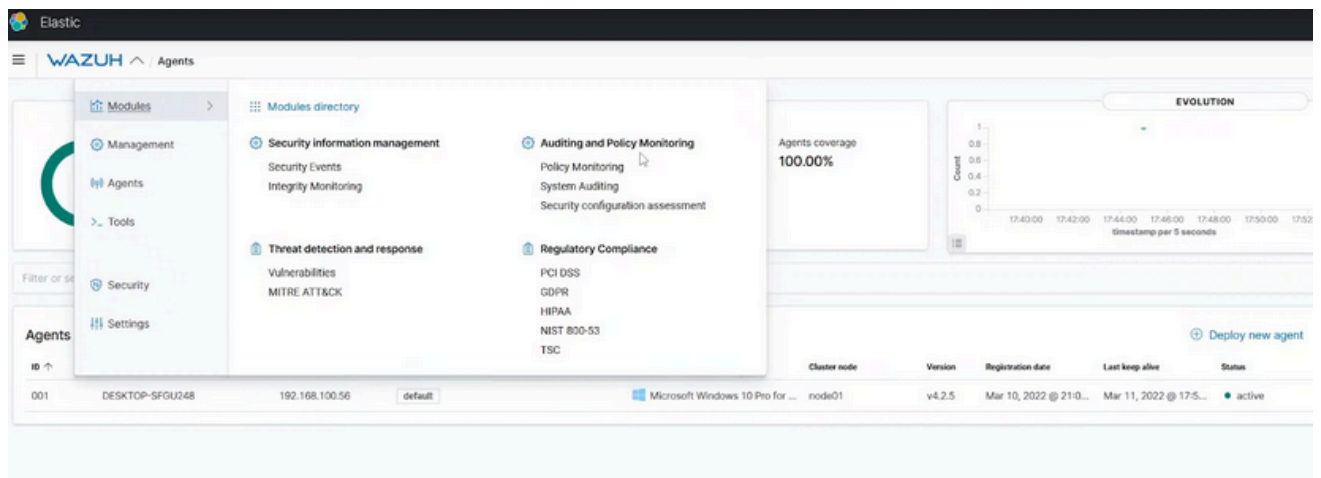
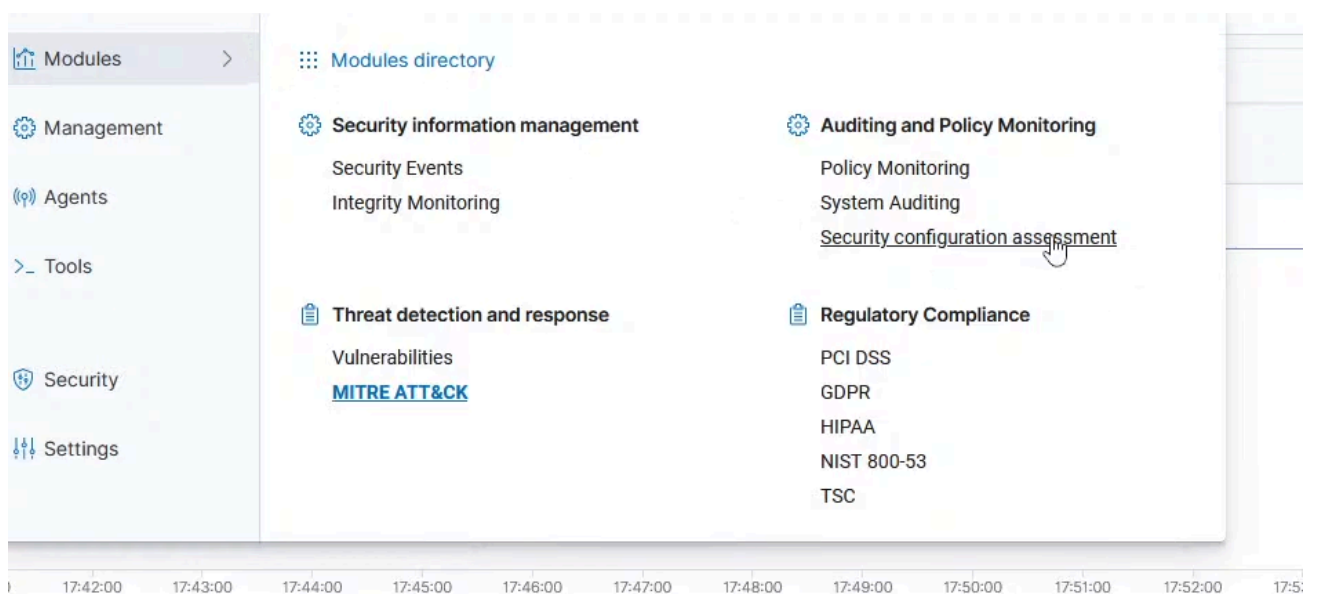


Para empezar, nos vamos a **modules, Security Events**.



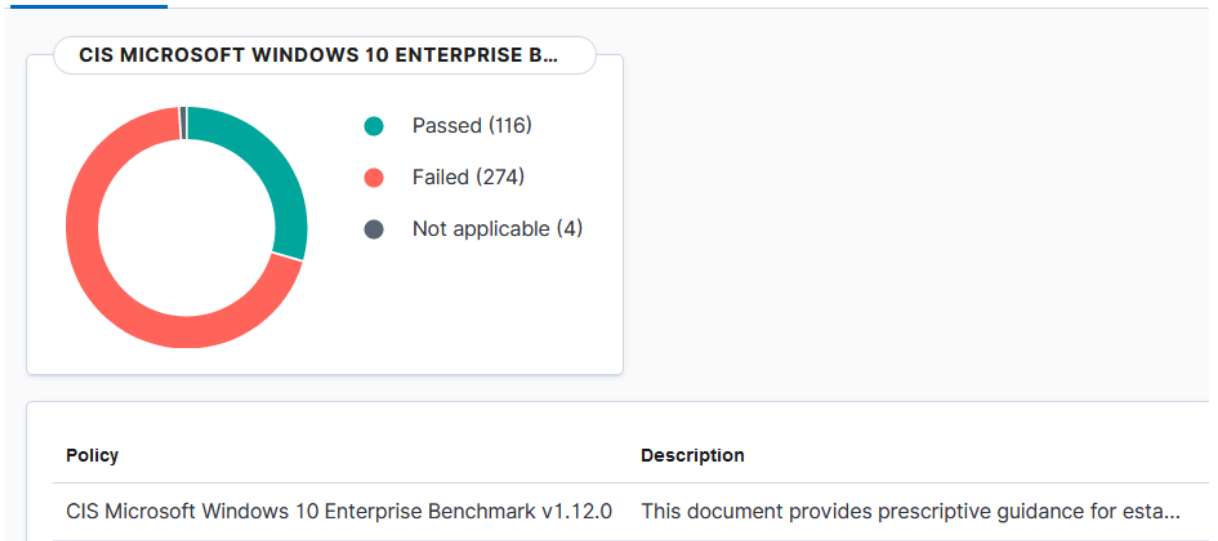
Por otro lado también tenemos:



Aquí es donde viene lo interesante:

Inventory

Events



<

CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0

Passed

116

Failed

274

Not applicable

4

Score

29%

End s

Apr 11, 2024 @

Checks (394)

Refresh

Search			
ID ↑	Title	Target	Result
15500	Ensure 'Enforce password history' is set to '24 or more password(s)'.	Command: net.exe accounts	Failed
15501	Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'.	Command: net.exe accounts	Failed
15502	Ensure 'Minimum password age' is set to '1 or more day(s)'.	Command: net.exe accounts	Failed
15503	Ensure 'Minimum password length' is set to '14 or more character(s)'.	Command: net.exe accounts	Failed
15505	Ensure 'Relax minimum password length limits' is set to 'Enabled'.	Registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SAM	Failed
15506	Ensure 'Account lockout duration' is set to '15 or more minute(s)'.	Command: net.exe accounts	Failed
15507	Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'.	Command: net.exe accounts	Failed
15508	Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'.	Command: net.exe accounts	Failed

Activar Windows

En el primero, 15500, tenemos que:

Rationale

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Remediation

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies>Password Policy\Enforce password history

Description

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: 24 or more password(s). Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center. Note #2: As of the publication of this benchmark, Microsoft currently has a maximum limit of 24 saved passwords. For more information, please visit [Enforce password history \(Windows 10\) - Windows security | Microsoft Docs](#)

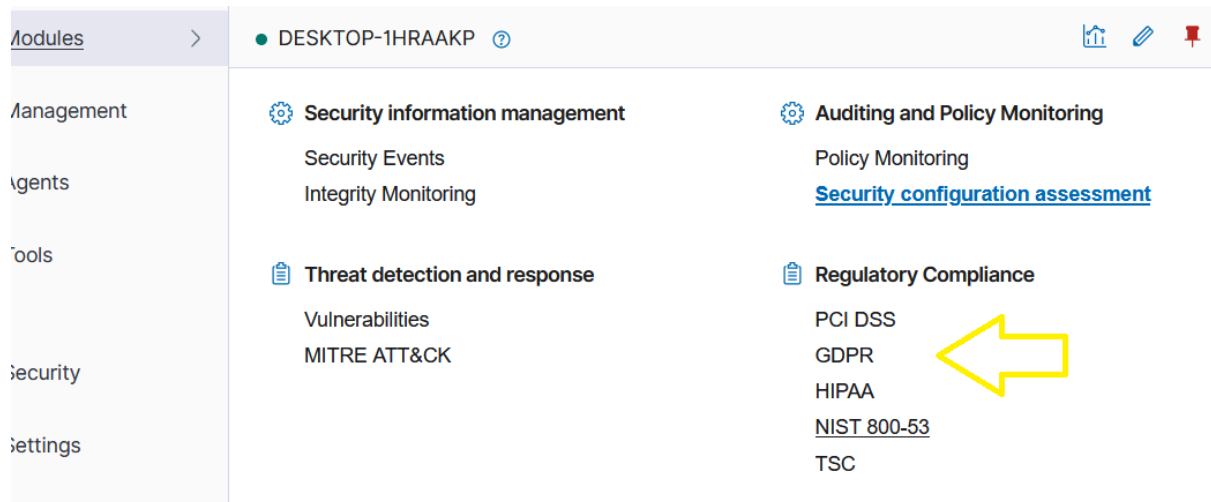
Check (Condition: all)

- c:\net.exe accounts → n:Length of password history maintained:\s+(\d+) compare >= 24

Debes asegurarte de establecer esta configuración en al menos 24 contraseñas para mantener la efectividad de la política de contraseñas y reducir el riesgo de que los usuarios reutilicen contraseñas antiguas.

Es importante tener en cuenta que estas configuraciones de políticas de contraseñas deben aplicarse adecuadamente en todo el dominio para que tengan efecto en todas las cuentas de usuario. Además, se recomienda usar la configuración de "Minimum password age" (Edad mínima de la contraseña) para evitar que los usuarios cambien repetidamente sus contraseñas hasta que puedan reutilizar su contraseña original.

En la parte de "Regulatory Compliance", qué significa PCI DSS, GDPR, HIPAA, NIST 600-53, TSC?



Estas son regulaciones o estándares de cumplimiento que se utilizan en el ámbito de la seguridad de la información y la privacidad de los datos:

1. **PCI DSS:** Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago). Es un conjunto de estándares de seguridad diseñados para garantizar que todas las empresas que aceptan, procesan, almacenan o transmiten información de tarjetas de crédito mantengan un entorno seguro de procesamiento de pagos.
2. **GDPR:** General Data Protection Regulation (Reglamento General de Protección de Datos). Es una regulación de la Unión Europea que establece las normas para la protección de datos personales y la privacidad de los individuos dentro de la Unión Europea y el Espacio Económico Europeo.
3. **HIPAA:** Health Insurance Portability and Accountability Act (Ley de Portabilidad y Responsabilidad del Seguro de Salud). Es una ley de Estados Unidos que establece estándares para la protección y seguridad de la información de salud electrónica.
4. **NIST 800-53:** National Institute of Standards and Technology Special Publication 800-53. Es un estándar del gobierno de Estados Unidos que proporciona directrices y controles de seguridad para sistemas de información federales y no federales.

