



Recomendaciones de remediación

BanCoppel

19 de Agosto del 2021

CONTENIDO

RECOMENDACIONES DE REMEDIACIÓN	3
Priorizar las acciones de remediación.....	3
Resumen de recomendaciones.....	4
Recomendaciones para la postura y la preparación.....	8
Fortalecimiento: Protecciones de cuentas y credenciales	36
Fortalecimiento: Puntos finales	50
Fortalecimiento: Red Hat Enterprise Linux.....	65
Contención: Erradicación	81
Mejoras estratégicas	95
APÉNDICE A: PLANTILLAS DE POLÍTICAS DE GRUPO - DATASTORE CENTRALIZADO	104
APÉNDICE B: ESTRATEGIA DE REMEDIACIÓN	105
Actividades de remediación	105
APÉNDICE C: EXPLICACIÓN DEL CICLO DE VIDA DEL ATAQUE DIRIGIDO	108
APÉNDICE D: DESCRIPCIÓN GENERAL DE SYSMON.....	109

RECOMENDACIONES DE REMEDIACIÓN

Priorizar las acciones de remediación

Etapas: Postura, preparación y fortalecimiento

Las recomendaciones de la etapa uno se califican como críticas. Estas actividades ayudarán a mejorar la detección de la actividad de los atacantes, fortalecer el entorno y prepararse para un evento de erradicación durante el cual BanCoppel eliminará el acceso de los atacantes al entorno. Mandiant recomienda que BanCoppel comience a ejecutar dichas actividades preparatorias de inmediato.

Etapas: Contención, mejoras a medio plazo y erradicación

Se recomienda que el evento de erradicación se ejecute durante un período corto de tiempo, generalmente 48 horas. Este enfoque elimina al atacante del entorno sin previo aviso, lo que minimiza las posibilidades de que el atacante cambie de táctica y se mueva sin ser detectado a otras partes del entorno.

El evento de erradicación sigue el siguiente proceso ordenado:

- Implementar bloqueos de red y sinkholes de DNS
- Deshabilitar o fortalecer las cuentas comprometidas
- Limpiar y verificar los sistemas a los que se accede
- Eliminar y reconstruir sistemas comprometidos
- Implementar una herramienta para analizar automáticamente el correo electrónico en busca de contenido malicioso
- Realizar el restablecimiento de la contraseña empresarial
- Rotar las contraseñas del administrador local
- Reemplazar los sistemas comprometidos

Etapas: mejoras estratégicas

Es probable que la implementación de las recomendaciones de la Etapa Tres lleve más tiempo que las actividades de la Etapa Uno o Dos. Estas iniciativas están diseñadas para mejorar aún más la capacidad de la organización para prevenir, detectar y responder a diversos ataques.

Estas recomendaciones están diseñadas para:

- Mejorar las capacidades fundamentales de seguridad
- Limitar el acceso remoto a los sistemas, especialmente los sistemas críticos
- Mejorar el monitoreo, la detección y la respuesta de la seguridad
- Fortalecer el entorno de la red
- Reducir el alcance de las cuentas privilegiadas basadas en dominios

Además, cualquier recomendación de la Etapa Uno o la Etapa Dos que no se pudo implementar dentro de la etapa identificada puede priorizarse para ser implementada como una recomendación de la Etapa Tres.

Resumen de recomendaciones

Recomendaciones	Categorización	Flujo de trabajo
Etapas de recomendaciones para la postura y la preparación		
1.1.1 Revisar los ajustes de configuración de la auditoría de Windows	Postura	Registro y monitoreo - Visibilidad
1.1.2 Asegurar el registro de eventos de la creación de procesos de línea de comandos	Postura	Registro y monitoreo - Visibilidad
1.1.3 Implementar Microsoft System Monitor (Sysmon) en sistemas clave	Postura	Registro y monitoreo - Visibilidad
1.1.4 Imponer la auditoría para eventos de tareas programadas	Postura	Registro y monitoreo - Visibilidad
1.1.5 Habilitar PowerShell, la gestión remota de Windows y la auditoría de WMI	Postura	Registro y monitoreo - Visibilidad
1.1.6 Mejorar el registro de DNS	Postura	Registro y monitoreo - Visibilidad
1.1.7 Mejorar el registro de Unix	Postura	Registro y monitoreo - Visibilidad
1.1.8 Verificar el reenvío de fuentes de bitácora críticas al SIEM	Postura	Registro y monitoreo - Visibilidad
1.1.9 Imponer la auditoría para objetos de la política de grupo (GPO)	Postura	Registro y monitoreo - Visibilidad
1.1.10 Identificar y documentar las cuentas privilegiadas basadas en dominios	Postura	Directorio activo – Preparación de fortalecimiento
1.1.11 Identificar y documentar cuentas de servicio basadas en dominios	Postura	Directorio activo – Preparación de fortalecimiento
1.1.12 Identificar y documentar cuentas con contraseñas sin caducidad	Postura	Directorio activo – Preparación de fortalecimiento
1.1.13 Revisar las políticas de contraseña y los controles de autenticación	Postura	Directorio activo – Preparación de fortalecimiento
1.1.14 Identificar y revisar el alcance de las cuentas con permisos administrativos locales	Postura	Cuentas de punto final - Fortalecimiento
1.1.15 Documentar la implementación y la cobertura de las herramientas de seguridad del antivirus y el punto final	Postura	Punto final – Preparación de fortalecimiento

Recomendaciones	Categorización	Flujo de trabajo
1.1.16 Revisar las asignaciones de derechos de los usuario y los permisos asignados a la política de grupo	Postura	Cuentas de punto final - Fortalecimiento
1.1.17 Documentar el acceso de terceros al entorno	Postura	Acceso externo
Etapas de Fortalecimiento - Recomendaciones de cuentas y credenciales		
1.2.1 Aprovechar el grupo de seguridad de usuarios protegidos para cuentas privilegiadas	Fortalecimiento	Cuentas - Fortalecimiento
1.2.2 Fortalecer el acceso a las cuentas de servicio	Fortalecimiento	Cuentas - Fortalecimiento
1.2.3 Credenciales seguras cuando se utilizan para una conectividad de escritorio remoto	Fortalecimiento	Cuentas - Fortalecimiento
1.2.4 Fortalecer las capacidades para que las cuentas locales se aprovechen para la autenticación remota	Fortalecimiento	Cuentas de punto final - Fortalecimiento
1.2.5 Deshabilitar la autenticación WDigest en los puntos finales	Fortalecimiento	Cuentas de punto final - Fortalecimiento
1.2.6 Deshabilitar la autenticación WDigest en los puntos finales	Fortalecimiento	Punto final - Fortalecimiento
Etapas de Fortalecimiento - Recomendaciones de puntos finales		
1.3.1 Restringir las comunicaciones de salida de los servidores	Fortalecimiento	Servidor - Fortalecimiento
1.3.2 Fortalecer las rutas comunes de la conectividad del movimiento lateral	Fortalecimiento	Punto final - Fortalecimiento
1.3.3 Fortalecimiento de comunicación remota de WinRM/PowerShell	Fortalecimiento	Punto final - Fortalecimiento
1.3.4 Fortalecer el uso del cliente del escritorio remoto en	Fortalecimiento	Punto final - Fortalecimiento
1.3.5 Imponer el reprocesamiento automatizado de las políticas de grupo	Fortalecimiento	Punto final - Fortalecimiento
1.3.6 Deshabilitar SMB v1.0	Fortalecimiento	Punto final - Fortalecimiento
Etapas de Fortalecimiento - Red Hat Enterprise Linux		
1.4.1 Habilitar el registro centralizado	Fortalecimiento de Linux	Registro y monitoreo - Visibilidad
1.4.2 Configurar la auditoría del sistema	Fortalecimiento de Linux	Registro y monitoreo - Visibilidad
1.4.3 Configurar el registro de fecha de la ejecución de la bitácora en el historial Shell	Fortalecimiento de Linux	Registro y monitoreo - Visibilidad

Recomendaciones	Categorización	Flujo de trabajo
1.4.4 Habilitar la grabación de sesiones	Fortalecimiento de Linux	Registro y monitoreo - Visibilidad
1.4.5 Imponer contraseñas seguras	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Cuentas
1.4.7 Cuentas seguras del sistema	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Cuentas
1.4.8 Imponer una máscara predeterminada de archivo	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL – Sistema de archivos
1.4.9 Habilitar funciones	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - SO
1.4.10 Proteger el servicio SSH	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL – Servicios
1.4.11 Limitar los puertos abiertos y los servicios	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL – Servicios
1.4.12 Revisar los Cron Jobs	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL – Servicios
1.4.13 Revisar y documentar cuentas privilegiadas	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Cuentas
1.4.14 Identificar y revisar los ejecutables SUID	Postura	Fortalecimiento del servidor RHEL - Cuentas
1.4.15 Monitoreo de integridad de archivos (FIM)	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL – Sistema de archivos
1.4.16 Eliminar los shells innecesarios o no utilizados de los sistemas Linux	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - SO
1.4.17 Implementar la gestión centralizada de identidad	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - SO
1.4.18 Actualizar el sistema operativo a la última versión, instalar parches de seguridad	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Cuentas
Etapa dos: Erradicación - Contención		

Recomendaciones	Categorización	Flujo de trabajo
2.1.1 Bloquear las direcciones IP, los puertos y los sinkholes de nombres de dominio maliciosos	Contención	Cuentas de punto final - Fortalecimiento
2.1.2 Habilitar "Password is Required" en cuentas identificadas	Contención	Cuentas de punto final - Fortalecimiento
2.1.3 Habilitar "Sensitive account and cannot be delegated" para todas las cuentas privilegiadas identificadas	Contención	Cuentas de punto final - Fortalecimiento
2.1.4 Eliminar el atributo "Admin SDHolder" de todas las cuentas que no están en grupos privilegiados	Contención	Cuentas de punto final - Fortalecimiento
2.1.5 Restablecer las contraseñas e imponer la caducidad de la contraseña en cuentas privilegiadas	Contención	Cuentas de punto final - Fortalecimiento
2.1.6 Fortalecer los permisos para la persistencia de	Fortalecimiento	Punto final - Fortalecimiento
2.1.7 Mejorar el nivel de autenticación del LAN Manager para	Fortalecimiento	Punto final - Fortalecimiento
2.1.8 Limpiar y verificar los sistemas "accedidos"	Fortalecimiento	Punto final - Fortalecimiento
2.1.9 Asegurarse de que el programa de administración de vulnerabilidades se aplique a todos los hosts	Fortalecimiento	Punto final - Fortalecimiento
2.1.10 Asegurarse de que los servidores a los que se puede acceder desde el exterior estén	Fortalecimiento	Punto final - Fortalecimiento
Etapas tres: Mejoras estratégicas		
3.1.1 Verificar si se pueden aprovechar las reglas de reducción de la superficie del ataque (ASR)	Fortalecimiento	Punto final - Fortalecimiento
3.1.1 Revisar los objetos de la política de grupo	Fortalecimiento	Punto final - Fortalecimiento
3.1.3 Implementar estaciones de trabajo de acceso privilegiado para administradores	Fortalecimiento	Punto final - Fortalecimiento

Tabla 1: Resumen de recomendaciones

Recomendaciones para la postura y la preparación

Acción propuesta	Categorización	Flujo de trabajo
1.1.1 Revisar los ajustes de configuración de la auditoría de Windows	Postura	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>BanCoppel debe implementar la configuración de la Política de auditoría en los sistemas Windows como se describe a continuación. La configuración de la Política de auditoría, para los controladores de dominio del directorio activo, se enlistan en la Tabla 2. La configuración de la Política de auditoría para todos los demás puntos finales (controladores que no son de dominio) se enlistan en la Tabla 3. Sólo se debe aplicar la configuración de Auditoría o Política de auditoría avanzada a un sistema.</p> <p>Además, BanCoppel deberá aumentar el tamaño máximo de los archivos críticos de la bitácora de eventos en los sistemas Windows para permitir un año de retención de bitácoras. El tamaño máximo de cada archivo de bitácora se puede determinar analizando la retención de la bitácora en cada archivo a lo largo del tiempo. A corto plazo, Mandiant recomienda configurar el tamaño máximo de la bitácora con los valores de la Tabla 4 después de evaluar el espacio disponible en disco en los sistemas afectados.</p> <p>BanCoppel debe reenviar todos los eventos desde los archivos críticos de bitácora, en controladores de dominio y servidores, a un dispositivo central de agregación de bitácoras, donde deben ser analizados y retenidos durante, al menos, un año.</p> <p>Los archivos críticos de bitácora incluyen:</p> <ul style="list-style-type: none"> • Seguridad • Aplicación • Sistema • TaskScheduler/Operational • PowerShell/Operational • PowerShell de Windows <p>Utilizando la Configuración avanzada de la política de auditoría (<i>Computer Configuration > Políticas > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies</i>), Bancoppel debe asegurarse de que el registro esté configurado en los puntos finales basados en Windows para los eventos documentados en la Tabla 2 y la Tabla 3.</p> <p>Nota: Asegúrese de que la configuración de "<i>Computer Configuration > Políticas > Windows Settings > Security Settings > Local Policies > Security Options > Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings</i>" está configurada como "Enabled".</p> <p>Nota: Si se ajusta alguna configuración avanzada de la política de auditoría en un GPO ANTES de habilitar e imponer la opción "<i>Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings</i>" la configuración avanzada de la política de auditoría no se aplicará y no se mostrará como configurado por medio de la salida RSOP, gpresult o auditpol. La "<i>Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings</i>" debe configurarse PRIMERO y, posteriormente, se puede definir la configuración específica de la auditoría. Si esto no se completó en el orden correcto, cualquier configuración de la política de auditoría, previamente configurada, deberá ser denegada y, posteriormente, reconfigurada después de imponer primero la opción "<i>Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings</i>".</p>		

