه میدهد که درایورهای دستگاه بصورت پویا توسط کاربر برروی سیستم بارگذاری شوند. این توانایی میتواند بصورت بالقوه برای نصب کدهای مخرب توسط حمله کننده(attacker) استفاده شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Load and unload device drivers" to only include the following accounts or groups:

Administrators

SCOS-2-124 : حساب های کاربری غیر مجاز نباید پالیسی Lock pages in memory را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

ویژگی "Lock pages in memory" میتواند اجازه دهد که حافظه فیزیکی به یک فرآیندهای اختصاص داده شود، که میتواند باعث مسائل مربوط به عملکرد و حمله DOS شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Lock pages in memory" to be defined but containing no entries (blank).

SCOS-2-125 : حساب های کاربری غیر مجاز نباید پالیسی Log on as a batch job را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

ویژگی "Log on as a batch job" اجازه میدهد که کاربران با استفاده از زمانبندی وظیفه وارد سیستم شوند که باید این محدود شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Log on as a batch job" to only include the following accounts or groups:

Administrators

SCOS-2-126 : ویژگی Manage auditing and security log برای حساب های کاربری غیر مجاز نباید فعال باشد.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری با پالیسی "Manage auditing and security log" میتوانند ورودهای امنیتی را مدیریت کنند و در پیکربندی auditing(بررسی لاگ ها) تغییر ایجاد کنند. این ویژگی میتواند برای پاک کردن شواهد دستکاری و تغییر داده استفاده شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Manage auditing and security log" to only include the following accounts or groups:

Administrators

SCOS-2-127 : حساب های کاربری غیر مجاز نباید پالیسی Modify an object label را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حساب های کاربری با داشتن ویژگی "Modify an object label" میتواند برچسب یکپارچگی یک شی را تغییر دهد. این میتواند برای اجرای کد در سطح دسترسی های بالاتر استفاده شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Modify an object label" to

be defined but containing no entries (blank).

SCOS-2-128 : حساب های کاربری غیر مجاز نباید پالیسی Modify firmware environment values را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حساب های کاربری که ویژگی "Modify firmware environment values" برای آنها فعال است میتوانند سخت افزار پیکربندی متغیرهای محیطی را تغییر دهند این میتواند باعث از بین رفتن سخت افزار و حمله DOS شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Modify firmware environment values" to only include the following accounts or groups:

Administrators

SCOS-2-129 : نباید پالیسی Perform volume maintenance tasks برای حساب های کاربری غیر مجاز فعال باشد.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری که ویژگی "Perform volume maintenance tasks" برای آنها فعال است میتوانند حجم و پیکربندی دیسک را مدیریت کنند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Perform volume maintenance tasks" to only include the following accounts or groups:

Administrators

SCOS-2-130 : حساب های کاربری غیر مجاز نباید پالیسی Profile single process را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری که دارای ویژگی "Profile single process" هستند میتوانند فرآیندهای غیرسیستمی را مانیتور کنند. و حمله کننده (attacker) میتواند از شناسایی این فرآیندها برای حمله استفاده کند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Profile single process" to only include the following accounts or groups:

Administrators

SCOS-2-131 : حساب های کاربری غیر مجاز نباید پالیسی Profile system performance را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری که دارای پالیسی "Profile system performance"هستند میتوانند فرآیندهای غیرسیستمی را مانیتور کنند. و حمله کننده (attacker) میتواند از شناسایی این فرآیندها برای حمله استفاده کند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Profile system performance" to only include the following accounts or groups:

Administrators

NT Service\WdiServiceHost

SCOS-2-132 : حساب های کاربری غیر مجاز نباید پالیسی Replace a process level token را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

ویژگی "Replace a process level token" اجازه میدهد یک فرآیند یا سرویس دیگر فرآیند یا سرویس ها را با token دسترسی امنیتی متفاوت شروع کند، یک کاربر با این توانایی میتواند دیگر حساب های کاربری را جعل هویت کند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Replace a process level token" to only include the following accounts or groups:

Local Service

Network Service

SCOS-2-133 : حساب های کاربری غیر مجاز نباید پالیسی Restore files and directories را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری که دارای پالیسی "Restore files and directories " هستند میتوانند فایل ها و دایرکتوری ها را دور بزنند و به اطلاعات حساس دسترسی داشته باشند. این میتواند برای بازنویسی داده های فعلی استفاده شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Restore files and directories" to only include the following accounts or groups:

Administrators

SCOS-2-134 : حساب های کاربری غیر مجاز نباید پالیسی Shut down the system را داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری که دارای پالیسی "Shut down the system" هستند میتوانند بصورت تعاملی سیستم را خاموش کنند و این میتواند منجر به حمله DOS شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment ->

"Shut down the system" to only include the following accounts or groups:

Administrators

SCOS-2-135 : حساب های کاربری غیر مجاز نباید پالیسی Take ownership of files or other objectsرا داشته باشند.

شرح اجمالی: اعطای نامناسب پالیسی به کاربران میتواند دسترسی سیستمی،administrative، و دیگر توانایی های سطح بالا برای آنها فراهم کند.

حسابهای کاربری که دارای پالیسی "Take ownership of files or other objects" هستند، میتوانند مالکیت اشیا را بگیرند و آنها را تغییر دهند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> "Take ownership of files or other objects" to only include the following accounts or groups:

Administrators.