5. **TSC:** Threat Stack Cloud Security. No es una regulación en sí misma, sino más bien una plataforma de seguridad en la nube que ayuda a las organizaciones a cumplir con diversas regulaciones y estándares de seguridad, como PCI DSS, GDPR y HIPAA, al proporcionar herramientas y controles de seguridad en la nube.

Estas regulaciones y estándares son importantes para diversas industrias y organizaciones, ya que establecen requisitos y prácticas de seguridad que ayudan a proteger la información confidencial y a garantizar la privacidad de los datos de los clientes y usuarios. Las organizaciones suelen estar obligadas a cumplir con estas regulaciones según su tipo de negocio y la naturaleza de los datos que manejan.

Ejemplo. Las gráficas de cumplimiento de regulaciones como HIPAA en Wazuh están estructuradas de acuerdo con las secciones y subsecciones de la regulación. Cada código como "164.312.b" o "164.312.a.2.I" se refiere a una sección o subsección específica de la regulación HIPAA.

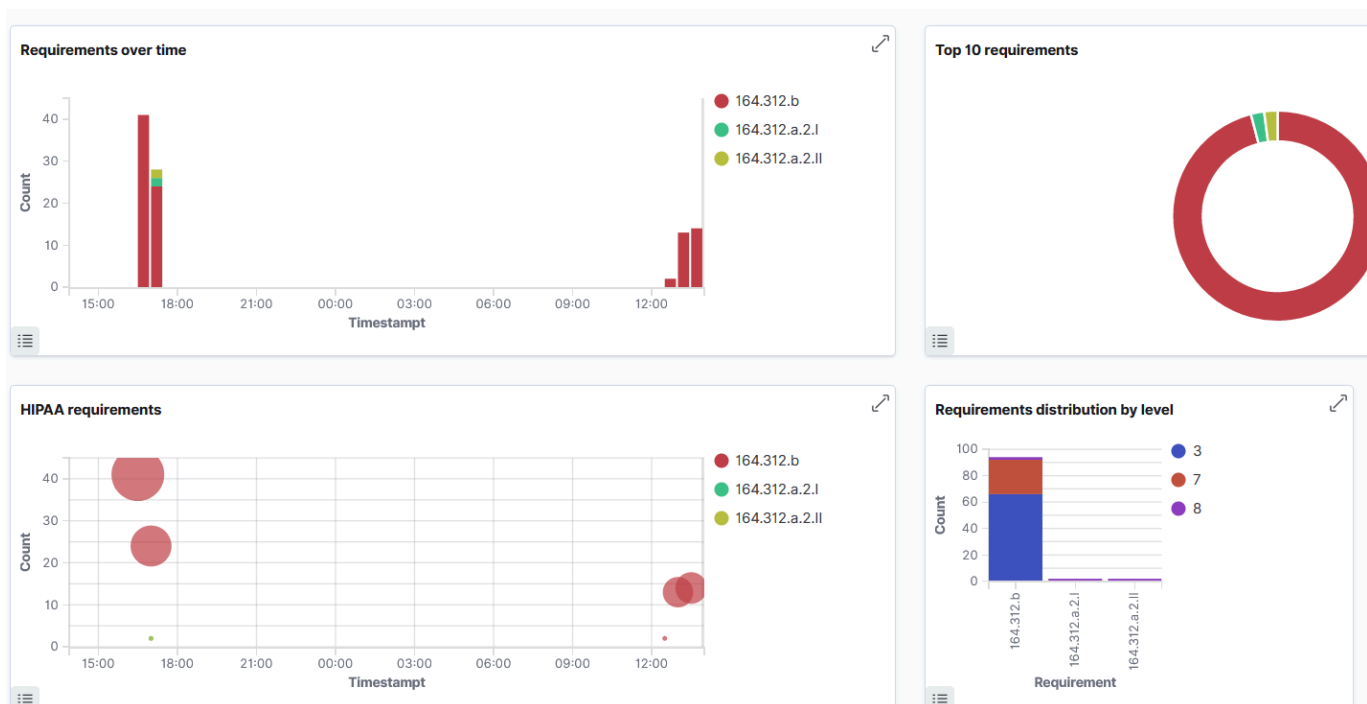
Para entender qué significan estos códigos y cómo se relacionan con HIPAA, es útil desglosarlos:

1. **Número de la sección principal:** En el ejemplo "164", este es el número de la sección principal de la regulación. En el caso de HIPAA, cada número principal se refiere a un área temática general, como seguridad de la información, privacidad de la información médica, entre otros.
2. **Subsecciones:** Los números y letras después del número principal representan las subsecciones o párrafos dentro de esa sección principal. Por ejemplo, "164.312.b" se refiere a la subsección "b" dentro de la sección "164.312".
3. **Detalles específicos:** Dentro de cada subsección, puede haber sub-subsecciones o requisitos específicos detallados con letras y números adicionales. Por ejemplo, en "164.312.a.2.I", "a" podría ser una subsección, "2" podría ser un sub-subsección, y "I" podría representar un requisito específico dentro de esa sub-subsección.

Para leer estas gráficas y comprender qué significan, puedes seguir estos pasos:

1. **Identifica la sección principal:** Encuentra el número principal y comprende el área temática general que abarca.
2. **Analiza las subsecciones:** Lee las subsecciones para comprender los requisitos específicos dentro de esa área temática.

3. **Examina los detalles específicos:** Si hay sub-subsecciones o requisitos detallados adicionales, analiza qué significan y cómo se aplican a las prácticas de seguridad de la información de tu organización.
4. **Evalúa el cumplimiento:** Utiliza esta información para evaluar el cumplimiento de tu organización con los requisitos específicos de HIPAA y para identificar áreas en las que puedas necesitar mejorar tu seguridad de la información y prácticas de privacidad de datos.



Los códigos como "2.2", "2.2.5", "10.2.5", "4.1" y "10.6.1" en el apartado "Top 5 PCI DSS requirements" de Wazuh se refieren a requisitos específicos dentro del estándar PCI DSS (Payment Card Industry Data Security Standard). Estos códigos representan secciones y subsecciones de la norma, y cada uno aborda un aspecto particular de la seguridad de la información y la protección de datos de tarjetas de pago. Aquí tienes una explicación de cada uno:

1. ****2.2**:** Este código se refiere a la sección 2, subsección 2 de PCI DSS. La sección 2 se centra en la implementación de configuraciones seguras para sistemas y aplicaciones. El requisito específico 2.2 puede abordar aspectos como la configuración segura de los sistemas, la eliminación de configuraciones inseguras por defecto, y la protección de las configuraciones críticas.

2. ****2.2.5****: Este código es una sub-subsección del requisito 2.2. Se refiere a un detalle específico dentro del requisito 2.2, que podría estar relacionado con la gestión de contraseñas, el control de acceso o la configuración segura de sistemas y aplicaciones.

3. ****10.2.5****: Este código se refiere al requisito 10.2.5 de PCI DSS. La sección 10 se centra en el monitoreo y seguimiento de acceso a los recursos de la red y datos de los titulares de tarjetas. El requisito 10.2.5 puede abordar la implementación de sistemas de registro y seguimiento para monitorear el acceso a los datos sensibles.

4. ****4.1****: Este código se refiere al requisito 4.1 de PCI DSS. La sección 4 se centra en el cifrado de los datos de tarjetas de pago en tránsito y en reposo. El requisito 4.1 puede abordar la implementación de cifrado para proteger los datos de tarjetas de pago mientras se transmiten a través de redes o se almacenan en sistemas de almacenamiento.

5. ****10.6.1****: Este código se refiere al requisito 10.6.1 de PCI DSS. Este requisito puede estar relacionado con la implementación de sistemas de registro de auditoría para registrar y monitorear las actividades relacionadas con los sistemas de tarjetas de pago y los datos sensibles.

En resumen, cada uno de estos códigos representa un requisito específico dentro del estándar PCI DSS y aborda aspectos clave de la seguridad de la información y la protección de datos de tarjetas de pago. Cumplir con estos requisitos es fundamental para garantizar la seguridad de los datos de tarjetas de pago y cumplir con las regulaciones de la industria de pagos.

El aviso **"rule.pci_dss: Descending"** en el contexto de Wazuh se refiere a una regla de seguridad asociada con el estándar PCI DSS (Payment Card Industry Data Security Standard). Cuando ves este aviso, indica que se ha activado una regla de seguridad específica que está diseñada para cumplir con un requisito o control establecido por PCI DSS.

El término "Descending" en este contexto generalmente significa que la regla se ha activado debido a una situación que está disminuyendo o deteriorando la seguridad en el entorno. En otras palabras, indica que la actividad o el evento detectado representan un riesgo potencial para la seguridad de los datos de tarjetas de pago y la privacidad de los clientes.

Por ejemplo, esta regla podría activarse en respuesta a actividades como:

1. Intentos de acceso no autorizados a sistemas o datos de tarjetas de pago.
2. Detección de tráfico de red no cifrado que involucra datos de tarjetas de pago.
3. Fallos en la autenticación o autorización que podrían permitir el acceso no autorizado a sistemas o datos sensibles.

Cuando ves este aviso en los registros de eventos de Wazuh, es importante investigar y tomar medidas para abordar la situación que lo activó. Esto puede incluir la corrección de vulnerabilidades, la mejora de la configuración de seguridad y la implementación de controles adicionales para proteger los datos de tarjetas de pago y cumplir con los requisitos de PCI DSS.

La norma NIST 800-53, desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, es un marco de seguridad ampliamente reconocido y utilizado para el gobierno federal de los EE. UU. Esta norma, titulada "Security and Privacy Controls for Federal Information Systems and Organizations" (Controles de Seguridad y Privacidad para Sistemas de Información y Organizaciones Federales), proporciona un conjunto exhaustivo de controles de seguridad y pautas para la protección de la información y los sistemas de información.

La NIST 800-53 establece un enfoque basado en el riesgo para la gestión de la seguridad de la información, lo que significa que las organizaciones pueden adaptar sus prácticas de seguridad para abordar los riesgos específicos que enfrentan. Este marco es utilizado no solo por las agencias federales de los EE. UU., sino también por organizaciones del sector privado y entidades gubernamentales en todo el mundo como una guía para el desarrollo de políticas y la implementación de controles de seguridad efectivos.

La norma NIST 800-53 se organiza en varias secciones, cada una de las cuales aborda un aspecto particular de la seguridad de la información. Estas secciones incluyen controles relacionados con la gestión de riesgos, la protección de datos, la autenticación, el control de acceso, la auditoría y el monitoreo, entre otros aspectos.

En resumen, la norma NIST 800-53 es un marco de seguridad integral que proporciona orientación detallada y práctica para ayudar a las organizaciones a proteger sus sistemas de información y datos contra amenazas y riesgos. Su enfoque basado en el riesgo y su

amplia adopción la convierten en un estándar importante en el campo de la seguridad de la información.

Un **"dashboard"** es una interfaz gráfica que proporciona una visualización consolidada de datos, métricas y estadísticas relevantes para un sistema, proceso o conjunto de actividades específicas. En el contexto de Wazuh, un dashboard puede ser una herramienta que muestra información clave relacionada con la seguridad de la información y la protección de activos en tiempo real.