Acción propuesta		Categorización	Flujo de trabajo
Ajustes recomendados de la auditoría del controlador de dominio			
Categoría	Subcategoría	Ajuste efectivo	
Inicio de sesión de cuenta	Auditoría de validación de credenciales	Exitoso, fallido	
Inicio de sesión de cuenta	Auditoría del servicio de autenticación de Kerberos	Exitoso, fallido	
Inicio de sesión de cuenta	Auditoría de operaciones de tickets de servicio de Kerberos	Exitoso, fallido	
Administración de cuentas	Auditoría de gestión de cuentas informáticas	Exitoso, fallido	
Administración de cuentas	Auditoría de otros eventos de gestión de cuentas	Exitoso, fallido	
Administración de cuentas	Auditoría de la gestión del grupo de seguridad	Exitoso, fallido	
Administración de cuentas	Auditoría de la gestión de cuentas del usuario	Exitoso, fallido	
Seguimiento detallado	Auditoría de la actividad de DPAPI	Exitoso, fallido	
Seguimiento detallado	Auditoría de creación de procesos	Exitoso, fallido	
Acceso DS	Auditoría del acceso al servicio del directorio	Exitoso, fallido	
Acceso DS	Auditoría de cambios en el servicio del directorio	Exitoso, fallido	
Inicio y cierre de sesión	Auditoría de bloqueo de cuenta	Exitoso	
Inicio y cierre de sesión	Auditoría de cierre de sesión	Exitoso	
Inicio y cierre de sesión	Auditoría de inicio de sesión	Exitoso, fallido	
Inicio y cierre de sesión	Auditoría de inicio de sesión especial	Exitoso, fallido	

Acción propuesta		Categorización	Flujo de trabajo
Acceso a objetos	Auditoría del objeto de kernel	Exitoso	
Uso de privilegios	Auditoría del uso de los privilegios sensibles	Exitoso, fallido	
Cambio de política	Auditoría de cambios en la política de autenticación	Exitoso, fallido	
Cambio de política	Auditoría de cambios de la política de autorización	Exitoso, fallido	
Cambio de política	Auditoría de cambios de la política	Exitoso, fallido	
Sistema	Auditoría del controlador IPsec	Exitoso, fallido	
Sistema	Auditoría de cambios del estado de seguridad	Exitoso, fallido	
Sistema	Auditoría de extensión del sistema de seguridad	Exitoso, fallido	

Tabla 2: Configuración de la política de auditoría del controlador de dominio

Ajustes recomendados de la auditoría del punto final (estación de trabajo/servidor)

Categoría	Subcategoría	Ajuste efectivo
Inicio de sesión de cuenta	Auditoría de validación de credenciales	Exitoso
Administración de cuentas	Auditoría de otros eventos de gestión de cuentas	Exitoso, fallido
Administración de cuentas	Auditoría de la gestión del grupo de seguridad	Exitoso, fallido
Administración de cuentas	Auditoría de la gestión de las cuentas de usuario	Exitoso, fallido
Seguimiento detallado	Auditoría de la actividad de DPAPI	Exitoso, fallido
Seguimiento detallado	Auditoría de creación de procesos	Exitoso

Acción propuesta		Categorización	Flujo de trabajo
Acceso DS	Auditoría del acceso al servicio del directorio	Exitoso, fallido	
Inicio y cierre de sesión	Auditoría de bloqueo de cuenta	Exitoso	
Inicio y cierre de sesión	Auditoría de cierre de sesión	Exitoso	
Inicio y cierre de sesión	Auditoría de inicio de sesión	Exitoso, fallido	
Inicio y cierre de sesión	Auditoría de inicio de sesión especial	Exitoso, fallido	
Acceso a objetos	Auditoría de otros eventos de acceso a objetos	Exitoso	
Acceso a objetos	Auditoría de objetos de kernel	Exitoso	
Cambio de política	Auditoría de cambio de política	Exitoso, fallido	
Cambio de política	Auditoría de cambios en la política de autenticación	Exitoso, fallido	
Sistema	Auditoría de cambio del estado de seguridad	Exitoso, fallido	
Sistema	Auditoría de extensión del sistema de seguridad	Exitoso	
Sistema	Auditoría de la integridad del sistema	Exitoso, fallido	

Tabla 3: Configuración de la política de auditoría de los puntos finales (no controladores de dominio)

Con la siguiente configuración de política de grupo, BanCoppel debe configurar el tamaño de la bitácora de eventos para hacer referencia a la configuración capturada en la Tabla 4.

- Computer Configuration > Policies > Administrative Templates > Windows Components > Event Log Service > (Application|Security|System|OtherEventLogs) > Specify the maximum log size (KB)
 - 2GB = 2,097,152 KB
 - 1GB = 1,048,576 KB

SO	Aplicación	Seguridad	Sistema	PowerShell	TaskScheduler
Windows 7+	1GB	2GB	1GB	1GB	150MB

Acción propuesta			Categorización		Flujo de trabajo
Windows Server 2008+	1GB	2GB	1GB	1GB	150MB
<p><i>Tabla 4: Tamaños máximos recomendados de bitácora</i></p> <p>Además, para configurar los tamaños máximos de la bitácora de eventos en los puntos finales individuales, esto puede lograrse por medio del registro local (Figura 1) o mediante la línea de comandos (Figura 2).</p> <p>HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\ (Application Security System OtherEventLogs)</p> <p>REG_DWORD = "MaxSize"</p> <p>The value must be set to a multiple of 64K for a System, Application, or Security log</p> <p><i>Figura 1: Llave de registro para configurar el tamaño máximo de la bitácora de eventos para un punto final</i></p> <p>wevtutil sl Security /ms:2147483648</p> <p><i>Figura 2: Método de línea de comando para configurar el tamaño máximo de la bitácora de eventos de seguridad para un punto final (ejemplo de 2 GB)</i></p> <p>Para verificar que se imponga la configuración, el comando de PowerShell, al que se hace referencia en la Figura 3, se puede ejecutar en un punto final.</p> <p>Get-winevent -listlog Security</p> <p><i>Figura 3: Comando para verificar el tamaño máximo configurado para una bitácora de eventos</i></p> <p>Nota: La auditoría de acceso a objetos puede producir un número excesivo de eventos y afectar el rendimiento del sistema. Sin embargo, puede ser útil capturar esta información para los recursos clave en el sistema de archivos (ej. la carpeta Windows\System32). Por lo tanto, la auditoría de acceso a objetos debe evaluarse caso por caso según el sistema, la función, los recursos y otros factores clave.</p>					
Justificación					
<p>La captura de detalles adicionales en la bitácora mejorará la capacidad de BanCoppel para determinar qué actividad ocurrió en un punto final. Este nivel de visibilidad también permite a BanCoppel mejorar la detección de eventos sospechosos al generar alertas basadas en patrones predefinidos de una actividad común de los atacantes. Esta información debe centralizarse en un SIEM para permitir el análisis en caso de que las bitácoras de eventos sean eliminadas.</p>					

Acción propuesta	Categorización	Flujo de trabajo
1.1.2 Asegurar el registro de eventos de la creación de procesos de línea de comandos	Postura	Registro y monitoreo - Visibilidad
Detalles de la recomendación <p>BanCoppel debe asegurarse de que el seguimiento de procesos esté habilitado en las bitácoras de eventos de seguridad (ID de evento 4688) para todos los puntos finales y que el historial de la línea de comandos se registre para dichos eventos en cada punto final.</p> <p>Esta función se puede habilitar instalando KB3004375 (https://www.microsoft.com/en-us/download/details.aspx?id=45627) y configurando los ajustes de la política de grupo que se indica a continuación:</p> <ul style="list-style-type: none"> Computer Configuration > Políticas > Administrative Templates > System > Audit Process Creation > Include command line in process creation events <p>Para obtener información adicional, consultar:</p> <ul style="list-style-type: none"> https://support.microsoft.com/en-us/kb/3004375 https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing 		
Justificación <p>La captura de eventos de creación de procesos mejorará la probabilidad para determinar qué hizo un atacante en un punto final. La mejora de la visibilidad de los argumentos de la línea de comandos que se utilizan para iniciar procesos proporciona una mejor detección y correlación de condiciones las cuales pueden ser maliciosas o sospechosas.</p> <p>Este nivel de visibilidad también permite a BanCoppel mejorar la detección de eventos sospechosos al generar alertas basadas en patrones predefinidos de actividad común de los atacantes.</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.1.3 Implementar Microsoft System Monitor (Sysmon) en sistemas clave	Postura	Registro y monitoreo - Visibilidad
Detalles de la recomendación <p>BanCoppel deberá implementar Microsoft Systems Monitor (Sysmon) en los sistemas clave (los tipos de ejemplo se enlistan a continuación). En cada tipo de sistema, BanCoppel debe configurar Sysmon para registrar eventos como se especifica en la Tabla 5 y, cuando sea posible, la bitácora de eventos debe enviarse a un sistema central de agregación de bitácoras.</p> <p>De forma predeterminada, los eventos de Sysmon se registran en la bitácora de eventos Microsoft-Windows-Sysmon/Operational.</p> <p>Además, BanCoppel debe configurar Sysmon para utilizar cualquier algoritmo de hash (MD5, SHA1, SHA256) que coincida con los datos recolectados por otros productos y soluciones de seguridad.</p> <p>Los tipos de sistemas clave incluyen:</p>		

- Sistemas a los que un atacante accedió o que lo infectó
- Controladores de dominio
- Hosts de salto
- Servidores de base de datos
- Sistemas Windows orientados a Internet
- Sistemas que albergan o gobiernan el acceso a datos sensibles y críticos

ID	Etiqueta	Evento	Bitácora
1	ProcessCreate	Process Create	Si
2	FileCreateTime	File creation time	Si <i>Precaución al implementar esto en servidores de archivos tradicionales</i>
3	NetworkConnect	Network Connection Detected	Si
5	ProcessTerminate	Process Terminated	Si
6	DriverLoad	Driver Loaded	No
7	ImageLoad	Image Loaded	No
8	CreateRemoteThread	CreateRemoteThread Detected	No
9	RawAccessRead	RawAccessRead Detected	No
10	ProcessAccess	Process Accessed	No
11	FileCreate	File Created	Si <i>Precaución al implementar esto en servidores de archivos tradicionales</i>
12	RegistryEvent	Registry object added or deleted	No
13	RegistryEvent	Registry value set	No
14	RegistryEvent	Registry object renamed	No
15	FileCreateStreamHash	File stream created	No
17	PipeEvent	Named pipe created	No
18	PipeEvent	Named pipe connected	No
19	WMIEventFilter	WmiEventFilter Activity Detected	Si
20	WMIEventFilter	WmiEventConsumer Activity Detected	Si

21	WMIEventFilter	WmiEventConsumerToFilter Activity Detected	Si
22	DNSEvent	Process executes a DNS query	Si
23	FileDelete	A file was deleted	No

Tabla 5: Configuración de filtrado de eventos de Sysmon

Los eventos de Sysmon se crean en la siguiente bitácora de eventos:

- Microsoft-Windows-Sysmon/Operational

Para obtener información adicional relacionada con Sysmon, consultar:

- <https://technet.microsoft.com/en-us/sysinternals/sysmon>

Justificación

Sysmon es una herramienta gratuita de Microsoft Sysinternals la cual puede monitorear y registrar la actividad de los puntos finales.

La captura de eventos detallados en un punto final mejora la probabilidad para determinar lo que logró un atacante, además de mejorar la visibilidad de los parámetros y condiciones las cuales pueden ser maliciosas o sospechosas.

Los datos adicionales de la bitácora de eventos, proporcionados por Sysmon, otorgan al equipo de investigación y al equipo de operaciones de seguridad de BanCoppel datos valiosos para investigar la actividad de los atacantes.