Crear un dashboard en Wazuh permite:

1. **Monitorizar la seguridad:** Un dashboard centraliza información sobre eventos de seguridad, alertas, tendencias y métricas importantes. Esto proporciona a los administradores y analistas una visión general de la postura de seguridad de la organización y les ayuda a identificar y responder rápidamente a posibles amenazas y vulnerabilidades.
2. **Visualizar datos de forma efectiva:** Los dashboards de Wazuh suelen presentar datos de seguridad de una manera visualmente atractiva y fácil de entender, utilizando gráficos, tablas y diagramas. Esto facilita la interpretación de la información y permite a los usuarios identificar patrones, anomalías y áreas de interés con rapidez.
3. **Tomar decisiones informadas:** Al proporcionar acceso rápido a datos relevantes y actualizados sobre la seguridad, los dashboards de Wazuh permiten a los equipos de seguridad tomar decisiones informadas y estratégicas. Los administradores pueden utilizar esta información para priorizar tareas, asignar recursos y mejorar continuamente las defensas de seguridad de la organización.
4. **Comunicar el estado de seguridad:** Los dashboards también pueden ser útiles para comunicar el estado de seguridad de la organización a partes interesadas internas y externas, como la alta dirección, los equipos de TI y los auditores. Al proporcionar una visualización clara y concisa de los datos de seguridad, los dashboards ayudan a mejorar la transparencia y la comunicación en torno a las iniciativas de seguridad.

En resumen, crear un dashboard en Wazuh es una forma efectiva de consolidar y visualizar información clave relacionada con la seguridad de la información, lo que ayuda a los

equipos de seguridad a monitorear, analizar y responder a las amenazas de manera proactiva y eficiente.

Mejoras:

15506 Failed

Ensure 'Account lockout duration' is set to **Command:** net.exe
'15 or more minute(s)'. accounts

Rationale

Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

Remediation

To establish the recommended configuration via GP, set the following UI path to 5 or fewer invalid login attempt(s), but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold

Description

This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform to the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 5 or fewer invalid logon attempt(s), but not 0. Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Checks (Condition: all)

- c:\net.exe accounts -> n:Lockout threshold:\s+(\d+) compare <= 5
- c:\net.exe accounts -> n:Lockout threshold:\s+(\d+) compare > 0

Compliance

cis: 1.2.2

cis_csc: 4.10

En la versión en español de Windows, para llegar a "Account Lockout Policy\Account lockout duration" debes seguir estos pasos:

1. Haz clic en el botón de "Inicio" y escribe "Directiva de seguridad local" en el cuadro de búsqueda.
2. Selecciona "Directiva de seguridad local" en los resultados de búsqueda y ábrelo.
3. En la ventana de "Directiva de seguridad local", expande la carpeta "Directivas de cuenta".
4. Luego, haz clic en "Directivas de bloqueo de cuentas".
5. En el panel derecho, encontrarás la directiva "Duración del bloqueo de cuentas". Haz doble clic en ella para modificar su configuración.

15507 Failed

Rationale

Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

Remediation

To establish the recommended configuration via GP, set the following UI path to 5 or fewer invalid login attempt(s), but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold

Description

This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform to the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 5 or fewer invalid logon attempt(s), but not 0. Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Checks (Condition: all)

- c:net.exe accounts -> n:Lockout threshold:\s+(\d+) compare <= 5
- c:net.exe accounts -> n:Lockout threshold:\s+(\d+) compare > 0

Este texto proporciona recomendaciones sobre cómo configurar el umbral de bloqueo de cuenta ("account lockout threshold") para reducir la probabilidad de que un ataque de fuerza bruta de contraseña tenga éxito.

- Establecer un umbral de bloqueo de cuenta reduce la probabilidad de éxito de un ataque de fuerza bruta en línea.
- Sin embargo, configurar el umbral de bloqueo de cuenta demasiado bajo aumenta el riesgo de bloqueos accidentales y/o que un actor malintencionado bloquee intencionalmente cuentas.

Para remediar esta situación y establecer la configuración recomendada a través de la Política de Grupo (GP), se sugiere establecer el número de intentos de inicio de sesión inválidos en 5 o menos, pero no en 0. Esto se puede hacer siguiendo la ruta de la interfaz de usuario (UI) proporcionada en la política de grupo.

La política determina el número de intentos de inicio de sesión fallidos antes de que la cuenta se bloquee. Configurar esta política en 0 no cumple con el estándar de seguridad, ya que desactiva el umbral de bloqueo de cuenta.

La recomendación es establecer el umbral en 5 o menos intentos de inicio de sesión inválidos, pero no en 0.

Al igual que con la configuración anterior, se destaca que las configuraciones de Política de Contraseña (sección 1.1) y de Política de Bloqueo de Cuenta (sección 1.2) deben aplicarse a través de la Política de Grupo predeterminada del dominio para que tengan efecto en todas las cuentas de usuario del dominio como su comportamiento predeterminado. Sin embargo, se puede definir excepciones personalizadas a través de Objetos de Configuración de Contraseñas (PSOs) para usuarios y/o grupos específicos utilizando el Active Directory Administrative Center.

15508 Failed

Rationale

Users can accidentally lock themselves out of their accounts if they mistype their password multiple times. To reduce the chance of such accidental lockouts, the Reset account lockout counter after setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers lockouts is reset to 0.

Remediation

To establish the recommended configuration via GP, set the following UI path to 15 or more minute(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after

Description

This policy setting determines the length of time before the Account lockout threshold resets to zero. The default value for this policy setting is Not Defined. If the Account lockout threshold is defined, this reset time must be less than or equal to the value for the Account lockout duration setting. If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts. If no policy were determined to reset the account lockout, it would be a manual task for administrators. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically. The recommended state for this setting is: 15 or more minute(s). Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be

globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Check (Condition: all)

- c:\net.exe accounts -> n:Lockout observation window \(\minutes\):s+(\d+) compare >= 15

Compliance

cis: 1.2.3

cis_csc: 4.10

Este texto describe la configuración "Reset account lockout counter after", que determina la cantidad de minutos que deben pasar antes de que se reinicie el contador que registra los intentos de inicio de sesión fallidos y desencadena bloqueos de cuentas. La descripción explica que esta configuración establece el tiempo que debe transcurrir antes de que el umbral de bloqueo de cuenta se restablezca a cero. Recomienda que este tiempo sea de al menos 15 minutos para reducir el riesgo de bloqueos accidentales y para evitar ataques de denegación de servicio (DoS). También destaca la importancia de aplicar esta configuración a través de la Política de Grupo predeterminada del dominio para que tenga efecto en todas las cuentas de usuario del dominio. Además, menciona la posibilidad de definir excepciones personalizadas a través de Objetos de Configuración de Contraseñas (PSOs) en el Active Directory Administrative Center.

Para configurar la política "Reset account lockout counter after" en un entorno de Windows, sigue estos pasos:

1. **Accede al Editor de directivas de grupo (GPE):**
 - Presiona **Windows + R** para abrir el cuadro de diálogo Ejecutar.
 - Escribe **gpedit.msc** y presiona Enter.
2. **Navega hasta la configuración de la política:**

- En el Editor de directivas de grupo, ve a Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuenta -> Directivas de bloqueo de cuentas.

3. **Configura la política:**

- Haz doble clic en "Reset account lockout counter after".
- Selecciona "Habilitado".
- Ingresa el valor de tiempo deseado, en minutos, para que el contador se restablezca. El valor recomendado es al menos 15 minutos.

4. **Aplica la configuración:**

- Haz clic en Aplicar y luego en Aceptar para guardar los cambios.

Es importante tener en cuenta que estas configuraciones se aplicarán a nivel de la política de grupo local en el equipo en el que estás realizando estos cambios. Si estás trabajando en un entorno de dominio, es posible que desees configurar esta política en la Directiva de Grupo predeterminada del dominio para que se aplique a todos los usuarios del dominio.

Para establecer la configuración recomendada mediante la Política de Grupo (GP) y establecer el umbral de bloqueo de cuenta en 5 o menos intentos de inicio de sesión inválidos, pero no en 0, sigue estos pasos:

1. **Abrir el Editor de directivas de grupo (GPE):**

- Presiona **Windows + R** para abrir el cuadro de diálogo Ejecutar.
- Escribe **gpedit.msc** y presiona Enter.

2. **Navegar a la configuración de la política:**

- En el Editor de directivas de grupo, ve a **Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de cuenta -> Directivas de bloqueo de cuentas.**

3. **Establecer el umbral de bloqueo de cuenta:**

- Haz doble clic en "Account lockout threshold".
- Selecciona la opción "Habilitado".
- Ingresa el número deseado de intentos de inicio de sesión inválidos. En este caso, establece el valor en 5 o menos.
- Asegúrate de que el valor no sea 0, ya que se recomienda no desactivar completamente el umbral de bloqueo de cuenta.

4. **Aplicar la configuración:**

- Haz clic en Aplicar y luego en Aceptar para guardar los cambios.

Con estos pasos, habrás configurado el umbral de bloqueo de cuenta según las recomendaciones proporcionadas en el mensaje. Esto ayudará a mitigar los riesgos de bloqueos accidentales y ataques maliciosos, al tiempo que mantendrá una medida de seguridad efectiva para proteger las cuentas de usuario.

!!! 15509 Failed

Rationale

In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Remediation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status

Description

This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the Domain Controllers organizational unit via group policy because Domain Controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings. The recommended state for this setting is: Disabled.

Este texto aborda la configuración de deshabilitar la cuenta de administrador incorporada en los sistemas Windows y proporciona la justificación, así como el remedio recomendado para esta configuración. Aquí hay un resumen de cada sección:

Justificación:

- En algunas organizaciones, mantener un horario regular para cambios de contraseña periódicos puede ser un desafío de gestión.
- En lugar de depender de cambios de contraseña regulares para proteger la cuenta de administrador incorporada, puede ser preferible deshabilitarla.
- **La cuenta de administrador incorporada no puede bloquearse, lo que la convierte en un objetivo atractivo para ataques de fuerza bruta que intentan adivinar contraseñas.**
- **Además, esta cuenta tiene un identificador de seguridad (SID) bien conocido, lo que facilita a los atacantes autenticarse utilizando el SID en lugar del nombre de la cuenta.**

Remedio:

- **Para establecer la configuración recomendada a través de la Política de Grupo (GP), se sugiere deshabilitar la cuenta de administrador incorporada.**
- La ruta de la interfaz de usuario (UI) proporcionada guía hacia la configuración necesaria.
- La configuración "Accounts: Administrator account status" se establece en "Disabled" para deshabilitar la cuenta de administrador incorporada.

Descripción:

- Esta política permite habilitar o deshabilitar la cuenta de administrador durante la operación normal.
- En el modo seguro, la cuenta de administrador siempre está habilitada, independientemente de cómo esté configurada esta configuración.
- Se señala que esta configuración no tendrá impacto cuando se aplique a la unidad organizativa de Controladores de Dominio a través de la política de grupo, ya que los Controladores de Dominio no tienen una base de datos de cuentas locales.
- Se recomienda establecer esta configuración en "Disabled" para deshabilitar la cuenta de administrador incorporada.

Para deshabilitar la cuenta de administrador incorporada en Windows y crear otra cuenta de administrador, sigue estos pasos:

Deshabilitar la cuenta de administrador:

1. Abre el símbolo del sistema con privilegios de administrador. Puedes hacerlo buscando "cmd" en el menú de inicio, haciendo clic derecho en "Símbolo del sistema" y seleccionando "Ejecutar como administrador".
2. En el símbolo del sistema, escribe el siguiente comando y presiona Enter:
bash

```
net user administrator /active:no
```

1. Esto desactivará la cuenta de administrador incorporada.

Crear una nueva cuenta de administrador:

1. Abre el Panel de Control. Puedes hacerlo buscándolo en el menú de inicio.
2. Haz clic en "Cuentas de usuario" o "Cuentas de usuario y protección infantil", dependiendo de la versión de Windows que estés utilizando.
3. Haz clic en "Agregar o quitar cuentas de usuario".
4. Haz clic en "Agregar una cuenta nueva en PC local".
5. Sigue las instrucciones para crear una nueva cuenta de usuario. Asegúrate de seleccionar "Administrador" como el tipo de cuenta durante el proceso de creación.

Una vez que hayas deshabilitado la cuenta de administrador y creado una nueva cuenta de administrador, puedes usar la nueva cuenta para realizar tareas de administración en el sistema. Asegúrate de recordar la contraseña de esta nueva cuenta para evitar problemas de acceso en el futuro.

Simplemente asegúrate de abrir el Símbolo del sistema o Windows PowerShell con privilegios de administrador antes de ejecutar el comando, para que tenga los permisos necesarios para realizar los cambios en las cuentas de usuario del sistema.

15510 Failed

Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used to log onto their computers will probably want to block

Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

Remediation

To establish the recommended configuration via GP, set the following UI path to Users can't add or log on with Microsoft accounts: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts

Description

This policy setting prevents users from adding new Microsoft accounts on this computer. The recommended state for this setting is: Users can't add or log on with Microsoft accounts

Este texto aborda la configuración para bloquear cuentas de Microsoft en sistemas Windows y proporciona justificación, remedio recomendado y una descripción de la configuración.

Justificación:

- Las organizaciones que desean implementar eficazmente políticas de gestión de identidad y mantener un control estricto sobre qué cuentas se utilizan para iniciar sesión en sus computadoras probablemente deseen bloquear las cuentas de Microsoft.
- También puede ser necesario bloquear las cuentas de Microsoft para cumplir con los requisitos de los estándares de cumplimiento que se aplican a sus sistemas de información.

Remedio:

- Para establecer la configuración recomendada a través de la Política de Grupo (GP), se sugiere bloquear las cuentas de Microsoft mediante la configuración "Block Microsoft accounts".
- La ruta de la interfaz de usuario (UI) proporcionada guía hacia la configuración necesaria.

Descripción:

- Esta configuración de política evita que los usuarios agreguen nuevas cuentas de Microsoft en esta computadora.
- La configuración recomendada es que "Los usuarios no puedan agregar ni iniciar sesión con cuentas de Microsoft".

Esta configuración es útil para las organizaciones que desean restringir el uso de cuentas de Microsoft en sus sistemas y mantener el control sobre las cuentas de usuario utilizadas en sus entornos de trabajo.

Bloquear las cuentas de Microsoft puede ser importante en ciertos entornos empresariales o institucionales donde se necesita un control estricto sobre qué cuentas se utilizan para acceder a los sistemas informáticos. Aquí hay algunas razones por las que podría ser importante bloquear las cuentas de Microsoft:

1. **Políticas de seguridad:** Al restringir el uso de cuentas de Microsoft, las organizaciones pueden implementar políticas de seguridad más estrictas y garantizar que solo se utilicen cuentas corporativas autorizadas para acceder a los recursos de la empresa.
2. **Cumplimiento normativo:** Algunas organizaciones deben cumplir con estándares de cumplimiento que requieren medidas de seguridad específicas, como restringir el uso de ciertos tipos de cuentas para acceder a los sistemas de información.
3. **Gestión de identidades:** Bloquear las cuentas de Microsoft puede formar parte de una estrategia más amplia de gestión de identidades, donde se centraliza el control sobre las cuentas de usuario y se simplifica la administración de credenciales.
4. **Privacidad y protección de datos:** Al limitar el uso de cuentas de Microsoft, las organizaciones pueden proteger mejor la privacidad y los datos confidenciales de la empresa al evitar que los empleados utilicen servicios en la nube de Microsoft que podrían estar fuera del control de la organización.

Bloquear las cuentas de Microsoft puede ser importante en ciertos entornos empresariales o institucionales donde se necesita un control estricto sobre qué cuentas se utilizan para acceder a los sistemas informáticos. Aquí hay algunas razones por las que podría ser importante bloquear las cuentas de Microsoft:

1. **Políticas de seguridad:** Al restringir el uso de cuentas de Microsoft, las organizaciones pueden implementar políticas de seguridad más estrictas y

garantizar que solo se utilicen cuentas corporativas autorizadas para acceder a los recursos de la empresa.

2. **Cumplimiento normativo:** Algunas organizaciones deben cumplir con estándares de cumplimiento que requieren medidas de seguridad específicas, como restringir el uso de ciertos tipos de cuentas para acceder a los sistemas de información.
3. **Gestión de identidades:** Bloquear las cuentas de Microsoft puede formar parte de una estrategia más amplia de gestión de identidades, donde se centraliza el control sobre las cuentas de usuario y se simplifica la administración de credenciales.
4. **Privacidad y protección de datos:** Al limitar el uso de cuentas de Microsoft, las organizaciones pueden proteger mejor la privacidad y los datos confidenciales de la empresa al evitar que los empleados utilicen servicios en la nube de Microsoft que podrían estar fuera del control de la organización.

Sin embargo, la importancia de bloquear las cuentas de Microsoft puede variar según el contexto y los requisitos específicos de seguridad y cumplimiento de cada organización. Es importante evaluar cuidadosamente las necesidades de seguridad y las políticas internas antes de implementar esta medida.

15511 Failed

Rationale

The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network, which could lead to the exposure or corruption of data.

Remediation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status

Description

This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system. The recommended state for this setting is: Disabled. Note: This setting will have no impact when

applied to the Domain Controllers organizational unit via group policy because Domain Controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.

Este texto aborda la configuración para deshabilitar la cuenta de invitado (Guest) en sistemas Windows y proporciona justificación, remedio recomendado y una descripción de la configuración.

Justificación:

- La cuenta de invitado por defecto permite que los usuarios de la red no autenticados inicien sesión como invitado sin contraseña. Esto significa que estos usuarios no autorizados podrían acceder a cualquier recurso accesible para la cuenta de invitado a través de la red.
- Esto podría llevar a la exposición o corrupción de datos, ya que cualquier recurso compartido en la red con permisos que permitan el acceso a la cuenta de invitado, al grupo de invitados (Guests) o al grupo de Todos (Everyone) serán accesibles, incluso sin autenticación.

Remedio:

- Para establecer la configuración recomendada a través de la Política de Grupo (GP), se sugiere deshabilitar la cuenta de invitado mediante la configuración "Guest account status".
- La ruta de la interfaz de usuario (UI) proporcionada guía hacia la configuración necesaria.

Descripción:

- Esta configuración de política determina si la cuenta de invitado está habilitada o deshabilitada.
- La cuenta de invitado permite que los usuarios de la red no autenticados obtengan acceso al sistema.
- La configuración recomendada es establecer esta configuración en "Disabled" (Deshabilitado).

En resumen, esta configuración es importante para mitigar los riesgos asociados con la capacidad de usuarios no autenticados para acceder a recursos de red y proteger la seguridad y la integridad de los datos del sistema.

Para deshabilitar la cuenta de invitado (Guest) en sistemas Windows a través de la Política de Grupo (GP), sigue estos pasos:

1. Abre el Editor de directivas de grupo (GPE):
 - Presiona **Windows + R** para abrir el cuadro de diálogo Ejecutar.
 - Escribe **gpedit.msc** y presiona Enter.
2. Navega hasta la configuración de la política:
 - En el Editor de directivas de grupo, ve a **Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad**.
3. Busca la configuración "Accounts: Guest account status" en la lista de configuraciones de políticas.
4. Haz doble clic en "Accounts: Guest account status" para editar la configuración.
5. Selecciona la opción "Disabled" (Deshabilitado).
6. Haz clic en Aplicar y luego en Aceptar para guardar los cambios.

Una vez que hayas realizado estos pasos, la cuenta de invitado estará deshabilitada en tu sistema Windows, lo que ayudará a proteger los recursos de red y los datos del sistema contra el acceso no autorizado a través de la cuenta de invitado.

15513 Failed

Rationale

The Administrator account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for

brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Remediation

To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account

Description

The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console).

Check (Condition: all)

- c:\net user administrator -> r:The user name could not be found.

15514 Failed

Rationale

The Guest account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Remediation

To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account

Description

The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security.

Check (Condition: all)

- c:\net user guest -> r:The user name could not be found.

15517 Failed

Rationale

Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

Remediation

To establish the recommended configuration via GP, set the following UI path to Administrators and Interactive Users: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media

Description

This policy setting determines who is allowed to format and eject removable NTFS media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges. The recommended state for this setting is: Administrators and Interactive Users.

Checks (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon -> AllocateDASD
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon -> AllocateDASD -> 2

Para llevar a cabo esta configuración en Windows 10 utilizando Directiva de grupo (GP), sigue estos pasos:

1. Presiona las teclas **Windows + R** para abrir el cuadro de diálogo "Ejecutar".
2. Escribe "gpedit.msc" y presiona Enter. Esto abrirá el Editor de directivas de grupo local.

3. En el Editor de directivas de grupo local, navega a la siguiente ruta en el panel izquierdo:
Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad.
4. En el panel derecho, busca la directiva llamada "Permitir formatear y expulsar dispositivos extraíbles" o similar.
5. Haz doble clic en esta directiva para editarla.
6. Selecciona la opción "Administradores e Usuarios interactivos" para permitir que ambos puedan formatear y expulsar dispositivos extraíbles.
7. Haz clic en "Aplicar" y luego en "Aceptar" para guardar los cambios.

Con estos pasos, habrás configurado la política para permitir que los administradores y usuarios interactivos puedan formatear y expulsar dispositivos extraíbles. Esto ayudará a prevenir que usuarios no autorizados muevan datos a otros dispositivos donde tienen privilegios de administrador y puedan modificarlos.

15518 Failed

Rationale

It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, in a high security environment, you should allow only Administrators, not users, to do this, because printer driver installation may unintentionally cause the computer to become less stable. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious software that masquerades as a printer driver. It is feasible for an attacker to disguise a Trojan horse program as a printer driver. The program may appear to users as if they must use it to print, but such a program could unleash malicious code on your computer network.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers

Description

For a computer to print to a shared printer, the driver for that shared printer must be installed on the local computer. This security setting determines who is allowed to install a printer driver as part of connecting to a shared printer. The recommended state for this setting is: Enabled. Note: This setting does not affect the ability to add a local printer. This setting does not affect Administrators.

Checks (Condition: all)

- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers -> AddPrinterDrivers
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers -> AddPrinterDrivers -> 1

15519 Passed

Rationale

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated-and sensitive information such as passwords are encrypted-but the channel is not integrity-checked, and not all information is encrypted. Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always)

Description

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted. The recommended state for this setting is: Enabled.

15520 Passed

Rationale

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated-and sensitive information such as passwords are encrypted-but the channel is not integrity-checked, and not all information is encrypted. Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible)

Description

This policy setting determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates. The recommended state for this setting is: Enabled.

15521 Passed

Rationale

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated-and sensitive information such as passwords are encrypted-but the channel is not integrity-checked, and not all information is encrypted. Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally sign secure channel data (when possible)

Description

This policy setting determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network. The recommended state for this setting is: Enabled.

15522 Passed

Rationale

The default configuration for Windows Server 2003-based computers that belong to a domain is that they are automatically required to change the passwords for their accounts every 30 days. If you disable this policy setting, computers that run Windows Server 2003 will retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk from an attacker who could determine the password for the computer's domain account.