Acción propuesta	Categorización	Flujo de trabajo
1.1.4 Imponer la auditoría para eventos de tareas programadas	Postura	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>En los sistemas Windows 7 (y superiores), de forma predeterminada, los eventos de las tareas programadas se registran en la bitácora de eventos “%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TaskScheduler%40operational.evtx”.</p> <p>Los ID comunes de eventos para revisión pueden incluir:</p> <ul style="list-style-type: none"> • 106 - Scheduled Task Created • 141 - Scheduled Task Deleted • 140 - Scheduled Task Updated <p>Al habilitar la configuración para “Audit Other Object Access Events” (<i>Computer Configuration > Políticas > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies</i>), los eventos de las tareas programadas también se pueden registrar en la bitácora de eventos de seguridad.</p> <p>Los ID relevantes de eventos para correlacionar (ej. SIEM Dashboard) y revisar (después de la base inicial y normalizar los datos) dentro de las bitácoras de eventos de seguridad incluyen:</p> <ul style="list-style-type: none"> • 4698 - Scheduled Task Created 		

- 4699 - Scheduled Task Deleted
- 4702 - Scheduled Task Updated

Los siguientes identificadores de eventos se pueden desactivar para reducir la cantidad de eventos que generan los sistemas (*Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies*):

- 5152 – Audit Filtering Platform Packet Drop
- 5157 – Audit Filtering Platform Connection

Para obtener información adicional, consultar:

- [https://technet.microsoft.com/en-us/library/dd772744\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd772744(v=ws.10).aspx)

Justificación

La captura de eventos de las tareas programados dentro de la bitácora de eventos de seguridad mejora la visibilidad de los eventos de las tareas programados las cuales ocurren en los sistemas en todo el entorno empresarial. Los atacantes comúnmente aprovechan las tareas programadas para la persistencia y para elevar los permisos para realizar funciones privilegiadas.

Este nivel de visibilidad también permite a BanCoppel mejorar la detección de eventos de tareas programadas (a escala) al generar alertas basadas en nombres de tareas programadas poco comunes, parámetros de línea de comandos sospechosos, además de alertar sobre binarios en rutas sospechosas que se invocan mediante una tarea programada.

Acción propuesta	Categorización	Flujo de trabajo
1.1.5 Habilitar PowerShell, la gestión remota de Windows y la auditoría de WMI	Postura	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>BanCoppel debe verificar que estén ejecutando (como mínimo) PowerShell v4.0 (preferiblemente v5.0 o superior) y que el registro de PowerShell esté configurado para admitir la recolección de artefactos forenses y de investigación. Deben desinstalarse las versiones inferiores de PowerShell para evitar los vectores de ataque de degradación.</p> <p>Para mejorar el registro y la retención de PowerShell, WinRM y WMI, será necesario que BanCoppel realice lo siguiente:</p> <ul style="list-style-type: none"> • Actualizar PowerShell a la versión 5.0 en todos los sistemas donde está instalado • Habilitar el registro del módulo de PowerShell • Habilitar el registro del bloqueo de guiones de PowerShell • Habilitar la transcripción de PowerShell • Configurar el tamaño máximo de la bitácora y el reenvío de bitácoras para los archivos de bitácora relacionados <p>Los archivos de bitácora relevantes incluyen:</p> <ul style="list-style-type: none"> • Microsoft-Windows-PowerShell/Operational • Microsoft-Windows-WinRM/Operational 		

- Microsoft-Windows-WMI-Activity/Operational

Para los sistemas Windows 7/8.1 / 2008/2012, la actualización de PowerShell, a la versión PowerShell 5.0 (recomendado), requiere:

- .NET 4.5
- Windows Management Framework (WMF) 4.0 (sólo Windows 7/2008)
- Windows Management Framework (WMF) 5.1
- Windows 7 y 2008 R2 deben actualizarse a Windows Management Framework (WMF) 4.0 antes de instalar WMF 5.1.

Para habilitar el registro del módulo de PowerShell:

1. Abrir la política de grupo y navegar hacia Computer Configuration > Políticas > Administrative Templates > Windows Components > Windows PowerShell.
2. Establecer “Turn on Module Logging” como “Enabled”.
3. En el panel de opciones, hacer clic en el botón para mostrar “Module Name”.
4. En la ventana “Module Names”, ingresar “*” para registrar todos los módulos.
5. Hacer clic en “OK” en la ventana “Module Names”.
6. Hacer clic en “OK” en la ventana “Module Logging”.

Para habilitar el registro del bloqueo de guiones de PowerShell:

1. Abrir la política de grupo y navegar hacia Configuration > Políticas > Administrative Templates > Windows Components > Windows PowerShell.
2. Establecer “Turn on PowerShell Script Block Logging” como “Enabled”.

Para habilitar la transcripción de PowerShell:

1. Abrir la política de grupo y navegar hacia Computer Configuration > Políticas > Administrative Templates > Windows Components > Windows PowerShell.
2. Establecer “Turn on PowerShell Transcription” como “Enabled”.
3. Marcar la casilla “Include invocation headers”.
4. De manera opcional, establecer un directorio centralizado de salida de transcripciones

Para deshabilitar PowerShell 2.0 en Windows 8.1 (y superior) y Windows Server 2012 (y superior):

- Desde un símbolo del sistema elevado (o dentro de un guion), ejecutar el siguiente comando:

```
DISM /online /disable-feature /featurename: Disable-WindowsOptionalFeature -Online -  
FeatureName MicrosoftWindowsPowerShellV2Root
```

Figura 4: Comando para deshabilitar PowerShell 2.0

- Desde una sesión elevada de PowerShell (o dentro de un guion de PowerShell), ejecutar el siguiente comando:

```
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root
```

Figura 5: Comando opcional para deshabilitar PowerShell 2.0

Justificación

La mejora de la visibilidad de la actividad de PowerShell proporciona una mejor detección y correlación de eventos que pueden ser maliciosos o sospechosos. Muchos atacantes ahora utilizan PowerShell para invocar

actividades maliciosas, moverse lateralmente y configurar mecanismos persistentes con el fin de aprovechar el acceso dentro de un entorno empresarial.

Incluso si las bitácoras detalladas de PowerShell no se reenvían a un SIEM para sistemas no críticos (ej. Estaciones de trabajo de usuario final, computadoras portátiles, servidores no críticos), la capacidad de capturar este nivel de información localmente en el punto final garantizará que el registro detallado este disponible en caso de una investigación.

Acción propuesta	Categorización	Flujo de trabajo
1.1.6 Mejorar el registro de DNS	Postura	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>BanCoppel debe asegurarse de que sus servidores internos de DNS estén configurados para registrar todas las consultas DNS provenientes de los puntos finales dentro de los dominios administrados.</p> <p>A partir de Windows Server 2012 R2, el registro y el diagnóstico mejorado de DNS están disponibles al instalar el registro de consultas y la revisión de auditoría de cambios (http://support.microsoft.com/kb/2956577). Específicamente, BanCoppel deberá considerar la implementación de bitácoras de eventos de auditoría y análisis de DNS para sus servidores DNS basados en Windows.</p> <p>Según Microsoft, el registro y el diagnóstico de DNS mejorados en Windows Server 2012 R2 (y versiones posteriores) incluyen eventos de auditoría de DNS y eventos de análisis de DNS. Las bitácoras de auditoría de DNS están habilitadas de forma predeterminada y no afectan significativamente el rendimiento del servidor DNS.</p> <p>Los registros analíticos de DNS no están habilitados de forma predeterminada y, por lo general, sólo afectarán el rendimiento del servidor DNS a tasas de consulta de DNS muy altas.</p> <ul style="list-style-type: none"> • Un servidor DNS que se ejecuta en hardware moderno el cual recibe 100,000 consultas por segundo (QPS) puede experimentar una degradación del rendimiento del 5% cuando los registros analíticos están habilitados. • No existe un impacto aparente en el rendimiento para las tasas de consulta de 50,000 QPS o menos. Sin embargo, siempre es recomendable supervisar el rendimiento del servidor DNS cuando se habilita un registro adicional. <p>Para obtener información adicional, consultar:</p> <p>https://technet.microsoft.com/en-us/library/dn800669(v=ws.11).aspx</p>		
Justificación		
<p>Tener visibilidad en tiempo real y datos históricos relacionados con las consultas de DNS proporciona a la organización un medio para rastrear y correlacionar los intentos de resolución de dominios sospechosos y potencialmente maliciosos.</p> <p>Durante una investigación, este tipo de datos es extremadamente valioso para rastrear y verificar los sistemas de origen, los cuales pueden tener una puerta trasera maliciosa instalada que está configurada para comunicarse con nombres de dominio específicos completamente calificados.</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.1.7 Mejorar el registro de Unix	Postura	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>BanCoppel debe verificar que los sistemas Unix estén configurados para registrar y retener información según las siguientes recomendaciones:</p> <ul style="list-style-type: none"> • Intentos de autenticación exitosos y fallidos, con prioridad en los servicios de red los cuales pueden proporcionar acceso administrativo (ej. SSH) • Uso de cualquier invocación de cuenta "root" o privilegiada, como el comando "su" (ej. Registro de "sudoers") • Conexiones entrantes denegadas (ej. aquellas bloqueadas por iptables) • Historial de comandos (ej. bitácoras del historial de bash shell), incluidos los registros de fechas <ul style="list-style-type: none"> ○ Los registros de fechas se pueden incluir con el historial de bash modificando el archivo predeterminado "bashrc" o "/etc/profile.d" (todos los usuarios) para incluir la siguiente sintaxis: <ul style="list-style-type: none"> ▪ <code>export HISTTIMEFORMAT="%d/%m/%y %T "</code> ○ Para obtener información adicional, consultar: https://www.unix-ninja[.]com/p/Adding_timestamps_to_Bash_history • Registro para el historial de ejecución de procesos (contabilidad) <ul style="list-style-type: none"> ○ Esto se puede lograr aprovechando auditd, psacct, o acct. • Gestión de usuarios o grupos, incluyendo: <ul style="list-style-type: none"> ○ Creación o modificación de cuenta ○ Creación o modificación de grupos ○ Modificación de la autorización (ej. modificación del archivo sudoers) ○ Creación o modificación de contraseña • Instalaciones de software • Ejecuciones de tareas programadas (ej. Cronjobs) • Binarios persistentes comunes y ubicaciones de inicio automático de servicios <ul style="list-style-type: none"> ○ cron ○ /etc/rc.d/init.d ○ /etc/bashrc ○ /home/<username>/.bash_profile ○ /etc/init/ <p>BanCoppel debe priorizar la identificación de servidores Unix o aquellos que brindan acceso administrativo para los sistemas que almacenan y procesan datos sensibles dentro del entorno. BanCoppel debe asegurarse de que las bitácoras del servidor se archiven y reenvíen a un SIEM para su almacenamiento, procesamiento y análisis fuera de línea.</p>		

Los archivos comunes de la bitácora de Unix, para su reenvío, se indican en la Tabla 6.

Archivo de bitácora	Descripción
/var/log/audit/audit.log	Eventos generados por auditd
/var/log/auth.log	Bitácoras de autenticación del sistema
/var/log/cron	Información sobre cron jobs iniciados por cron daemon
/var/log/dpkg.log	Bitácoras de instalación y eliminación de paquetes para dpkg
/var/log/faillog Failed authentication logs	Bitácoras de autenticaciones fallidas
/var/log/mail.err	Eventos creados por el servidor de correo
/var/log/maillog	
/var/log/mail.log	
/var/log/messages	Mensajes del sistema global, incluidos eventos de correo, cron, daemon, kern, auth, etc.
/var/log/samba/	Eventos creados por Samba, una aplicación que permite compartir archivos y otros
/var/log/secure	Eventos de autenticación y autorización
/var/log/sudo	Eventos de autenticación y autorización
/var/log/syslog	Eventos que se envían a la función de registro de syslog
/var/log/wtmp	Eventos de inicio de sesión
/var/log/utmp	
/var/log/yum.log	Bitácoras de los eventos de instalación del paquete Yum
RHEL / Red Hat / CentOS / Fedora Linux Apache access logs – /var/log/httpd/access_log	Bitácoras de acceso de Apache
Debian / Ubuntu Linux Apache access logs – /var/log/apache2/access.log	

FreeBSD Apache access logs –
/var/log/httpd-access.log

Tabla 6: Archivos comunes de la bitácora de Unix

Justificación

Los datos de bitácora completos, consistentes y centralizados pueden empoderar significativamente a una organización para detectar e investigar la actividad maliciosa de manera oportuna.