Remediation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password changes

Description

This policy setting determines whether a domain member can periodically change its computer account password. Computers that cannot automatically change their account passwords are potentially vulnerable, because an attacker might be able to determine the password for the system's domain account. The recommended state for this setting is: Disabled. Note: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

15523 Failed

Rationale

In Active Directory-based domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers

no longer change their passwords, an attacker will have more time to undertake a brute force attack to guess the password of one or more computer accounts.

Remediation

To establish the recommended configuration via GP, set the following UI path to 30 or fewer days, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age

Description

This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days. If you increase this interval significantly so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts. The recommended state for this setting is: 30 or fewer days, but not 0. Note: A value of 0 does not conform to the benchmark as it disables maximum password age. Note #2: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

15524 Passed

Rationale

Session keys that are used to establish secure channel communications between Domain Controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping. (Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or be redirected.)

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled:
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key

Description

When this policy setting is enabled, a secure channel can only be established with Domain Controllers that are capable of encrypting secure channel data with a strong (128-bit) session key. To enable this policy setting, all Domain Controllers in the domain must be able to encrypt secure channel data with a strong key, which means all Domain Controllers must be running Microsoft Windows 2000 or newer. The recommended state for this setting is: Enabled.

Checks (Condition: any)

- not
r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters
- not
r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters -> RequireStrongKey
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters -> RequireStrongKey -> 1

15525 Failed

Rationale

Microsoft developed this feature to make it easier for users with certain types of physical impairments to log on to computers that run Windows. If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path. An attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The attacker would then be able to log on to the compromised account with whatever level of privilege that user has.

Remediation

To establish the recommended configuration via GP, set the following UI path to Disabled:
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL

Description

This policy setting determines whether users must press CTRL+ALT+DEL before they log on. The recommended state for this setting is: Disabled.

Checks (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> DisableCAD
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> DisableCAD -> 0

15526 Failed

Rationale

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Remote Desktop Services) could view **the name of the last user who logged on to the server**. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Don't display last signed-in. Note: In older versions of Microsoft Windows, this setting was named Interactive logon: Do not display last user name, but it was renamed starting with Windows 10 Release 1703.

Description

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: Enabled.

Checks (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> DontDisplayLastUserName
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> DontDisplayLastUserName -> 1

15527 Failed

Rationale

If a machine is lost or stolen, or if an insider threat attempts a brute force password attack against the computer, it is important to ensure that BitLocker will lock the computer and therefore prevent a successful attack.

Remediation

To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid logon attempts, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine account lockout threshold

Description

This security setting determines the number of failed logon attempts that causes the machine to be locked out. Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password protected screen savers counts as failed logon attempts. The machine lockout policy is enforced only on those machines that have BitLocker enabled for protecting OS volumes. Please ensure that appropriate recovery password backup policies are enabled. The recommended state for this setting is: 10 or fewer invalid logon attempts, but not 0. Note: A value of 0 does not conform to the benchmark as it disables the machine account lockout threshold. Values from 1 to 3 will be interpreted as 4.

Checks (Condition: all)

- not
r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> MaxDevicePasswordFailedAttempts -> 0
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> MaxDevicePasswordFailedAttempts
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> MaxDevicePasswordFailedAttempts -> n:^(\\d+) compare <=30

Este fragmento describe una medida de seguridad relacionada con el bloqueo de cuentas de máquina en caso de intentos de inicio de sesión fallidos en un sistema Windows con BitLocker habilitado. Aquí hay una explicación de cada parte:

1. **Rationale (Justificación):** Si una máquina se pierde o es robada, o si alguien dentro de la organización intenta un ataque de fuerza bruta contra la contraseña de la máquina, es importante garantizar que BitLocker bloquee la máquina y prevenga un ataque exitoso.
2. **Remediation (Remediación):** Para establecer la configuración recomendada mediante Directiva de Grupo (GP), se debe configurar el umbral de bloqueo de la cuenta de la máquina en 10 o menos intentos de inicio de sesión fallidos, pero no en 0. Esto significa que después de un cierto número de intentos de inicio de sesión fallidos, la máquina se bloqueará y no permitirá más intentos de inicio de sesión hasta que se restablezca.
3. **Description (Descripción):** Esta configuración de seguridad determina el número de intentos de inicio de sesión fallidos que causan el bloqueo de la máquina. Los intentos fallidos de contraseña contra estaciones de trabajo o servidores miembros que han sido bloqueados mediante CTRL+ALT+DELETE o salvapantallas protegidos con contraseña se cuentan como intentos de inicio de sesión fallidos. Esta política de bloqueo de máquina se aplica solo en aquellas máquinas que tienen habilitado BitLocker para proteger los volúmenes del sistema operativo.
4. **Checks (Condiciones):** Se mencionan las claves del Registro de Windows que se deben verificar para asegurarse de que la configuración esté establecida correctamente. En este caso, se verifica que la clave MaxDevicePasswordFailedAttempts no sea igual a 0 y que su valor sea menor o igual a 30, lo que indica que se permite un número limitado de intentos de inicio de sesión fallidos antes de bloquear la máquina.

En resumen, esta medida de seguridad asegura que las máquinas con BitLocker habilitado se bloqueen después de un número específico de intentos de inicio de sesión fallidos, lo que ayuda a prevenir ataques de fuerza bruta y protege la integridad del sistema.



en el primer parrafo, qué es BitLocker?

ChatGPT

BitLocker es una característica de seguridad integrada en los sistemas operativos Windows que proporciona cifrado de disco completo para ayudar a proteger los datos almacenados en unidades de disco duro y unidades de estado sólido (SSD). Cuando BitLocker está habilitado, cifra automáticamente todo el contenido de la unidad, incluidos los archivos del sistema operativo, las aplicaciones instaladas y los archivos del usuario.

El cifrado de disco completo de BitLocker ayuda a proteger los datos almacenados en un dispositivo en caso de que sea perdido o robado, ya que el acceso a los datos cifrados requiere autenticación adecuada, como una contraseña, una tarjeta inteligente o una clave USB. Sin la autenticación adecuada, los datos cifrados no pueden ser accesibles ni legibles.

En resumen, BitLocker es una herramienta de cifrado de disco completo desarrollada por Microsoft que proporciona una capa adicional de seguridad para proteger los datos almacenados en unidades de disco en sistemas operativos Windows.

Si una máquina se bloquea después de alcanzar el número máximo de intentos de inicio de sesión fallidos, generalmente puedes desbloquearla de una de estas formas:

1. **Utilizando una cuenta de administrador:** Si tienes acceso a una cuenta de administrador del sistema, puedes iniciar sesión con esa cuenta y luego restablecer o desbloquear la cuenta bloqueada a través de la configuración de administración de usuarios o mediante herramientas administrativas proporcionadas por el sistema operativo.
2. **Utilizando una cuenta de recuperación de BitLocker:** Si la máquina tiene habilitado BitLocker y has configurado una clave de recuperación o una contraseña de BitLocker, puedes utilizar esta clave o contraseña para desbloquear la unidad de disco y acceder al sistema. Esto te permitirá iniciar sesión en el sistema y realizar las acciones necesarias para desbloquear la cuenta de usuario.
3. **Poniéndote en contacto con el soporte técnico:** Si no puedes desbloquear la máquina utilizando los métodos anteriores, es posible que necesites ponerte en contacto con el soporte técnico de tu organización o con el soporte técnico de Microsoft para obtener asistencia adicional. El soporte técnico puede proporcionarte orientación específica sobre cómo desbloquear la máquina en tu entorno particular.

En cualquier caso, es importante tener en cuenta que el proceso exacto para desbloquear una máquina puede variar dependiendo de la configuración específica del sistema y las políticas de seguridad de tu organización. Siempre es recomendable seguir los

procedimientos y las políticas establecidas por tu organización para la gestión de contraseñas y la recuperación de cuentas bloqueadas.

Fail 15528

Rationale

If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

Remediation

To establish the recommended configuration via GP, set the following UI path to 900 or fewer seconds, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit

Description

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session. The recommended state for this setting is: 900 or fewer second(s), but not 0. Note: A value of 0 does not conform to the benchmark as it disables the machine inactivity limit.

Fail 15529

Rationale

Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons—for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

Remediation

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message text for users attempting to log on

Description

This policy setting specifies a text message that displays to users when they log on. Set the following group policy to a value that is consistent with the security and operational requirements of your organization.

Fail 15531

Rationale

The number that is assigned to this policy setting indicates the number of users whose logon information the computer will cache locally. If the number is set to 4, then the computer caches logon information for 4 users. When a 5th user logs on to the computer, the server overwrites the oldest cached logon session. Users who access the computer console will have their logon credentials cached on that computer. An attacker who is able to access the file system of the computer could locate this cached information and use a brute force attack to attempt to determine user passwords. To mitigate this type of attack, Windows encrypts the information and obscures its physical location.

Remediation

To establish the recommended configuration via GP, set the following UI path to 4 or fewer logon(s): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available)

Description

This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a Domain Controller cannot be contacted. This policy setting determines the number of unique users for whom logon information is cached locally. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords. The recommended state for this setting is: 4 or fewer logon(s).

Este texto parece ser parte de una documentación o guía de configuración relacionada con la administración de políticas de seguridad en entornos de red Windows. En particular, se

refiere a la configuración de la caché de credenciales de inicio de sesión en computadoras cliente que forman parte de un dominio de Windows.

Aquí hay una explicación de los puntos clave:

1. **Número de usuarios en la caché de inicio de sesión:** Esta configuración determina cuántos usuarios pueden tener sus credenciales de inicio de sesión almacenadas localmente en una computadora cliente. Por ejemplo, si se establece en 4, la computadora almacenará las credenciales de inicio de sesión de hasta 4 usuarios. Cuando un quinto usuario inicia sesión, la sesión de inicio de sesión más antigua se sobrescribe.
2. **Mitigación de ataques:** Se menciona que la información de inicio de sesión almacenada localmente está encriptada y su ubicación física está oculta para evitar ataques de fuerza bruta por parte de atacantes que puedan acceder al sistema de archivos de la computadora. Si un atacante logra acceder a esta información, podría intentar adivinar las contraseñas de los usuarios mediante un ataque de fuerza bruta.
3. **Remediación:** Se proporciona una recomendación sobre cómo configurar esta política de seguridad a través de la política de grupo (GP) en entornos de red de Windows. Se sugiere que el número máximo de usuarios cuyas credenciales se almacenan en caché sea de 4 o menos.
4. **Descripción de la política:** Se explica que esta configuración controla si los usuarios pueden iniciar sesión en un dominio de Windows utilizando información de cuenta en caché, lo que permite el acceso incluso si no se puede contactar con un Controlador de Dominio. Se advierte sobre el riesgo de seguridad si esta información se encuentra comprometida y se recomienda establecer la cantidad máxima de usuarios en la caché de inicio de sesión.

Si estás utilizando tanto una cuenta de administrador como una cuenta de usuario estándar y deseas que ambas cuentas tengan acceso a la caché de credenciales de inicio de sesión en caso de que el controlador de dominio no esté disponible, entonces deberías establecer el número máximo de usuarios en la caché en al menos 2.

Esto garantizará que las credenciales de inicio de sesión de ambas cuentas se almacenen en la caché, lo que permitirá que ambas cuentas inicien sesión incluso cuando el sistema no pueda comunicarse con el controlador de dominio. De esta manera, podrás utilizar diferentes contraseñas para las cuentas de administrador y usuario sin problemas de acceso en situaciones donde el controlador de dominio no esté disponible.

Fail 15533 Rationale

Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

Remediation

To establish the recommended configuration via GP, set the following UI path to Lock Workstation (or, if applicable for your environment, Force Logoff or Disconnect if a Remote Desktop Services session): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior

Description

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: Lock Workstation. Configuring this setting to Force Logoff or Disconnect if a Remote Desktop Services session also conforms to the benchmark.

1. **Motivo:** A menudo, los usuarios olvidan bloquear sus estaciones de trabajo cuando se alejan de ellas, lo que podría permitir que usuarios malintencionados accedan a sus computadoras. Si se utilizan tarjetas inteligentes para la autenticación, es importante que la computadora se bloquee automáticamente cuando se retire la tarjeta, para garantizar que solo el usuario autorizado con la tarjeta inteligente pueda acceder a los recursos utilizando esas credenciales.
2. **Remediación:** Se proporciona una recomendación sobre cómo configurar esta política de seguridad a través de la política de grupo (GP) en entornos de red de Windows. La configuración sugerida es establecer el comportamiento de la extracción de la tarjeta inteligente en "Bloquear estación de trabajo". Esto asegura que la estación de trabajo se bloquee automáticamente cuando se retire la tarjeta inteligente.
3. **Descripción de la política:** Esta configuración determina qué sucede cuando se retira la tarjeta inteligente de un usuario que ha iniciado sesión en la computadora. La opción recomendada es "Bloquear estación de trabajo", lo que significa que la

estación de trabajo se bloqueará automáticamente cuando se retire la tarjeta inteligente. Otras opciones como "Forzar cierre de sesión" o "Desconectar" también pueden cumplir con los estándares de seguridad, dependiendo de la configuración específica del entorno, especialmente en entornos de servicios de escritorio remoto.

Fail 15534 Rationale

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)

Description

This policy setting determines whether packet signing is required by the SMB client component. Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: Enabled.

Este texto describe una política de seguridad relacionada con la firma digital de comunicaciones SMB (Server Message Block), un protocolo utilizado para compartir recursos en redes de Windows. Aquí está una explicación de los puntos clave:

1. **Motivo:** La suplantación de sesión (session hijacking) es una técnica utilizada por atacantes que tienen acceso a la misma red que el cliente o servidor para interrumpir, finalizar o robar una sesión en progreso. Los atacantes pueden potencialmente interceptar y modificar paquetes SMB no firmados y luego modificar el tráfico y reenviarlo para que el servidor realice acciones no deseadas. Alternativamente, el atacante podría hacerse pasar por el servidor o cliente después de la autenticación legítima y obtener acceso no autorizado a los datos.
2. **Remediación:** Se proporciona una recomendación sobre cómo configurar esta política de seguridad a través de la política de grupo (GP) en entornos de red de Windows. Se sugiere habilitar la firma digital de comunicaciones SMB en el cliente (es decir, la computadora que inicia la solicitud de comunicación). Esto asegura que tanto los usuarios como los servidores que alojan los datos estén autenticados antes de la transmisión de datos.
3. **Descripción de la política:** Esta configuración determina si la firma de paquetes es requerida por el componente cliente SMB. Se menciona la importancia de sincronizar esta configuración con su configuración complementaria en los servidores remotos a los que se conectan los clientes. La recomendación es establecer esta configuración en "Habilitado" para garantizar la seguridad de las comunicaciones SMB

La configuración de requerir firmas digitales en las comunicaciones SMB es generalmente recomendable tanto para empresas como para particulares, especialmente en entornos donde la seguridad de la red y la integridad de los datos son importantes.

Para empresas:

- En entornos empresariales, donde la seguridad de los datos y la protección contra ataques cibernéticos son prioridades fundamentales, habilitar la firma digital en las comunicaciones SMB puede proporcionar una capa adicional de seguridad.
- Las empresas suelen tener una mayor cantidad de recursos compartidos en red y una mayor cantidad de usuarios que acceden a estos recursos, lo que aumenta el riesgo de ataques de suplantación de sesión y manipulación de datos. Por lo tanto, la firma digital puede ayudar a mitigar estos riesgos.

Para particulares:

- Aunque los particulares pueden tener menos recursos compartidos en red que las empresas, aún así pueden ser vulnerables a ataques de suplantación de sesión y manipulación de datos, especialmente si están utilizando redes compartidas o públicas.
- Habilitar la firma digital en las comunicaciones SMB puede ayudar a proteger los datos personales y evitar la interceptación o manipulación de información confidencial.

En resumen, la configuración de requerir firmas digitales en las comunicaciones SMB es recomendable tanto para empresas como para particulares que buscan aumentar la seguridad de sus redes y proteger la integridad de sus datos.



Al intentar habilitar esta opción, me sale la siguiente advertencia: Si modifica esta configuración, puede tener un impacto en la compatibilidad con los clientes, servicios y aplicaciones.(Q823659). Necesito asegurarme que esto no va a ser un problema.

ChatGPT

La advertencia que mencionas es una precaución estándar que se muestra al modificar configuraciones de seguridad en Windows. Indica que al cambiar esta configuración, podría haber impactos en la interoperabilidad y compatibilidad con ciertos clientes, servicios o aplicaciones.

Sin embargo, en la mayoría de los casos, habilitar la firma digital en las comunicaciones SMB no debería causar problemas de compatibilidad significativos, especialmente en entornos domésticos o pequeñas empresas. Esta función es una medida de seguridad estándar y ampliamente aceptada en entornos corporativos y de red.

Para asegurarte de que no habrá problemas de compatibilidad, podrías realizar pruebas después de habilitar la firma digital para verificar si hay algún impacto negativo en el funcionamiento de tus aplicaciones o servicios habituales. Además, si tienes aplicaciones críticas que podrían verse afectadas, es posible que desees consultar con el proveedor de la aplicación o el servicio para obtener orientación específica sobre cómo habilitar la firma digital de manera segura.

En general, para la mayoría de los usuarios domésticos, habilitar la firma digital en las comunicaciones SMB debería mejorar la seguridad de la red sin causar problemas

significativos de compatibilidad. Siempre es una buena práctica realizar copias de seguridad antes de realizar cambios de configuración importantes para poder revertirlos si es necesario.

15537 Passed Rationale

Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive.

Remediation

To establish the recommended configuration via GP, set the following UI path to 15 or fewer minute(s): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session

Description

This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished. The maximum value is 99999, which is over 69 days; in effect, this value disables the setting. The recommended state for this setting is: 15 or fewer minute(s).

15538 Failed Rationale

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users

and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)

Description

This policy setting determines whether packet signing is required by the SMB server component. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: Enabled.

Passed 15539

Rationale

If your organization configures logon hours for users, then it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire

Description

This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable Network security: Force logoff when logon hours expire (Rule 2.3.11.6). If your organization configures logon hours for users, this policy setting is necessary to ensure they are effective. The recommended state for this setting is: Enabled.

15540 Failed

Rationale

The identity of a computer can be spoofed to gain unauthorized access to network resources.

Remediation

To establish the recommended configuration via GP, set the following UI path to Accept if provided by client (configuring to Required from client also conforms to the benchmark): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Server SPN target name validation level

Description

This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. The recommended state for this setting is: Accept if provided by client. Configuring this setting to Required from client also conforms to the benchmark.

Este texto describe una política de seguridad relacionada con la validación del nombre de destino del nombre principal del servicio (SPN) en servidores SMB (Server Message Block). Aquí está una explicación de los puntos clave:

1. **Motivo:** La identidad de un servidor puede ser falsificada para obtener acceso no autorizado a los recursos de red. Por lo tanto, es importante establecer configuraciones de seguridad que validen adecuadamente la identidad del servidor al establecer conexiones SMB.
2. **Remediación:** Se proporciona una recomendación sobre cómo configurar esta política de seguridad a través de la política de grupo (GP) en entornos de red de Windows. Se sugiere establecer el nivel de validación del nombre de destino del SPN en "Aceptar si se proporciona por el cliente". También se menciona que configurarlo en "Requerido por el cliente" también cumple con el estándar de seguridad.
3. **Descripción de la política:** Esta configuración controla el nivel de validación que realiza un servidor SMB en el nombre de destino del SPN proporcionado por el cliente cuando se establece una sesión utilizando el protocolo SMB. El protocolo

SMB es utilizado para compartir archivos e impresoras y otras operaciones de red en sistemas Windows. Esta configuración ayuda a prevenir ataques de falsificación de identidad conocidos como ataques de relé SMB. Esta configuración afecta tanto a SMB1 como a SMB2.

El texto proporcionado describe una recomendación de configuración específica para la validación del nombre de destino del nombre principal del servicio (SPN) en servidores SMB, como parte de las políticas de seguridad de Windows. La recomendación es establecer la configuración en "Aceptar si lo requiere el cliente" o "Requerido del cliente" para cumplir con las mejores prácticas de seguridad. Aquí está la explicación:

- **"Aceptar si lo requiere el cliente"**: Esta configuración indica que el servidor SMB aceptará el nombre de destino del SPN proporcionado por el cliente si este lo proporciona. Si el cliente no proporciona un nombre de destino del SPN, el servidor aceptará la conexión de todos modos. Esta opción proporciona cierta flexibilidad y es útil si necesitas equilibrar la seguridad con la compatibilidad con clientes que no proporcionan el nombre de destino del SPN.
- **"Requerido del cliente"**: Esta configuración indica que el servidor SMB solo aceptará la conexión si el cliente proporciona un nombre de destino del SPN válido. Si el cliente no proporciona un nombre de destino del SPN o si es inválido, la conexión será rechazada. Esta opción proporciona un mayor nivel de seguridad, ya que garantiza que el cliente proporcione información de identificación válida antes de establecer la conexión.

En resumen, esta política de seguridad ayuda a proteger los servidores SMB al validar adecuadamente la identidad del cliente que establece una conexión, lo que ayuda a prevenir ataques de falsificación de identidad y garantiza la seguridad de los recursos compartidos en red.

Sí, puede haber casos en los que clientes auténticos no proporcionen SPNs válidos. Esto puede ocurrir por varias razones, como:

1. **Configuración incorrecta del cliente**: Si la configuración del cliente no está correctamente alineada con los requisitos de autenticación del servidor, es posible que no proporcione un SPN válido.

2. **Errores de red:** En entornos de red complejos o poco confiables, los paquetes de red pueden perderse o alterarse, lo que podría hacer que la información de autenticación no llegue correctamente al servidor.
3. **Implementaciones personalizadas:** Algunas implementaciones de aplicaciones o sistemas pueden no proporcionar automáticamente los SPNs esperados debido a configuraciones personalizadas o requisitos específicos de la aplicación.

En estos casos, es importante tener en cuenta que la falta de un SPN válido no necesariamente indica un intento malicioso. Sin embargo, la verificación de SPN es una capa adicional de seguridad diseñada para prevenir ataques de suplantación de identidad y garantizar la integridad de las conexiones SMB. Por lo tanto, la configuración de "Requerido del cliente" puede ser más adecuada en entornos donde la seguridad es una prioridad, aunque se debe equilibrar con consideraciones de compatibilidad y usabilidad.

Passed 15541 Rationale

If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

Remediation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation

Description

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. The recommended state for this setting is: Disabled.

15542 Passed

Rationale

An unauthorized user could anonymously list account names and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts

Description

This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will not be able to enumerate domain account user names on the systems in your environment. This policy setting also allows additional restrictions on anonymous connections. The recommended state for this setting is: Enabled. Note: This policy has no effect on Domain Controllers.