Acción propuesta	Categorización	Flujo de trabajo
1.1.8 Verificar el reenvío de fuentes de bitácora críticas al SIEM	Postura	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>BanCoppel debe verificar y validar que las bitácoras críticas y las fuentes de datos se recolecten y agreguen dentro de un SEIM. El SIEM debe almacenar al menos un año de datos de bitácora con capacidad de búsqueda.</p> <p>Como mínimo, BanCoppel debe asegurarse de que las siguientes fuentes de datos se almacenen y agreguen dentro de su SIEM:</p> <ul style="list-style-type: none"> • Bitácoras del cortafuegos/NetFlow y proxy web • Bitácoras de proxy inverso/WAF • Bitácoras del balanceador de carga (incluidos los encabezados HTTP X-Forwarded-For) • Intentos de resolución de DNS (todos los servidores DNS, en cada dominio) • Bitácoras DHCP (todos los servidores DHCP, en cada dominio) <ul style="list-style-type: none"> ○ Ubicación predeterminada para Windows = "%windir%\System32\Dhcp" • Bitácoras de autenticación de VPN, incluida la IP de origen y el nombre de host (todos los dispositivos VPN) • Bitácoras de eventos de seguridad (controladores de dominio, servidores y sistemas críticos) • Bitácoras de autenticación de Citrix/VDI • Bitácoras de acceso y autenticación de Exchange • Bitácoras de autenticación web (IIS, Apache) de sistemas y servicios críticos • Bitácoras de la solución de administración de cuentas privilegiadas (PAM) • Bitácoras de portal/consola administrativa de MFA • Bitácoras de tecnología de detección basada en antivirus/host 		
Justificación		

Los datos de bitácora completos, consistentes y centralizados pueden empoderar significativamente a una organización para detectar e investigar la actividad maliciosa de manera oportuna.

Acción propuesta	Categorización	Flujo de trabajo
1.1.9 Imponer la auditoría para objetos de la política de grupo (GPO)	Postura	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>BanCoppel deberá considerar la aplicación de auditorías avanzadas en los controladores de dominio para registrar y monitorear eventos relacionados con las creaciones, modificaciones y eliminaciones de GPO.</p> <p>BanCoppel primero deberá asegurarse de que se imponga la auditoría “Audit Directory Service Changes” para los controladores de dominio.</p> <ul style="list-style-type: none"> Computer Configuration > Políticas > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > DS Access > Audit Directory Service Changes <ul style="list-style-type: none"> Exitoso, fallido <p>Con ADSIEdit, la auditoría del grupo “Everyone” deberá configurarse para las siguientes acciones (Figura 6):</p> <ul style="list-style-type: none"> Create groupPolicyContainer objects Write Modify Permissions Write versionNumber <p>Para configurar la auditoría para el grupo “Everyone”:</p> <ol style="list-style-type: none"> ADSI Edit > Conectarse al contexto de nomenclatura predeterminado. Navegar hacia “CN=System”. Navegar hacia “CN=Políticas”. Hacer clic derecho y seleccionar la pestaña “Properties” > click the “Security”. Hacer clic en la pestaña “Advanced” > “Auditing”. <ul style="list-style-type: none"> Add the Principal "Everyone" Type: "Success" Applies to: Seleccionar “This object and Descendant objects" Permissions: Seleccionar las siguientes casillas de verificación: <ul style="list-style-type: none"> Create groupPolicyContainer objects Delete Modify Permissions Write versionNumber 		

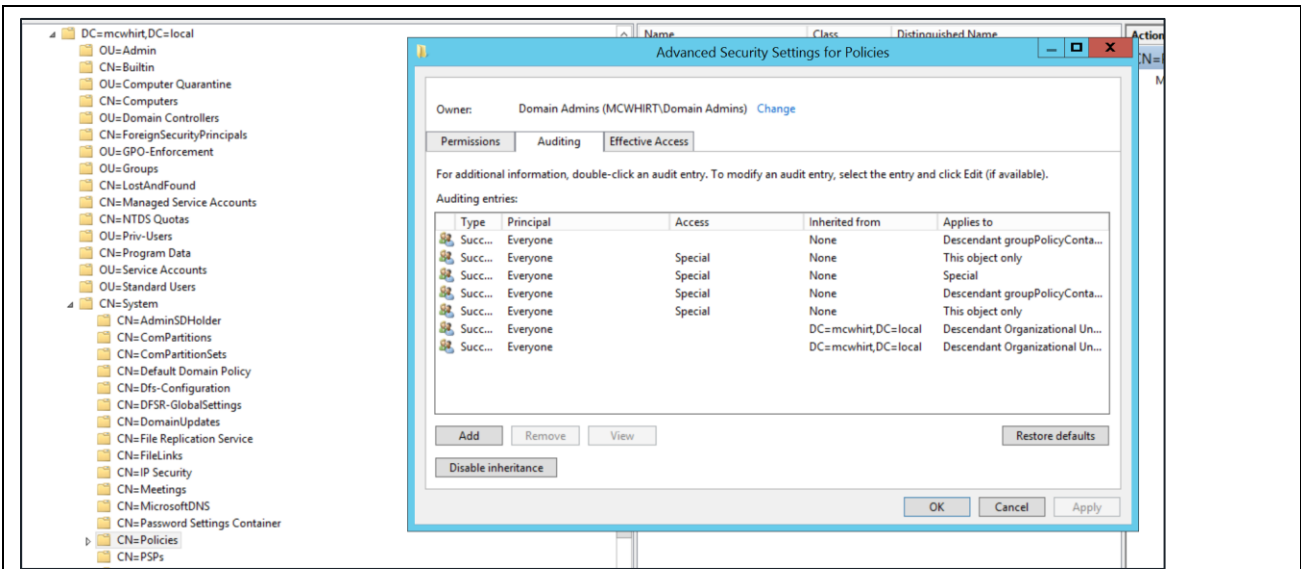


Figura 6: Requisitos de permisos dentro del contenedor de políticas en ADSIEdit

Una vez completado, los siguientes ID de eventos (EID) deben registrarse en la bitácora de eventos de seguridad en los controladores de dominio:

- 5137 – Group policy creations
- 5136 – Group policy modifications, links, unlinks
- 5141 – Group policy deletions

Además, BanCoppel puede aprovechar el cmdlet de PowerShell que se indica en la Figura 7 para obtener una lista de todos los GPO, el cual incluirá los registros de fechas creados y modificados para cada GPO. El resultado se puede revisar de forma recurrente para determinar si se ha creado o modificado algún GPO.

```
get-gpo -all | export-csv -path $outputdir\GPO-Listing-All.csv -NoTypeInfoation
```

Figura 7: Cmdlet de PowerShell para revisar cualquier GPO creado o modificado

Justificación

La captura de eventos relevantes de auditoría para los GPO mejora la visibilidad y la detección de la actividad la cual podría afectar la postura de seguridad de un punto final, o cuando los GPO se aprovechan para la propagación masiva de malware dirigido a puntos finales.

Acción propuesta	Categorización	Flujo de trabajo
1.1.10 Identificar y documentar las cuentas privilegiadas basadas en dominios	Postura	Directorio activo – Preparación de fortalecimiento
Detalles de la recomendación		

BanCoppel debe revisar y documentar las cuentas privilegiadas en sus dominios del directorio activo y aquellas administradas por contratistas externos (si corresponde). La documentación debe incluir información explícita sobre el alcance de las cuentas privilegiadas y los datos necesarios para identificar las cuentas heredadas, inactivas e innecesarias. Cualquier cuenta que se identifique como ya no necesaria, obsoleta o con acceso privilegiado por encima de lo necesario para las operaciones diarias debe desactivarse y eliminarse de cualquier grupo privilegiado.

La documentación de la cuenta privilegiada debe incluir a los miembros de los grupos a los que se les haya delegado acceso privilegiado dentro del dominio y a los miembros de todos los grupos privilegiados integrados, incluidos los siguientes:

- Operadores de cuentas
- Administradores
- Operaciones de respaldo
- Administradores de DNS
- Administradores de dominio
- Administradores de empresas
- Administradores de esquemas
- Operadores de servidor

Para identificar el alcance de las cuentas privilegiadas residentes en grupos privilegiados basados en dominios predeterminados, se pueden aprovechar los cmdlets de PowerShell registrados en la Figura 8.

```
get-ADGroupMember -Identity "Domain Admins" -Recursive
get-ADGroupMember -Identity "Enterprise Admins" -Recursive
get-ADGroupMember -Identity "Schema Admins" -Recursive
get-ADGroupMember -Identity "Administrators" -Recursive
get-ADGroupMember -Identity "Account Operators" -Recursive
get-ADGroupMember -Identity "Backup Operators" -Recursive
get-ADGroupMember -Identity "DNS Admins" -Recursive
get-ADGroupMember -Identity "Cert Publishers" -Recursive
get-ADGroupMember -Identity "Print Operators" -Recursive
get-ADGroupMember -Identity "Server Operators" -Recursive
get-ADGroupMember -Identity "Denied RODC Password Replication Group" -Recursive
get-ADUser -Filter {(AdminCount -eq 1) -And (Enabled -eq $True)}
```

Figura 8: Cmdlets de PowerShell para identificar la pertenencia a grupos privilegiados basados en dominios predeterminados


Justificación

Para eliminar el acceso de los atacantes al entorno y fortalecer el entorno contra futuros ataques, BanCoppel deberá cambiar todas las contraseñas (a escala empresarial) y reducir el privilegio de las cuentas.

La identificación de cuentas privilegiadas ayudará a BanCoppel a coordinar las actividades de restablecimiento de contraseñas y planificar la implementación de una gestión mejorada de cuentas privilegiadas y controles de refuerzo adicionales.

Acción propuesta	Categorización	Flujo de trabajo
1.1.11 Identificar y documentar cuentas de servicio basadas en dominios	Postura	Directorio activo – Preparación de fortalecimiento
Detalles de la recomendación		
<p>BanCoppel debe revisar y documentar las cuentas de servicio basadas en dominios en sus dominios del directorio activo y aquellas administradas por sus contratistas externos (si corresponde).</p> <p>La documentación debe, como mínimo, incluir la siguiente información relativa a cada cuenta de servicio:</p> <ul style="list-style-type: none"> • Nombre de la cuenta • Función de cuenta • Propietario comercial y técnico del sistema, la aplicación o la cuenta • Sistema y aplicación que utiliza la cuenta • Proceso para cambiar la contraseña de la cuenta • Nivel de privilegio o acceso <p>Para comenzar a identificar las cuentas de servicio residentes en el entorno, se puede aprovechar el cmdlet de PowerShell registrado en la Figura 9. Este cmdlet identificará todas las cuentas que no sean de computadora configuradas con un nombre principal de servicio (SPN), que probablemente se correlacione con las cuentas de servicio.</p>		
<pre>get-aduser -filter {(ServicePrincipalName -like "*")} Select-Object name,samaccountname,sid,enabled,DistinguishedName</pre>		
<p><i>Figura 9: Comando de PowerShell para identificar cuentas, que no son de computadora, con SPN</i></p> <p>Nota: Este cmdlet no generará una lista completa de todas las cuentas de servicio. Es probable que se requieran pasos adicionales para identificar todas las cuentas de servicio potenciales dentro de un entorno.</p>		
Justificación		
<p>Para eliminar el acceso de los atacantes al entorno y fortalecer el entorno contra futuros ataques, BanCoppel deberá cambiar todas las contraseñas (a escala empresarial) y reducir el privilegio de las cuentas.</p> <p>Revisar y documentar las cuentas de servicio ayudará a BanCoppel a coordinar el cambio de contraseñas de las cuentas de servicio durante el evento de erradicación. Además, la revisión puede identificar cuentas de servicio configuradas con privilegios innecesarios dentro de los entornos.</p>		

Acción propuesta	Categorización	Flujo de trabajo
------------------	----------------	------------------

1.1.12 Identificar y documentar cuentas con contraseñas sin caducidad	Postura	Directorio activo – Preparación de fortalecimiento
Detalles de la recomendación		
<p>BanCoppel debe revisar las cuentas basadas en dominios con contraseñas sin caducidad. Es probable que estas cuentas se correlacionen con cuentas de servicio, aplicaciones o privilegiadas, las cuales deberían estar dentro del alcance si se requiere un restablecimiento de contraseña empresarial.</p> <p>Para identificar una lista de cuentas basadas en dominio con contraseñas sin caducidad, se puede utilizar el cmdlet de PowerShell que se indica en la Figura 10.</p>		
<pre>get-ADUser -Filter {PasswordNeverExpires -eq \$true}</pre>		
<p><i>Figura 10: Cmdlet de PowerShell para identificar cuentas basadas en dominios con contraseñas sin caducidad</i></p> <p>Adjuntos:</p> 		
Justificación		
<p>Para eliminar el acceso de los atacantes al entorno y fortalecer el entorno contra futuros ataques, BanCoppel deberá cambiar todas las contraseñas (a escala empresarial), incluidas las cuentas configuradas con contraseñas sin caducidad.</p> <p>La identificación y documentación proactiva de cuentas basadas en dominios con contraseñas sin caducidad ayudará a BanCoppel a planear y coordinar los cambios de contraseña para estas cuentas. Además, la revisión proactiva probablemente identificará las cuentas que no necesitan configurarse con contraseñas sin caducidad y se pueden configurar para imponer una contraseña rotada de forma predefinida.</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.1.13 Revisar las políticas de contraseña y los controles de autenticación	Postura	Directorio activo – Preparación de fortalecimiento
Detalles de la recomendación		
<p>Si el nivel funcional del dominio actual es Windows Server 2008 (o superior), BanCoppel debe configurar varias políticas de contraseñas, según los siguientes requisitos (consultar la Tabla 7).</p> <p>Nota: Si el nivel funcional de dominio actual de BanCoppel es Windows Server 2003, no se admiten varias políticas de contraseña de dominio y se requiere una actualización a un nivel funcional de dominio de Windows Server 2008 (o superior)</p> <ul style="list-style-type: none"> Cuentas de usuario estándar (AD, LDAP, RADIUS/VPN): 		