15543 Passed

Este texto describe una recomendación de seguridad relacionada con la enumeración anónima de cuentas SAM (Security Account Manager) y recursos compartidos de red en sistemas Windows. Aquí está una explicación de los puntos clave:

1. **Motivo:** La enumeración anónima de cuentas SAM y recursos compartidos de red puede proporcionar a usuarios no autorizados información valiosa que podría ser utilizada para intentar adivinar contraseñas o realizar ataques de ingeniería social. Por lo tanto, es importante limitar esta capacidad para mitigar el riesgo de acceso no autorizado a los recursos de la red.
2. **Remediación:** Se proporciona una recomendación sobre cómo configurar esta política de seguridad a través de la política de grupo (GP) en entornos de red de Windows. Se sugiere habilitar la configuración que impide la enumeración anónima de cuentas SAM y recursos compartidos de red. Esto se logra estableciendo la política de "No permitir la enumeración anónima de cuentas SAM y recursos compartidos de red" en "Habilitado".

3. **Descripción de la política:** Esta configuración controla la capacidad de los usuarios anónimos para enumerar cuentas SAM y recursos compartidos de red en sistemas Windows. Si esta configuración está habilitada, los usuarios anónimos no podrán enumerar nombres de usuarios de cuentas de dominio ni nombres de recursos compartidos de red en los sistemas en tu entorno. La recomendación es habilitar esta configuración para aumentar la seguridad de la red limitando la cantidad de información sensible que está disponible para usuarios no autenticados.

En resumen, esta política de seguridad ayuda a proteger los recursos de la red limitando la información que está disponible para usuarios no autenticados, lo que reduce el riesgo de ataques de seguridad y protege la privacidad de los usuarios y la integridad de los datos.

Failed 15544 Rationale

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares

Description

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the systems in your environment. The recommended state for this setting is: Enabled. Note: This policy has no effect on Domain Controllers.

Este texto describe una recomendación de seguridad relacionada con la enumeración anónima de cuentas SAM (Security Account Manager) y recursos compartidos de red en sistemas Windows. Aquí está una explicación de los puntos clave:

1. **Motivo:** La enumeración anónima de cuentas SAM y recursos compartidos de red puede proporcionar a usuarios no autorizados información valiosa que podría ser utilizada para intentar adivinar contraseñas o realizar ataques de ingeniería social. Por lo tanto, es importante limitar esta capacidad para mitigar el riesgo de acceso no autorizado a los recursos de la red.
2. **Remediación:** Se proporciona una recomendación sobre cómo configurar esta política de seguridad a través de la política de grupo (GP) en entornos de red de Windows. Se sugiere habilitar la configuración que impide la enumeración anónima de cuentas SAM y recursos compartidos de red. Esto se logra estableciendo la política de "No permitir la enumeración anónima de cuentas SAM y recursos compartidos de red" en "Habilitado".
3. **Descripción de la política:** Esta configuración controla la capacidad de los usuarios anónimos para enumerar cuentas SAM y recursos compartidos de red en sistemas Windows. Si esta configuración está habilitada, los usuarios anónimos no podrán enumerar nombres de usuarios de cuentas de dominio ni nombres de recursos compartidos de red en los sistemas en tu entorno. La recomendación es habilitar esta configuración para aumentar la seguridad de la red limitando la cantidad de información sensible que está disponible para usuarios no autenticados.

En resumen, esta política de seguridad ayuda a proteger los recursos de la red limitando la información que está disponible para usuarios no autenticados, lo que reduce el riesgo de ataques de seguridad y protege la privacidad de los usuarios y la integridad de los datos.

La incompatibilidad con clientes podría surgir si algún software o dispositivo en la red depende de la capacidad de enumerar cuentas SAM y recursos compartidos de forma anónima para su funcionamiento adecuado. Aunque la enumeración anónima puede representar un riesgo de seguridad, algunos sistemas o aplicaciones pueden requerirla por razones legítimas o funcionales.

Si una configuración de seguridad impide la enumeración anónima de cuentas SAM y recursos compartidos de red, los clientes que dependen de esta funcionalidad pueden dejar de funcionar correctamente. Por ejemplo:

1. **Software de administración remota:** Algunas herramientas de administración remota pueden requerir la capacidad de enumerar cuentas y recursos compartidos

de forma anónima para funcionar correctamente, especialmente si están diseñadas para realizar tareas de administración en entornos de red.

2. **Dispositivos de red:** Algunos dispositivos de red, como impresoras o sistemas de almacenamiento en red (NAS), pueden requerir la enumeración anónima de recursos compartidos para ser accesibles desde la red.
3. **Aplicaciones personalizadas:** Las aplicaciones personalizadas desarrolladas internamente o por terceros pueden haber sido diseñadas con la expectativa de que la enumeración anónima esté disponible y pueden experimentar problemas si esta funcionalidad se deshabilita.

En estos casos, la implementación de políticas de seguridad que deshabilitan la enumeración anónima de cuentas SAM y recursos compartidos puede resultar en incompatibilidades con ciertos clientes o dispositivos que dependen de esta funcionalidad. Por lo tanto, al establecer estas políticas, es importante evaluar cuidadosamente el impacto en la funcionalidad de la red y realizar pruebas exhaustivas para identificar y abordar cualquier incompatibilidad potencial.

15545 Rationale

Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication

Description

This policy setting determines whether Credential Manager (formerly called Stored User Names and Passwords) saves passwords or credentials for later use when it gains domain authentication. The recommended state for this setting is: Enabled. Note: Changes to this setting will not take effect until Windows is restarted.

Este texto describe una recomendación de seguridad relacionada con el almacenamiento de contraseñas y credenciales para la autenticación en red en Windows. Aquí está una explicación de los puntos clave:

1. **Motivo:** Las contraseñas y credenciales almacenadas en la memoria caché pueden ser accesibles para el usuario cuando está conectado a la computadora. Esto puede representar un riesgo de seguridad si el usuario ejecuta código malicioso sin saberlo, ya que este código podría leer las contraseñas almacenadas y enviarlas a un usuario no autorizado.
2. **Remediación:** Se proporciona una recomendación sobre cómo configurar esta política de seguridad a través de la política de grupo (GP) en entornos de Windows. Se sugiere habilitar la configuración que evita el almacenamiento de contraseñas y credenciales para la autenticación en red. Esto se logra estableciendo la política de "No permitir el almacenamiento de contraseñas y credenciales para la autenticación en red" en "Habilitado".
3. **Descripción de la política:** Esta configuración determina si el Administrador de Credenciales (anteriormente llamado Nombres de usuario y contraseñas almacenados) guarda contraseñas o credenciales para su uso posterior cuando obtiene autenticación de dominio. Al habilitar esta configuración, se evita que Windows almacene contraseñas y credenciales en la memoria caché, reduciendo así el riesgo de exposición en caso de compromiso del sistema.

En resumen, esta política de seguridad ayuda a proteger las contraseñas y credenciales de red almacenadas en la memoria caché del sistema, reduciendo el riesgo de exposición en caso de que el sistema sea comprometido por código malicioso ejecutado por el usuario.

15547 Passed

Rationale

Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Remediation

To establish the recommended configuration via GP, set the following UI path to <blank> (i.e. None): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Named Pipes that can be accessed anonymously

Description

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access. The recommended state for this setting is: <blank> (i.e. None).

Las "named pipes" (tubos con nombre) son un mecanismo de comunicación interprocesos (IPC) en sistemas operativos como Windows. Permiten que dos procesos se comuniquen entre sí a través del sistema de archivos. Cada named pipe tiene un nombre único y puede utilizarse para transferir datos entre procesos, incluso si los procesos se están ejecutando en diferentes sesiones de usuario.

La recomendación de seguridad mencionada en el texto sugiere limitar las named pipes que pueden ser accedidas de forma anónima. Esto significa restringir el acceso a named pipes sin requerir autenticación, lo que puede reducir la superficie de ataque del sistema al limitar las oportunidades para que los usuarios no autenticados accedan a recursos del sistema a través de named pipes.

La "remediación" recomendada es establecer la configuración de "Named Pipes que pueden ser accedidas de forma anónima" en "<blank>" (es decir, ninguno), lo que impide el acceso anónimo a cualquier named pipe en el sistema. Esto ayuda a fortalecer la seguridad limitando las posibles vulnerabilidades asociadas con el acceso anónimo a named pipes.

En resumen, esta política de seguridad tiene como objetivo reducir el riesgo de ataques al sistema restringiendo el acceso anónimo a named pipes, lo que puede ayudar a proteger la integridad y seguridad del sistema operativo.

15548 Passed

Rationale

The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker could use this information to facilitate unauthorized

activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

Remediation

To establish the recommended configuration via GP, set the following UI path to:
System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server
Applications SOFTWARE\Microsoft\Windows NT\CurrentVersion Computer
Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Remotely accessible registry paths

Description

This policy setting determines which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the winreg registry key. Note: This setting does not exist in Windows XP. There was a setting with that name in Windows XP, but it is called 'Network access: Remotely accessible registry paths and sub-paths' in Windows Server 2003, Windows Vista, and Windows Server 2008 (non-R2). Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. The recommended state for this setting is:
System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server
Applications Software\Microsoft\Windows NT\CurrentVersion

15549 Passed

Rationale

The registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack.

Remediation

To establish the recommended configuration via GP, set the following UI path to:
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog SOFTWARE\Microsoft\OLAP Server
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Windows	System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal	Server
System\CurrentControlSet\Control\Terminal	Server\UserConfig
System\CurrentControlSet\Control\Terminal	Server\DefaultUserConfiguration
SOFTWARE\Microsoft\Windows	NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog	Computer Configuration\Policies\Windows
Settings\Security	Settings\Local Policies\Security Options\Network access: Remotely
accessible registry paths and sub-paths	
Description	
<p>This policy setting determines which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the winreg registry key. Note: In Windows XP this setting is called 'Network access: Remotely accessible registry paths,' the setting with that same name in Windows Vista, Windows Server 2008 (non-R2), and Windows Server 2003 does not exist in Windows XP. Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. The recommended state for this setting is:</p>	
System\CurrentControlSet\Control\Print\Printers	
System\CurrentControlSet\Services\Eventlog	Software\Microsoft\OLAP
Server	
Software\Microsoft\Windows	NT\CurrentVersion\Print
Software\Microsoft\Windows	
NT\CurrentVersion\Windows	System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal	Server
System\CurrentControlSet\Control\Terminal	Server\UserConfig
System\CurrentControlSet\Control\Terminal	Server\DefaultUserConfiguration
Software\Microsoft\Windows	NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog	

15550 Passed

Rationale

Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named Pipes and Shares

Description

When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the Network access: Named pipes that can be accessed anonymously and Network access: Shares that can be accessed anonymously settings. This policy setting controls null session access to shares on your computers by adding RestrictNullSessAccess with the value 1 in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources. The recommended state for this setting is: Enabled.

15552 Passed Rationale

It is very dangerous to allow any values in this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Remediation

To establish the recommended configuration via GP, set the following UI path to <blank> (i.e. None): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously

Description

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server. The recommended state for this setting is: <blank> (i.e. None).

15553 Rationale

With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase

security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

Remediation

To establish the recommended configuration via GP, set the following UI path to Classic - local users authenticate as themselves: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts

Description

This policy setting determines how network logons that use local accounts are authenticated. The Classic option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The Guest only option allows you to treat all users equally. In this context, all users authenticate as Guest only to receive the same access level to a given resource. The recommended state for this setting is: Classic - local users authenticate as themselves. Note: This setting does not affect interactive logons that are performed remotely by using such services as Telnet or Remote Desktop Services (formerly called Terminal Services).

15554 Failed

Rationale

When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008 (non-R2), services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM

Description

This policy setting determines whether Local System services that use Negotiate when reverting to NTLM authentication can use the computer identity. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: Enabled.