- Requiere un mínimo de contraseñas de 15 caracteres. Esta longitud garantiza que el hash del LAN Manager (LM) heredado no se pueda almacenar; las contraseñas de 14 o menos caracteres se dividen en dos cadenas de siete caracteres y, posteriormente, se procesan para formar el hash LM. Las contraseñas más largas son más resistentes a los intentos de craqueo por fuerza bruta contra los hashes.
- Requiere que las contraseñas se cambien cada 90 días.
- Requiere que la antigüedad mínima de la contraseña sea de al menos un día.
- Bloquear cuentas después de un máximo de 10 intentos fallidos de inicio de sesión en 60 minutos.
- Restablecer las cuentas bloqueadas después de 30 minutos.
- Evitar que los usuarios reutilicen contraseñas. El historial de contraseñas debe configurarse para recordar las últimas 10 contraseñas para reducir la reutilización de contraseñas.
- Habilitar “Passwords must meet complexity requirements”.
- Cuentas de usuario de dominio privilegiado (administrador de dominio, administrador de empresa, AD, LDAP, RADIUS/VPN):
 - Requiere un mínimo de contraseñas de 20 caracteres.
 - Los mismos requisitos enlistados para las cuentas de usuario habituales.
- Cuentas de servicio y aplicación (AD, LDAP):
 - Requiere un mínimo de contraseñas de 30 caracteres.
 - Los mismos requisitos enlistados para las cuentas de usuario habituales

Política	Tipo de cuenta		
	Usuario estándar	Cuenta privilegiada	Cuenta de servicio
Duración del bloqueo de la cuenta	30 minutos	0 (indefinido)	0 (indefinido)
Umbral del bloqueo de la cuenta	10 intentos	5 intentos	5 intentos
Imponer el historial de contraseñas	24 contraseñas	24 contraseñas	24 contraseñas
Antigüedad máxima de la contraseña	90 días	60 días <i>Si se utiliza tecnología PAM, esto se puede reducir a 24 horas.</i>	120 días
Antigüedad mínima de la contraseña	1 día	1 día	1 día
Longitud mínima de la contraseña	15 caracteres	20 caracteres	30 caracteres

La contraseña debe cumplir los requisitos de complejidad	Habilitado	Habilitado	Habilitado
Restablecer el contador de bloqueo después de	60 minutos	60 minutos	60 minutos
Almacenar las contraseñas mediante un cifrado reversible	Deshabilitado	Deshabilitado	Deshabilitado

Tabla 7: Recomendaciones de política de contraseñas

Si no se puede aplicar una contraseña de 15 caracteres para cuentas de usuario estándar, como mínimo, los hash del LAN Manager (LM Hash) deben deshabilitarse explícitamente para que no se almacenen en un sistema. Esto se puede lograr mediante la siguiente configuración de política de grupo:

- Computer Configuration > Políticas > Windows Settings > Security Settings > Local Policies > Security Options
 - Network security: Do not store LAN Manager hash value on next password change
 - Habilitado

Para imponer (como mínimo) una contraseña de 15 caracteres dentro del directorio activo, BanCoppel deberá aprovechar las políticas de contraseñas detalladas (dentro del Centro de administración del directorio activo). El siguiente ejemplo muestra la configuración de esta configuración (por medio de Server 2012 o superior) para cuentas de usuario estándar.

1. <DomainName> > System > Password Settings Container
2. Hacer clic derecho en > New > Password Settings
3. Una vez que el Objeto de configuración de contraseña (PSO) se haya actualizado y configurado en función de los parámetros de contraseña requeridos (y establecido con una precedencia de "1" o superior), aplicar al grupo "Domain Users".
4. La nueva política se aplicará a los usuarios en el siguiente cambio de contraseña programado.

Se pueden configurar y aplicar ajustes detallados similares a los grupos de seguridad del directorio activo los cuales contienen cuentas privilegiadas, de servicio y específicas de la aplicación.

Note: Si se aplican varias políticas detalladas a la misma cuenta, gana la política que tenga el valor de precedencia más bajo.

Los nuevos cambios entrarán en vigor para cada cuenta la siguiente vez que se cambie la contraseña de la cuenta, por lo que es importante cambiar esta configuración antes de un restablecimiento de contraseña coordinado.

Para entornos de Windows Server 2008, ADSIEdit se puede utilizar para crear políticas similares.

Para la replicación de contraseñas y cuentas del directorio activo local con Azure Active Directory, la política de contraseñas local se replica (incluida la nueva configuración de longitud máxima de contraseña que se impone mediante las políticas de contraseñas detalladas); por lo tanto, ya no se impondrá la configuración predeterminada para una longitud máxima de contraseña de "16" para Azure Active Directory.

Para obtener información adicional sobre las políticas de contraseñas detalladas, consultar:

<https://blogs.technet.microsoft.com/canitpro/2013/05/29/step-by-step-enabling-and-using-fine-grained-password-policies-in-ad/>

Justificación

Para fortalecer aún más el entorno y minimizar los riesgos de robo de credenciales y escalación de privilegios, la política actual de contraseñas debe actualizarse con controles más estrictos.

Acción propuesta	Categorización	Flujo de trabajo
1.1.14 Identificar y revisar el alcance de las cuentas con permisos administrativos locales	Postura	Cuentas de punto final - Fortalecimiento
Detalles de la recomendación		
<p>BanCoppel debe identificar y revisar el alcance de las cuentas que tienen permisos administrativos locales en los puntos finales. Antes y durante el evento de remediación, se recomienda que el alcance de las cuentas que tienen permisos administrativos locales permitidos en los puntos finales se reduzca en los entornos de dominio administrados.</p> <p>Antes de imponer esta restricción, BanCoppel debe comprender completamente los impactos de eliminar este nivel de acceso y documentar y rastrear todos los sistemas y excepciones de las cuentas donde el modelo de imposición centralizado no se puede implementar. Para cada cuenta y el alcance correlativo de los sistemas donde se requieren permisos administrativos locales, BanCoppel debe asegurarse de que la aprobación y la aceptación del riesgo se documenten y se rastreen de acuerdo con las políticas de organización y seguridad.</p> <p>Con SCCM, el inventario de cuentas con permisos de administración local se puede recolectar haciendo referencia al siguiente enlace:</p> <p>https://blogs.technet.microsoft.com/sudheesn/2014/12/12/collect-hardware-inventory-of-local-admins/</p> <p>Con PowerShell, esto se puede programar para recuperar una lista de cuentas administrativas locales (por sistema). El método de guiones de PowerShell se basará en WMI, WinRM o ADSI (RPC y DCOM), por lo que se requerirán los puertos necesarios y el alcance de acceso para recuperar la información.</p>		
Justificación		
<p>El alcance de las cuentas con permisos administrativos locales debe reducirse en un entorno empresarial. Para minimizar el impacto y las posibles interrupciones operativas, primero se debe recolectar y revisar una lista de cuentas con permisos administrativos locales para determinar el alcance del impacto para eliminar y restringir el acceso privilegiado local en los puntos finales.</p>		

Acción propuesta	Categorización	Flujo de trabajo
------------------	----------------	------------------

1.1.15 Documentar la implementación y la cobertura de las herramientas de seguridad del antivirus y el punto final	Postura	Punto final – Preparación de fortalecimiento
Detalles de la recomendación		
<p>BanCoppel debe revisar el antivirus existente y la implementación de la herramienta de seguridad basada en el host (cada dominio) realizando las siguientes acciones:</p> <ul style="list-style-type: none"> • Documentar la implementación de la herramienta de seguridad basada en el host y en el antivirus, incluido el alcance de la implementación, la versión del software, el mecanismo de implementación, la configuración de detección, la frecuencia de actualización de la firma/IOC y el acceso administrativo y la configuración para cada plataforma de tecnología de back-end. • Revisar la configuración y los mecanismos de alerta para las infecciones y detecciones de malware identificadas y asegurarse de que exista la visibilidad adecuada y los canales de notificación para las alertas de alta fidelidad generadas desde cada plataforma tecnológica. • Identificar y mitigar problemas de configuración, los cuales incluyen: <ul style="list-style-type: none"> ○ Sistemas sin antivirus ni herramientas de seguridad implementadas para los puntos finales ○ Sistemas en los que los servicios del agente de punto final se han cerrado o desactivado ○ Sistemas donde la tecnología de seguridad de punto final no está configurada para eliminar/bloquear todas las amenazas ○ Sistemas donde la tecnología de seguridad de punto final no escanea ni monitorea directorios críticos donde el malware puede residir o ejecutarse comúnmente 		
Justificación		
<p>BanCoppel aprovecha varias herramientas de seguridad de punto final para monitorear sistemas y alertar sobre actividades sospechosas, familias de malware, puertas traseras y amenazas basadas comunes los cuales se han identificado a lo largo de la investigación. BanCoppel debe garantizar que se maximice la cobertura y el despliegue adecuado en todo el alcance de los sistemas gestionados (basados en dominios).</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.1.16 Revisar las asignaciones de derechos de los usuario y los permisos asignados a la política de grupo	Postura	Cuentas de punto final - Fortalecimiento
Detalles de la recomendación		
<p>BanCoppel debe buscar crear o modificar objetos de políticas de GPO que denieguen a las cuentas locales o con privilegios de dominio los derechos para acceder a estaciones de trabajo y computadoras portátiles estándar. Como mínimo, imponer restricciones de inicio de sesión remoto para el permiso "SeDenyNetworkLogonRight" (denegar el acceso a esta computadora desde la red).</p>		

Acción propuesta	Categorización	Flujo de trabajo
<p>Además, tanto la Política de dominio predeterminada como la Política de controlador de dominio predeterminada deben reconfigurarse para eliminar “SeDebugPrivilege” de los siguientes grupos:</p> <ul style="list-style-type: none"> • BUILTIN\Administrators <p>Microsoft confirmó en el siguiente artículo de soporte que los grupos de Exchange Trusted Subsystem y Exchange Servers no deben recibir el “SeDebugPrivilege”: https://support.microsoft.com/en-us/help/4073098/ets-and-exs-groups-are-incorrectly-granted-sedebugprivilege-in-exchang</p> <p>A las cuentas delegadas con acceso privilegiado local o de dominio se les debe denegar explícitamente el acceso a estaciones de trabajo estándar y sistemas portátiles dentro del contexto de las siguientes configuraciones:</p> <ul style="list-style-type: none"> • <i>Computer Configuration > Políticas > Windows Settings > Security Settings > Local Policies > User Rights Assignment.</i> <ul style="list-style-type: none"> ○ Denegar el acceso a esta computadora desde la red (SeDenyNetworkLogonRight) ○ Denegar el inicio de sesión como trabajo por lotes (SeDenyBatchLogonRight) ○ Denegar el inicio de sesión como servicio (SeDenyServiceLogonRight) ○ Denegar el inicio de sesión localmente (SeDenyInteractiveLogonRight) ○ Denegar el inicio de sesión por medio de servicios de terminal (SeDenyRemoteInteractiveLogonRight) ○ Los programas de depuración (SeDebugPrivilege) deben eliminarse para todos los usuarios, incluidos los administradores locales <p>Para respaldar esto, BanCoppel debe diseñar y organizar segmentos de red en niveles protegidos dentro de su entorno y designar estos segmentos como el único punto de origen autorizado desde el cual pueden ocurrir funciones privilegiadas (ej. administración de servidor remoto, administración de base de datos, administración de aplicaciones, administración del directorio activo, funciones del Help Desk). Esto debe ser impuesto por los controles en la red, el directorio activo y las capas basadas en el host.</p> <p>Idealmente, la arquitectura debe admitir varios niveles para el control de acceso:</p> <ul style="list-style-type: none"> • Nivel 0 = Controladores de dominio y servicios altamente críticos • Nivel 1 = Servidores y aplicaciones alojadas • Nivel 2 = Estaciones de trabajo de usuario, computadoras portátiles y servidores de acceso común (ej. servidor RDS) <p>Controles de seguridad adicionales a considerar:</p>		

Acción propuesta	Categorización	Flujo de trabajo														
<ul style="list-style-type: none">El acceso directo (utilizando puertos administrativos y de gestión, por ejemplo, RDP, SSH, WinRM) de los sistemas de nivel 2 a los sistemas de nivel 0 debe bloquearse explícitamenteA las cuentas específicas sólo se les debe delegar el acceso a los sistemas de nivel 0 (y sólo se deben iniciar desde sistemas dentro de la capa de nivel 0)A las cuentas específicas sólo se les debe delegar el acceso a los sistemas de nivel 1 (y sólo se deben iniciar desde sistemas dentro de la capa de nivel 1)																
<p>En los sistemas de Nivel 2, las cuentas delegadas para el acceso de Nivel 0 y Nivel 1 deben denegarse explícitamente para el acceso mediante la siguiente configuración, la cual se puede configurar dentro del contexto de la configuración de GPO (Figura 11):</p>																
<ul style="list-style-type: none">Denegar el acceso a esta computadora desde la red (“SeDenyNetworkLogonRight” también incluye “S-1-5-114: NT AUTHORITY\Local account and member of Administrators group”)Denegar el inicio de sesión localmente (“SeDenyInteractiveLogonRight”)Denegar el inicio de sesión por medio de servicios de terminal (“SeDenyRemoteInteractiveLogonRight”)Denegar el inicio de sesión como trabajo por lotes (“SeDenyBatchLogonRight”)Denegar el inicio de sesión como servicio (“SeDenyServiceLogonRight”)																
<table border="1"><thead><tr><th colspan="2">Local Policies/User Rights Assignment</th></tr><tr><th>Policy</th><th>Setting</th></tr></thead><tbody><tr><td>Deny access to this computer from the network</td><td>Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts</td></tr><tr><td>Deny log on as a batch job</td><td>Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts</td></tr><tr><td>Deny log on as a service</td><td>Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts</td></tr><tr><td>Deny log on locally</td><td>MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts</td></tr><tr><td>Deny log on through Terminal Services</td><td>Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts</td></tr></tbody></table>			Local Policies/User Rights Assignment		Policy	Setting	Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts	Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts	Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts	Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts	Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Local Policies/User Rights Assignment																
Policy	Setting															
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts															
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts															
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts															
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts															
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts															
<p>Figura 11: Puntos finales de nivel 2 - Restricciones de cuentas privilegiadas - Ejemplo de GPO</p>																
<p>En los sistemas de Nivel 1, las cuentas delegadas para el acceso de Nivel 0 deben denegarse explícitamente para el acceso mediante la siguiente configuración, la cual se puede configurar dentro del contexto de la configuración de GPO (Figura 12).</p>																
<ul style="list-style-type: none">Denegar el inicio de sesión localmente (“SeDenyInteractiveLogonRight”)																

Acción propuesta	Categorización	Flujo de trabajo
<ul style="list-style-type: none">• Denegar el inicio de sesión por medio de servicios de terminal (“SeDenyRemoteInteractiveLogonRight”)• Denegar el inicio de sesión como trabajo por lotes (“SeDenyBatchLogonRight”)• Denegar el inicio de sesión como servicio (“SeDenyServiceLogonRight”)• Denegar el acceso a esta computadora desde la red (“SeDenyNetworkLogonRight”)		

Local Policies/User Rights Assignment	
Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts

Figura 12: Puntos finales de nivel 1 - Restricciones de cuentas privilegiadas - Ejemplo de GPO

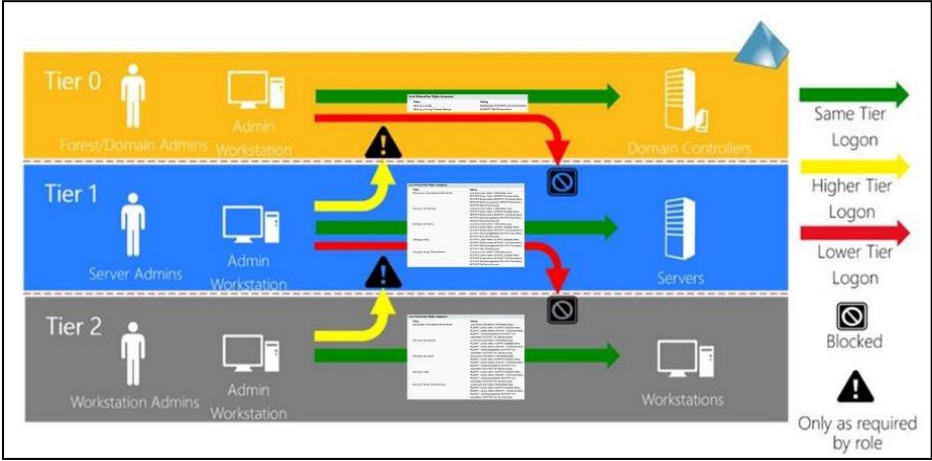
En los sistemas de Nivel 0, solo las cuentas designadas para fines de administración de Nivel 0 deben tener acceso mediante la siguiente configuración, que se puede configurar dentro del contexto de la configuración de GPO (Figura 13).

- Permitir el inicio de sesión localmente
- Permitir el inicio de sesión por medio d servicios de terminal

Local Policies/User Rights Assignment	
Policy	Setting
Allow log on locally	Administrators, MCWHIRT\Tier0-DomainAdmins
Allow log on through Terminal Services	MCWHIRT\Tier0-DomainAdmins

Figura 13: Puntos finales de nivel 0 - Restricciones de cuentas privilegiadas - Ejemplo de GPO

El siguiente diagrama, al que se hace referencia en la Figura 14, proporciona una descripción general de la arquitectura de alto nivel de este modelo y las recomendaciones enlistadas anteriormente.

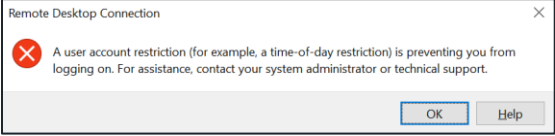
Acción propuesta	Categorización	Flujo de trabajo
		<div data-bbox="347 258 1273 716"></div> <p data-bbox="264 737 1359 793"><i>Figura 14: Modelo de arquitectura por niveles: Por medio de https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material</i></p> <p data-bbox="159 814 1438 877">Además, se deben aprovechar métodos específicos que no dejen credenciales reutilizables en un punto final de destino, los cuales incluyen:</p> <ul data-bbox="207 898 695 1270" style="list-style-type: none">• MMC• NET USE• PowerShell WinRM (sin CredSSP)• PSEXEC (sin credenciales explícitas)• Credential Guard• RDP de administrador restringido• Remote Credential Guard (RDP) <p data-bbox="159 1339 1464 1440">Note: Para el SID “S-1-5-114: NT AUTHORITY\Local account and member of Administrators group”, si se utiliza la agrupación en clústeres de conmutación por error, esta función debe aprovechar una cuenta local no administrativa (CLIUSR) para la administración de los nodos del clúster.</p> <p data-bbox="159 1461 1438 1591">Sin embargo, si esta cuenta es miembro del grupo de administradores locales en un extremo que forma parte de un clúster, bloquear los permisos de inicio de sesión de la red puede hacer que los servicios del clúster fallen. Tener cuidado y probar detalladamente esta configuración en servidores donde se utiliza la agrupación en clústeres de conmutación por error.</p> <p data-bbox="159 1612 1432 1675">Los grupos privilegiados comunes basados en dominios que se deben considerar para el objetivo inicial (por medio de la configuración anterior) incluyen:</p> <ul data-bbox="207 1696 750 1858" style="list-style-type: none">• Grupos que contienen cuentas de servicio• Operadores de cuentas• Administradores• Operaciones de respaldo

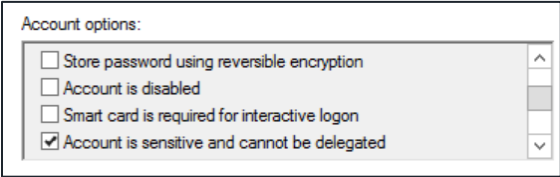
Acción propuesta	Categorización	Flujo de trabajo
<ul style="list-style-type: none"> • Administradores de dominio • Administradores de empresas • Administradores de esquemas • Operadores de servidor <p>Para cada dominio dentro del alcance, Mandiant identificó cuentas de usuario y grupos adicionales que tienen acceso privilegiado en todos los dominios dentro del alcance, y los cuales podrían utilizarse como una ruta para escalar privilegios y obtener acceso elevado. Estas cuentas también deben incluirse dentro del alcance de las restricciones de inicio de sesión mencionadas anteriormente.</p>		
Justificación		
<p>La captura de detalles adicionales de la bitácora mejorará la capacidad de BanCoppel para determinar qué actividad ocurrió en un punto final. Este nivel de visibilidad también permite a BanCoppel mejorar la detección de eventos sospechosos al generar alertas basadas en patrones predefinidos de actividad común de los atacantes. Esta información debe centralizarse en un SIEM para permitir el análisis en caso de que las bitácoras de eventos hayan sido eliminadas.</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.1.17 Documentar el acceso de terceros al entorno	Postura	Acceso externo
Detalles de la recomendación		
<p>BanCoppel debe documentar todas las entidades de terceros que tienen acceso al entorno. La documentación debe incluir el mecanismo utilizado por cada parte para acceder al entorno y la fuente de autenticación del mecanismo (ej. Directorio activo, RSA SecurID), además de la segmentación lógica y los controles de acceso que se imponen.</p> <p>Cualquier mecanismo de acceso de terceros que no requiera autenticación multi factor, para conexiones desde redes que no sean de confianza, debe identificarse específicamente en la documentación. Para cada uno de estos mecanismos de acceso, BanCoppel debe evaluar la viabilidad de imponer la autenticación multi factor para un acceso continuo.</p>		
Justificación		
<p>Documentar y revisar el alcance de las entidades de terceros que tienen acceso al entorno puede identificar todas las vías potenciales que un atacante pudiese aprovechar para acceder al entorno.</p> <p>Además, esta revisión también puede proporcionar conciencia y verificación de los controles de seguridad y los mecanismos de autenticación que pueden no estar alineados con las políticas de la organización o las mejores prácticas de seguridad.</p>		

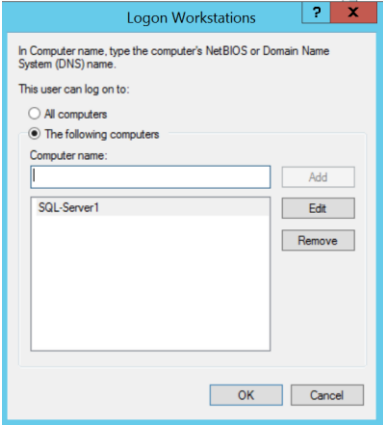
Fortalecimiento: Protecciones de cuentas y credenciales


Acción propuesta	Categorización	Flujo de trabajo
1.2.1 Aprovechar el grupo de seguridad de usuarios protegidos para cuentas privilegiadas	Fortalecimiento	Cuentas - Fortalecimiento
Detalles de la recomendación		
<p>A partir de Microsoft Windows Server 2012 R2 y Windows 8.1, se introdujo el grupo de seguridad Usuarios protegidos para administrar la exposición de credenciales para cuentas privilegiadas. Los miembros de este grupo tienen automáticamente protecciones no configurables aplicadas a sus cuentas, que incluyen:</p> <ul style="list-style-type: none"> • El ticket granting ticket (TGT) de Kerberos caduca después de cuatro horas, en lugar de la configuración predeterminada normal de 10 horas • Las credenciales almacenadas en caché están bloqueadas; un controlador de dominio debe estar disponible para autenticar la cuenta • Las contraseñas de texto claro no se almacenan en caché para la autenticación implícita de Windows o la delegación de credenciales predeterminada (CredSSP), independientemente de la configuración de la política aplicada del punto final • La función unidireccional NTLM (NTOWF) está bloqueada • DES y RC4 no se pueden utilizar para la autenticación previa de Kerberos (Server 2012 R2 o superior) • Las cuentas no se pueden utilizar para la delegación restringida o no restringida (equivalente a imponer la configuración "Account is sensitive and cannot be delegated" en usuarios y equipos del directorio activo) <p>Para obtener información adicional relacionada con este paso, consultar: https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group</p> <p>Además, el aviso de seguridad de Microsoft KB2871997 agrega compatibilidad con las protecciones aplicadas para los miembros del grupo de seguridad Usuarios protegidos en Windows 7, Windows Server 2008 R2 y Windows Server 2012.</p> <p>BanCoppel debe probar y, posteriormente, considerar agregar cuentas con muchos privilegios (ej. aquellas cuentas que tienen permisos de nivel de administrador de dominio o de empresa o acceso dentro del entorno) al grupo de seguridad de Usuarios Protegidos en el directorio activo.</p> <p>Nota: Las siguientes son advertencias que deben tenerse en cuenta al aprovechar el grupo de seguridad Usuarios protegidos:</p> <ul style="list-style-type: none"> • BanCoppel no debe agregar ninguna cuenta con muchos privilegios al grupo de seguridad de Usuarios Protegidos hasta que se hayan probado todos los impactos potenciales. Más bien, apuntar a un subconjunto específico de cuentas privilegiadas para las pruebas iniciales. • Cuando un miembro del grupo de seguridad de Usuarios protegidos inicia RDP, se debe utilizar (y configurar en el punto final de destino) RDP de administrador restringido (<code>mstsc /restrictedadmin</code>) o Remote Credential Guard (<code>mstsc /remoteguard</code>). • Cuando RDP es iniciado por un miembro del grupo de seguridad de Usuarios Protegidos, si se utiliza la dirección IP del servidor remoto para conectarse (en lugar del nombre de host), la conectividad fallará debido a que NTLM se utiliza para la autenticación (Figura 15). 		