Este texto se refiere a una configuración de seguridad en Windows que afecta cómo los servicios que se ejecutan como Local System manejan la **autenticación NTLM (NT LAN Manager) cuando utilizan SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism)**.

Aquí hay una explicación de los puntos clave:

1. **Contexto:** En versiones anteriores de Windows, cuando un servicio que se ejecuta como Local System utiliza SPNEGO para la autenticación y luego vuelve a NTLM, puede usar la identidad del equipo para la autenticación. Esto puede ocurrir cuando el servicio se conecta a computadoras que ejecutan versiones de Windows anteriores a Windows Vista o Windows Server 2008.
2. **Comportamiento en Windows 7 y versiones posteriores:** En Windows 7 y versiones posteriores, al conectarse a un servidor que ejecuta Windows Server 2008 o Windows Vista, un servicio del sistema puede usar tanto la identidad del equipo como una sesión nula para la autenticación. La sesión nula genera una clave de sesión sin protección, lo que permite a las aplicaciones firmar y cifrar datos sin errores, pero sin ofrecer protección real.
3. **Remediación:** La recomendación es habilitar la configuración que permite a los servicios del sistema Local System utilizar la identidad del equipo para la autenticación NTLM cuando utilizan SPNEGO y luego vuelven a NTLM. Esta configuración se aplica a Windows 7 o versiones posteriores, así como a Windows Server 2008 R2 o versiones posteriores.

En resumen, esta política de seguridad determina si los servicios del sistema Local System pueden usar la identidad del equipo para la autenticación NTLM en determinadas circunstancias, lo que puede afectar la forma en que se maneja la autenticación y la protección de datos en entornos de red de Windows.

15555 passed

Rationale

NULL sessions are less secure because by definition they are unauthenticated.

Remediation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback

Description

This policy setting determines whether NTLM is allowed to fall back to a NULL session when used with LocalSystem. The recommended state for this setting is: Disabled.

Este texto se refiere a una configuración de seguridad en Windows relacionada con las "NULL sessions" (sesiones nulas) en el contexto de la autenticación NTLM (NT LAN Manager). Aquí está una explicación de los puntos clave:

1. **Contexto de las NULL sessions:** Una "NULL session" es una conexión anónima a un recurso compartido de red en un sistema Windows. Estas sesiones no están autenticadas, lo que significa que no se requiere un nombre de usuario ni una contraseña para acceder a los recursos compartidos. Las NULL sessions pueden representar un riesgo de seguridad porque proporcionan acceso anónimo a ciertos recursos del sistema.
2. **Comportamiento de NTLM y LocalSystem:** NTLM es un protocolo de autenticación utilizado en sistemas Windows. La configuración mencionada en el texto determina si NTLM está permitido para recurrir a una NULL session cuando se utiliza con LocalSystem, que es una cuenta de sistema especial en Windows que tiene privilegios elevados.
3. **Remediación:** La recomendación es deshabilitar la configuración que permite que NTLM recurra a una NULL session cuando se usa con LocalSystem. Al deshabilitar esta opción, se evita que NTLM use NULL sessions, lo que mejora la seguridad al prevenir el acceso anónimo no autenticado a recursos del sistema.

15556 Passed Rationale

The PKU2U protocol is a peer-to-peer authentication protocol - authentication should be managed centrally in most managed networks.

Remediation

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities

Description

This setting determines if online identities are able to authenticate to this computer. The Public Key Cryptography Based User-to-User (PKU2U) protocol introduced in Windows 7 and Windows Server 2008 R2 is implemented as a security support provider (SSP). The SSP enables peer-to-peer authentication, particularly through the Windows 7 media and file sharing feature called HomeGroup, which permits sharing between computers that are not members of a domain. With PKU2U, a new extension was introduced to the Negotiate authentication package, Spnego.dll. In previous versions of Windows, Negotiate decided whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, Negoexts.dll, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U. When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes. The recommended state for this setting is: Disabled.

15557 Failed

Rationale

The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Remediation

To establish the recommended configuration via GP, set the following UI path to AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Configure encryption types allowed for Kerberos

Description

This policy setting allows you to set the encryption types that Kerberos is allowed to use. The recommended state for this setting is: AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types. Note: Some legacy applications and OSes may still require RC4_HMAC_MD5 - we recommend you test in your environment and verify whether you can safely remove it.

Este texto se refiere a una configuración de seguridad en Windows que afecta los tipos de cifrado permitidos para la autenticación Kerberos. Aquí está una explicación de los puntos clave:

1. **Contexto de la autenticación Kerberos:** Kerberos es un protocolo de autenticación de red que se utiliza ampliamente en entornos Windows para la autenticación de usuarios y servicios. Los tipos de cifrado especifican los algoritmos utilizados para cifrar los datos durante el proceso de autenticación, lo que ayuda a garantizar la seguridad de la comunicación.
2. **Consideraciones de seguridad:** La fuerza de cada algoritmo de cifrado varía, y elegir algoritmos más fuertes puede reducir el riesgo de compromiso de la seguridad. Sin embargo, es importante tener en cuenta que algunos sistemas y aplicaciones pueden no ser compatibles con ciertos algoritmos de cifrado más fuertes. Por lo tanto, al configurar los tipos de cifrado permitidos, es necesario equilibrar la seguridad con la compatibilidad.
3. **Remediación:** La recomendación es establecer los tipos de cifrado permitidos para Kerberos en "AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types". Esto permite el uso de algoritmos de cifrado más fuertes como AES128 y AES256, junto con cualquier tipo de cifrado futuro que pueda ser introducido en versiones posteriores de Windows.

Para un uso particular, como jugar a videojuegos en plataformas como Steam y Epic Games, la configuración de los tipos de cifrado permitidos para Kerberos mencionada en el texto no afectará directamente tu experiencia de juego. Esta configuración es más relevante en entornos empresariales o de red, donde la seguridad de la autenticación Kerberos es una consideración importante.

Sin embargo, es importante tener en cuenta que ajustar esta configuración podría afectar la compatibilidad con otros sistemas o aplicaciones en tu red local. Por ejemplo, si tienes otros dispositivos o servicios que utilizan la autenticación Kerberos y no son compatibles con los tipos de cifrado seleccionados, podrías experimentar problemas de conectividad.

Dado que tu caso es para un uso particular y no en un entorno empresarial, es posible que no necesites realizar cambios en esta configuración a menos que tengas un conocimiento profundo de cómo afectará a tu red local y estés dispuesto a asumir cualquier riesgo potencial de compatibilidad. En general, para un usuario particular, es más importante enfocarse en mantener actualizado el software, utilizar contraseñas seguras y seguir las mejores prácticas de seguridad cibernética en lugar de realizar ajustes avanzados en la configuración de seguridad del sistema operativo.

15558 Passed Rationale

The SAM file can be targeted by attackers who seek access to username and password hashes. Such attacks use special tools to crack passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks will not be prevented if you enable this policy setting, but it will be much more difficult for these types of attacks to succeed.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change
Description

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Microsoft Windows NT hash. Since LM hashes are stored on the local computer in the security database, passwords can then be easily compromised if the database is attacked. Note: Older operating systems and some third-party applications may fail when this policy setting is enabled. Also, note that the password will need to be changed on all accounts after you enable this setting to gain the proper benefit. The recommended state for this setting is: Enabled

15560 Failed

Rationale

Windows 2000 and Windows XP clients were configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM).

The default settings in OSes predating Windows Vista / Windows Server 2008 (non- R2) allowed all clients to authenticate with servers and use their resources. However, this meant that LM responses - the weakest form of authentication response - were sent over the network, and it was potentially possible for attackers to sniff that traffic to more easily reproduce the user's password. The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for older clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 or newer Domain Controllers. For these reasons, it is strongly preferred to restrict the use of LM & NTLM (non-v2) as much as possible.

Remediation

To establish the recommended configuration via GP, set the following UI path to: Send NTLMv2 response only. Refuse LM & NTLM: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level

Description

LAN Manager (LM) was a family of early Microsoft client/server software (predating Windows NT) that allowed users to link personal computers together on a single network. LM network capabilities included transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations: -Join a domain -Authenticate between Active Directory forests -Authenticate to down-level domains -Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP -Authenticate to computers that are not in the domain. The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers. The recommended state for this setting is: Send NTLMv2 response only. Refuse LM & NTLM.

Este texto se refiere a una configuración de seguridad en Windows que afecta los protocolos de autenticación utilizados para las conexiones de red en entornos de dominio de Windows. Aquí está una explicación de los puntos clave:

1. **Contexto de LM, NTLM y NTLMv2:** LM (LAN Manager) y NTLM (NT LAN Manager) son protocolos de autenticación más antiguos utilizados en versiones anteriores de Windows. Estos protocolos son menos seguros y pueden ser vulnerables a ataques de fuerza bruta y ataques de "replay". NTLMv2 es una versión mejorada de NTLM que ofrece una mayor seguridad al utilizar un canal seguro para proteger el proceso de autenticación.
2. **Motivo de la recomendación:** En versiones anteriores de Windows, los clientes estaban configurados por defecto para enviar respuestas de autenticación LM y NTLM, lo que potencialmente exponía las contraseñas de los usuarios a ataques de sniffing en la red. La recomendación es restringir el uso de LM y NTLM (no-v2) tanto como sea posible y utilizar NTLMv2 como el protocolo de autenticación preferido para mejorar la seguridad de la red.
3. **Remediación:** La recomendación es establecer la configuración de nivel de autenticación LAN Manager en "Enviar solo respuesta NTLMv2. Rechazar LM y NTLM". Esto asegura que solo se utilice NTLMv2 para la autenticación de red y se rechacen las respuestas LM y NTLM menos seguras.

En resumen, esta política de seguridad ayuda a fortalecer la seguridad de la autenticación de red al restringir el uso de los protocolos de autenticación menos seguros (LM y NTLM) y promover el uso de NTLMv2, que ofrece una mayor seguridad y protección contra ataques de seguridad.

Algunas aplicaciones o escenarios en los que podrías encontrar problemas de compatibilidad al restringir el uso de los protocolos de autenticación menos seguros (LM y NTLM) incluyen:

1. **Aplicaciones heredadas:** Programas de software más antiguos que no han sido actualizados para utilizar métodos de autenticación más modernos pueden depender de los protocolos LM o NTLM para la autenticación. Esto podría incluir aplicaciones empresariales personalizadas o software de terceros más antiguo.

2. **Dispositivos de red:** Algunos dispositivos de red, como impresoras, escáneres, sistemas de almacenamiento en red (NAS) u otros dispositivos que acceden a recursos compartidos de archivos, pueden utilizar protocolos de autenticación más antiguos que no son compatibles con NTLMv2.
3. **Integración con sistemas heredados:** Si tu sistema está integrado con sistemas heredados o entornos de TI más antiguos que aún utilizan protocolos de autenticación menos seguros, es posible que necesites mantener la compatibilidad con estos sistemas al restringir el uso de LM y NTLM.
4. **Acceso a recursos compartidos en redes no actualizadas:** En entornos de red mixtos donde algunos dispositivos o sistemas no han sido actualizados para utilizar NTLMv2, restringir el uso de LM y NTLM podría causar problemas de acceso a recursos compartidos en esas redes.

Estos son solo algunos ejemplos de situaciones en las que podrías encontrar problemas de compatibilidad al restringir el uso de los protocolos de autenticación menos seguros. Es importante evaluar cuidadosamente tu entorno y realizar pruebas exhaustivas después de aplicar cualquier cambio en la configuración de seguridad para garantizar que todas las aplicaciones y sistemas funcionen correctamente.

Score 31%

End scan

Apr 23, 2024 @ 09:52:25.000