Acción propuesta	Categorización	Flujo de trabajo
<div data-bbox="256 275 807 409"></div> <p data-bbox="256 430 1055 457"><i>Figura 15: Mensaje de error al intentar autenticarse utilizando RDP y NTLM</i></p> <ul data-bbox="207 478 1461 1108" style="list-style-type: none">• Las cuentas de servicio y de computadora NO deben ser miembros del grupo de seguridad de Usuarios Protegidos. La autenticación fallará con el error "the username or password is incorrect" para cualquier servicio o cuenta de computadora que se agregue al grupo de seguridad de Usuarios protegidos.• Los miembros del grupo de seguridad de Usuarios protegidos deben poder autenticarse mediante Kerberos con cifrado AES. Este método requiere claves AES para la cuenta en el directorio activo. El administrador integrado no tiene una clave AES a menos que se haya cambiado la contraseña en un controlador de dominio que ejecuta Windows Server 2008 o posterior.• Cambiar la contraseña de todas las cuentas de dominio que se crearon antes de que el dominio se promoviera a un nivel funcional de 2008 (o dominio superior). De lo contrario, estas cuentas no se pueden autenticar si residen en el grupo de seguridad Usuarios protegidos.• La pertenencia al grupo de seguridad de Usuarios protegidos desactiva automáticamente la autenticación NTLM; por lo tanto, la autenticación fallará para cualquier cuenta de usuario protegido que intente acceder a aplicaciones o servicios que requieran NTLM para la autenticación debido a que los SPN no existen, ya que Kerberos requiere un SPN válido para configurar el servicio. Esto sucederá automáticamente si el servicio de la aplicación se ejecuta como un sistema local, pero no ocurrirá si se utiliza una cuenta de servicio personalizada, ya que un administrador de dominio debe registrar manualmente el SPN. <p data-bbox="159 1119 1461 1249">Además de la bitácora de eventos de seguridad estándar en puntos finales y controladores de dominio, los eventos de inicio de sesión exitosos (ID. de evento 303, 304) o fallidos (ID. de evento 100, 104) para miembros del grupo de seguridad de Usuarios protegidos se pueden registrar en los controladores de dominio dentro de las siguientes bitácoras de eventos:</p> <ul data-bbox="207 1264 1128 1407" style="list-style-type: none">• %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Authentication%4ProtectedUserSuccesses-DomainController.evtx• %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Authentication%4ProtectedUserFailures-DomainController.evtx <p data-bbox="159 1419 1461 1549">Las bitácoras de eventos están deshabilitadas de forma predeterminada y deben habilitarse en cada controlador de dominio. Los cmdlets de PowerShell, a los que se hace referencia en la Figura 16, se pueden aprovechar para habilitar las bitácoras de eventos para el grupo de seguridad de Usuarios protegidos en un controlador de dominio.</p>		
<pre data-bbox="159 1570 1412 1875">\$log1 = New-Object System.Diagnostics.Eventing.Reader.EventLogConfiguration Microsoft-Windows-Authentication/ProtectedUserSuccesses-DomainController \$log1.IsEnabled=\$true \$log1.SaveChanges() \$log2 = New-Object System.Diagnostics.Eventing.Reader.EventLogConfiguration Microsoft-Windows-Authentication/ProtectedUserFailures-DomainController \$log2.IsEnabled=\$true</pre>		

Acción propuesta	Categorización	Flujo de trabajo
<p><code>\$log2.SaveChanges()</code></p> <p><i>Figura 16: Cmdlet de PowerShell para habilitar la bitácora de eventos para el grupo de seguridad de usuarios protegidos en los controladores de dominio</i></p> <p>En los casos en que no se pueda utilizar el grupo de seguridad de Usuarios protegidos, BanCoppel debe asegurarse de que estén configuradas las siguientes opciones de Política de grupo.</p> <ul style="list-style-type: none"> Asegurarse de que “Enable computer and user accounts to be trusted for delegation” no incluya cuentas privilegiadas o administrativas. <ul style="list-style-type: none"> Computer Configuration > Políticas > Windows Settings > Security Settings > Local Policies > User Rights Assignment > Enable computer and user accounts to be trusted for delegation Asegurarse de que “Account is sensitive and cannot be delegated” esté configurada para cuentas privilegiadas o administrativas (Figura 17).  <p><i>Figura 17: Configuración de fortalecimiento de la cuenta del directorio activo</i></p> <p>Para obtener información adicional, consultar:</p> <ul style="list-style-type: none"> https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/reading-the-fine-print-on-the-protected-users-group/ba-p/258470 		

Acción propuesta	Categorización	Flujo de trabajo
1.2.2 Fortalecer el acceso a las cuentas de servicio	Fortalecimiento	Cuentas - Fortalecimiento
Detalles de la recomendación		
<p>BanCoppel debe identificar y, cuando corresponda, mejorar la seguridad de las cuentas de servicio basadas en dominios para restringir la capacidad de las cuentas que se utilizarán para el escritorio remoto interactivo y los inicios de sesión basados en la red. Siempre que sea posible, las cuentas de servicio y otras cuentas privilegiadas deben colocarse en CyberArk.</p> <p>Fortalecimiento de inicio de sesión mínimo recomendado para cuentas de servicio (en puntos finales donde la cuenta de servicio no es necesaria para fines de inicio de sesión remoto o interactivo):</p> <ul style="list-style-type: none"> Computer Configuration > Políticas > Windows Settings > Security Settings > Local Policies > User Rights Assignment <ul style="list-style-type: none"> Denegar el inicio de sesión localmente (SeDenyInteractiveLogonRight) Denegar el inicio de sesión por medio de servicios de terminal (SeDenyRemoteInteractiveLogonRight) 		

Acción propuesta	Categorización	Flujo de trabajo
<p>Fortalecimiento adicional de inicio de sesión recomendado para cuentas de servicio (en puntos finales donde las cuentas de servicio no son necesarias para fines de inicio de sesión basados en la red):</p> <ul style="list-style-type: none">• Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment<ul style="list-style-type: none">○ Denegar el acceso a esta computadora desde la red (SeDenyNetworkLogonRight) <p>Además, si sólo se requiere que una cuenta de servicio se aproveche en un solo punto final para ejecutar un servicio específico, utilizando Usuarios y equipos del directorio activo, la cuenta de servicio se puede restringir aún más para permitir sólo el uso de la cuenta en una lista predefinida de puntos finales (Figura 18).</p> <ol style="list-style-type: none">1. Active Directory Users and Computers > Seleccionar la cuenta2. Pestaña Account3. Botón “Log On To” > Seleccionar el alcance adecuado de las computadoras para acceder 		
<p><code>get-aduser -filter {(ServicePrincipalName -like "*") } Select-Object name,samaccountname,sid,enabled,DistinguishedName</code></p>		
<p><i>Figura 19: Comando de PowerShell para identificar cuentas que no son de computadora con SPN</i></p> <p>Para automatizar la administración de contraseñas fortalecidas para las cuentas de servicios dedicados que están asociados con puntos finales específicos, BanCoppel puede considerar aprovechar las cuentas de servicio administradas de Windows (MSA) y/o las cuentas de servicio administradas de grupo (gMSA), que rotarán automáticamente la contraseña de las cuentas cada 30 días en el directorio activo.</p> <p>Nota: Los MSA se introdujeron por primera vez en Windows Server 2008 R2, mientras que los gMSA se introdujeron en Windows Server 2012 y requieren puntos finales que ejecuten Windows Server 2012 (o superior) para su uso.</p> <p>Siguiendo las mejores prácticas para proteger MSA y gMSA, los beneficios incluyen:</p> <ul style="list-style-type: none">• Gestión automatizada de contraseñas para MSA, sin exponer la contraseña a los administradores		

Acción propuesta	Categorización	Flujo de trabajo
<ul style="list-style-type: none"> Riesgo reducido de movimiento lateral y escalación de privilegios utilizando cuentas de servicio Riesgo reducido de ataques Kerberoasting y Silver Ticket aprovechando un MSA Cuentas de servicio que no se pueden utilizar para el inicio de sesión interactivo Cuentas de servicio que se pueden utilizar en un alcance limitado de puntos finales <p>Adjuntos:</p>  <p>Bancoppel Service Accounts.xlsx</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.2.3 Credenciales seguras cuando se utilizan para una conectividad de escritorio remoto	Fortalecimiento	Cuentas - Fortalecimiento
Detalles de la recomendación <p>BanCoppel deberá considerar la aplicación de métodos fortalecidos que reduzcan la exposición de las credenciales privilegiadas cuando se conectan de forma remota a los puntos finales mediante el Escritorio remoto. Aprovechar los métodos fortalecidos para la conectividad del escritorio remoto puede proteger las credenciales privilegiadas para que no queden expuestas en la memoria de los puntos finales de destino.</p> <p>Modo de administrador restringido</p> <p>El modo de administrador restringido se puede habilitar para todos los sistemas de usuario final asignados al personal que realiza conexiones de escritorio remoto a servidores o estaciones de trabajo con credenciales de administrador. Esta función puede limitar la exposición en memoria de las credenciales administrativas en un punto final de destino al que se accede mediante el Protocolo de escritorio remoto (RDP).</p> <p>Nota: Para aprovechar el modo de administrador restringido para conectarse a puntos finales, si el punto final de origen es anterior a Windows 8.1 o Windows Server 2012 R2, se debe instalar KB2871997. Además, el punto final de destino debe ejecutar al menos Windows 8.1 o Windows Server 2012 R2. Por último, la cuenta utilizada para la autenticación debe tener privilegios de administrador local en el punto final de destino. Las cuentas que sólo son miembros del grupo "Remote Desktop Users" no podrán aprovechar el RDP de administrador restringido.</p> <p>Para aprovechar el RDP de administrador restringido, utilizar el comando al que se hace referencia en la Figura 20.</p> <p>mstsc.exe /RestrictedAdmin</p> <p><i>Figura 20: Comando para aprovechar el RDP del administrador restringido</i></p> <p>Cuando una conexión RDP utiliza la función de administrador restringido, si la cuenta de autenticación es un administrador en el punto final de destino, las credenciales de la cuenta de usuario no se almacenan en la memoria; más bien, el contexto de la cuenta de usuario aparece como la cuenta de la máquina de destino (domain\destination-computer\$).</p> <p>Para aprovechar el modo de administrador restringido, la configuración debe aplicarse tanto en los puntos finales de origen como en los de destino.</p>		

Punto final de origen (modo cliente: Windows 7 y Windows Server 2008 R2 y superior):

Se debe aplicar una configuración de GPO al punto final de origen que inicia la sesión de escritorio remoto mediante la función /RestrictedAdmin.

- Computer Configuration > Policies > System > Credential Delegation > Restrict delegation of credentials to remote servers
 - Require Restricted Admin > establecer como Enabled

Punto final de destino (modo de servidor: Windows 8.1 y Windows Server 2012 R2 y superior):

Se deberá configurar una ajuste de registro (Figura 21).

HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin

0 = Enabled

1 = Disabled

Figura 21: Configuración de registro para habilitar o deshabilitar RestrictedAdmin RDP

Con RDP de administrador restringido, otra opción que debe configurarse es la llave de registro "DisableRestrictedAdminOutboundCreds" (Figura 22). **Error! Reference source not found.**

HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdminOutboundCreds

0 = default value (doesn't exist) - Admin Outbound Creds are Enabled

1 = Admin Outbound Creds are Disabled

Figura 22: Configuración de registro para deshabilitar las credenciales salientes del administrador

Nota: Con esta configuración establecida en "0", cualquier solicitud de autenticación saliente aparece como el sistema (domain\destination-computer\$) al que se conectó un usuario mediante RDP de administrador restringido. Establecer esto en "1" deshabilita la capacidad de autenticarse en cualquier recurso de red descendente cuando se intenta autenticar la salida de un sistema al que un usuario se conectó usando RDP de administrador restringido.

Para obtener información adicional sobre el RDP de administrador restringido, consultar:

- <https://support.microsoft.com/kb/2973351>
- <https://blogs.technet.microsoft.com/kfalde/2013/08/14/restricted-admin-mode-for-rdp-in-windows-8-1-2012-r2/>

Remote Credential Guard

BanCoppel deberá probar Credential Guard para los puntos finales de Windows 10 y Windows Server 2016 para su uso en el entorno. Remote Credential Guard se puede aprovechar para reducir la exposición de las cuentas privilegiadas en la memoria en los puntos finales de destino cuando se utiliza el escritorio remoto para la conectividad. Con Remote Credential Guard, todas las credenciales permanecen en el cliente (sistema de origen) y no están directamente expuestas al punto final de destino. En cambio, las credenciales permanecen en el punto final de origen y, el punto final de destino, solicita tickets de servicio del origen según sea necesario. Cuando un usuario inicia sesión por medio de RDP en un punto final que tiene Remote Credential Guard habilitado, ninguno de los proveedores de soporte de seguridad (SSP) en la memoria almacena la contraseña de texto claro o el hash de contraseña del usuario. Tener en cuenta que los tickets de Kerberos permanecen en la memoria para permitir experiencias interactivas (y SSO) desde el servidor de destino. Para aprovechar Remote Credential Guard, son necesarios los siguientes requisitos.

El host del cliente de escritorio remoto (origen):

- Debe ejecutar al menos Windows 10 (v1703) para poder proporcionar credenciales
- Debe ejecutar al menos Windows 10 (v1607) o Windows Server 2016 para utilizar las credenciales de inicio de sesión del usuario (sin solicitud de credenciales)
Esto requiere que la cuenta del usuario pueda iniciar sesión tanto en el cliente (origen) como en el extremo remoto (destino).
- Debe ejecutar la aplicación clásica de Windows Remote Desktop
La aplicación de la plataforma universal de Windows de escritorio remoto no es compatible con Windows Defender Remote Credential Guard.
- Debe utilizar la autenticación Kerberos para conectarse al host remoto
Si el cliente no puede conectarse a un controlador de dominio, RDP intenta recurrir a NTLM. *Windows Defender Remote Credential Guard no permite el respaldo de NTLM porque esto expondría las credenciales a riesgos.*

El host remoto (destino) del Escritorio remoto:

- Debe ejecutar al menos Windows 10 (v1607) o Windows Server 2016
- Debe permitir conexiones de administrador restringidas
- Debe permitir que el usuario del dominio del cliente acceda a las conexiones de Escritorio remoto
- Debe permitir la delegación de credenciales no exportables

Para habilitar Remote Credential Guard en el host del cliente (origen):

- Computer Configuration > Policies > Administrative Templates > System > Credentials Delegation > Restrict delegation of credentials to remote servers
 - Para requerir el modo de administrador restringido o Windows Defender Remote Credential Guard, seleccionar “Prefer Windows Defender Remote Credential Guard”.
 - En esta configuración, se prefiere Remote Credential Guard, pero se utilizará el modo de administrador restringido (si es compatible) cuando no se pueda utilizar Remote Credential Guard.
 - Ni el modo Remote Credential Guard ni el modo de administrador restringido enviarán las credenciales en texto claro al servidor de escritorio remoto.
 - Para solicitar Remote Credential Guard, seleccionar “Require Windows Defender Remote Credential Guard”.
 - En esta configuración, una conexión de Escritorio remoto sólo se realizará correctamente si la computadora remota cumple con los requisitos de Remote Credential Guard.

De manera alternativa, el registro se puede configurar para habilitar Remote Credential Guard en el host remoto (destino) (Figura 23):

HKLM\System\CurrentControlSet\Control\Lsa

Registry Entry: DisableRestrictedAdmin

Value: 0

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /d 0 /t REG_DWORD
```

Figura 23: Llave de registro y comando para habilitar Remote Credential Guard en un host remoto (destino)

Para aprovechar Remote Credential Guard, aprovechar el comando que se indica en la Figura 24:

```
mstsc.exe /remoteguard
```

Figura 24: Comando para aprovechar el Credential Guard remoto

Acción propuesta	Categorización	Flujo de trabajo
1.2.4 Fortalecer las capacidades para que las cuentas locales se aprovechen para la autenticación remota	Fortalecimiento	Cuentas de punto final - Fortalecimiento
Detalles de la recomendación		
<p>BanCoppel deberá considerar implementar las capacidades de fortalecimiento para restringir el uso de cuentas locales que existen en los puntos finales para reducir el riesgo de movimiento lateral en todo el entorno.</p> <p>Microsoft KB2871997 (https://support.microsoft.com/en-us/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-a) introdujo dos SID bien conocidos que se pueden aprovechar en Configuración de GPO para restringir el uso de las cuentas locales para el movimiento lateral.</p> <ul style="list-style-type: none"> • S-1-5-113: NT AUTHORITY\Local account • S-1-5-114: NT AUTHORITY\Local account and member of Administrators group <p>Específicamente, el SID “S-1-5-114: NT AUTHORITY\Local account and member of Administrators group” se agrega al token de acceso de una cuenta si la cuenta local es miembro del grupo BUILTIN\Administradores. Este es el SID más beneficioso que se puede aprovechar para detener a un atacante que se propaga utilizando credenciales para cuentas administrativas locales.</p> <p>Nota: Para el SID “S-1-5-114: NT AUTHORITY\Local account and member of Administrators group”, si se utiliza la agrupación en clústeres de conmutación por error, esta función debe aprovechar una cuenta local no administrativa (CLIUSR) para la administración de nodos de clúster. Sin embargo, si esta cuenta es miembro del grupo de administradores locales en un extremo que forma parte de un clúster, bloquear los permisos de inicio de sesión de la red puede hacer que los servicios del clúster fallen. Tener cuidado y probar detalladamente esta configuración en servidores donde se utiliza la agrupación de clústeres de conmutación por error.</p> <p>Opción 1: Fortalecimiento de SID S-1-5-114</p> <p>Para evitar que el uso de cuentas administrativas locales se utilicen para movimientos laterales, utilizar el SID “S-1-5-114: NT AUTHORITY\Local account and member of Administrators group” dentro de las siguientes configuraciones:</p> <ul style="list-style-type: none"> • Computer Configuration > Políticas > Windows Settings > Security Settings > Local Policies > User Rights Assignment <ul style="list-style-type: none"> ○ Denegar el acceso a esta computadora desde la red (SeDenyNetworkLogonRight) ○ Denegar el inicio de sesión como trabajo por lotes (SeDenyBatchLogonRight) ○ Denegar el inicio de sesión como servicio (SeDenyServiceLogonRight) ○ Denegar el inicio de sesión por medio de servicios de terminal (SeDenyRemoteInteractiveLogonRight) 		

- Programas de depuración (SeDebugPrivilege – permiso utilizado para el intento de escalación de privilegios e inyección de procesos)

Opción 2: Filtrado de tokens UAC

Un control adicional que se puede imponer por medio de GPO se refiere al uso de cuentas locales para la administración remota y la conectividad por medio de un inicio de sesión en la red. Si no se puede implementar el alcance completo de los permisos (mencionados anteriormente) en un período de tiempo corto, considerar la posibilidad de aplicar el método de filtrado de tokens de UAC a las cuentas locales para inicios de sesión basados en la red.

Para aprovechar esta configuración por medio de una configuración de GPO:

1. Descargar el kit de herramientas de cumplimiento de seguridad (<https://www.microsoft.com/en-us/download/details.aspx?id=55319>) para utilizar el archivo ADMX de la "MS Security Guide".
2. Una vez descargados, los archivos "SecGuide.admx" y "SecGuide.adml" deben copiarse en los directorios \Windows\PolicyDefinitions y \Windows\PolicyDefinitions\en-US respectivamente.
3. Si se configura un almacenamiento de GPO centralizado para el dominio, copie la carpeta "PolicyDefinitions" en la carpeta C:\Windows\SYSVOL\sysvol\<domain>\Policies.

Configuración de GPO:

- Computer Configuration > Políticas > Administrative Templates > MS Security Guide > Apply UAC restrictions to local accounts on network logons
 - Habilitado

Una vez habilitado, el valor de registro (Figura 25) se configurará en cada punto final:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy
REG_DWORD = "0" (Enabled)

Figura 25: Valor de registro para habilitar restricciones de UAC para cuentas locales en inicios de sesión de red

Cuando se establece en "0", las conexiones remotas con tokens de acceso de alta integridad sólo son posibles utilizando la credencial de texto sin formato o el hash de contraseña del administrador local de RID 500 (y solo entonces dependiendo de la configuración de "FilterAdministratorToken").

La opción "FilterAdministratorToken" puede habilitar (1) o deshabilitar (0 = predeterminado) el modo "Admin Approval" para el administrador local de RID 500. Cuando está habilitado, el token de acceso para la cuenta de administrador local de RID 500 se filtra y, por lo tanto, se aplica el Control de cuentas de usuario (UAC) para esta cuenta (lo que, en última instancia, puede detener los intentos de aprovechar esta cuenta para el movimiento lateral entre los puntos finales).

Configuración de GPO

- Computer Configuration > Políticas > Windows Settings > Security Settings > Local Policies > Security Options > User Account Control: Run all administrators in Admin Approval Mode
 - Habilitado

Una vez habilitado, el valor del registro (Figura 26) se configurará en cada punto final:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorToken
REG_DWORD = "1" (Enabled)

Figura 26: Valor de registro para habilitar las restricciones de UAC para: ejecutar todos los administradores en "Admin Approval Mode"

Nota: El filtrado del token de acceso de UAC no afectará a ninguna cuenta de dominio en el grupo de administradores locales en un punto final.

Acción propuesta	Categorización	Flujo de trabajo
1.2.5 Deshabilitar la autenticación WDigest en los puntos finales	Fortalecimiento	Cuentas de punto final - Fortalecimiento
Detalles de la recomendación		
<p>En los sistemas operativos Windows más antiguos, las contraseñas de texto claro se almacenan en la memoria (LSASS) para admitir principalmente la autenticación WDigest.</p> <p>BanCoppel deberá deshabilitar explícitamente la autenticación WDigest en todos los puntos finales de Windows. De forma predeterminada, la autenticación WDigest está deshabilitada en Windows 8.1 (superior) y en Windows Server 2012 R2 (superior).</p> <p>A partir de Windows 7 y Windows Server 2008 R2, después de instalar KB2871997, la autenticación WDigest se puede configurar modificando el registro (Figura 27) o utilizando la plantilla de GPO de la Guía de seguridad de Microsoft del Kit de herramientas de cumplimiento de seguridad de Microsoft (https://www.microsoft.com/en-us/download/details.aspx?id=55319).</p> <p>Método de registro:</p> <p>HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential REG_DWORD = "0"</p>		
<p><i>Figura 27: Llave de registro y valor para deshabilitar la autenticación WDigest</i></p>		
<p>Método de política de grupo (método recomendado):</p> <ol style="list-style-type: none"> 1. Descargar el kit de herramientas de cumplimiento de seguridad (https://www.microsoft.com/en-us/download/details.aspx?id=55319) para utilizar el archivo ADMX del "MS Security Guide". 2. Una vez descargados, los archivos "SecGuide.admx" y "SecGuide.adml" deben copiarse en los directorios \Windows\PolicyDefinitions y \Windows\PolicyDefinitions\en-US respectivamente. 3. Si un almacenamiento de GPO centralizado está configurado para el dominio, si aún no está presente en un controlador de dominio, copiar la carpeta "PolicyDefinitions" en la carpeta C:\Windows\SYVOL\syvol\<domain>\Policies. <ol style="list-style-type: none"> a. Alternativamente, si existe la carpeta "PolicyDefinitions", copiar los archivos ADMX y ADML en los directorios apropiados dentro de la carpeta "PolicyDefinitions". b. Los archivos ADMX se colocarán en la raíz de la carpeta "PolicyDefinitions". c. Los archivos ADML se colocarán en la subcarpeta "EN-US" dentro de la carpeta "PolicyDefinitions". <p>Con la plantilla de la política de grupo Microsoft Security Guide la autenticación WDigest se puede deshabilitar mediante una configuración de GPO (Figura 28). Se recomienda comenzar con estaciones de trabajo y, posteriormente, imponer gradualmente a los servidores en un enfoque por etapas.</p>		

- Computer Configuration > Políticas > Administrative Templates > MS Security Guide > WDigest Authentication
 - Deshabilitado













Setting	State	Comment
 Configure SMB v1 server	Not configured	No
 Configure SMB v1 client driver	Not configured	No
 Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Not configured	No
 Extended Protection for LDAP Authentication (Domain Controllers only)	Not configured	No
 Turn on Windows Defender protection against Potentially Unwanted Applications (DEPRECATED)	Not configured	No
 Enable Structured Exception Handling Overwrite Protection (SEHOP)	Not configured	No
 Apply UAC restrictions to local accounts on network logons	Not configured	No
 WDigest Authentication (disabling may require KB2871997)	Disabled	No
 Lsass.exe audit mode	Not configured	No
 LSA Protection	Not configured	No
 Remove "Run As Different User" from context menus	Not configured	No
 Block Flash activation in Office documents	Not configured	No

Figura 28: Deshabilitar la autenticación WDigest por medio de la plantilla de la política de grupo "MS Security Guide"

Un actor malicioso podría aprovechar esto habilitando manualmente la autenticación WDigest en los puntos finales modificando directamente el registro (UseLogonCredential configurado con un valor de 1). Incluso en los puntos finales donde la autenticación WDigest está automáticamente deshabilitada de forma predeterminada, se recomienda imponer la configuración de GPO que se indica en la Figura 28 y configurar el reprocesamiento automático de políticas de grupo para los ajustes configurados.

Además, BanCoppel debe verificar que la configuración "Allow*" no esté especificada dentro de la llave de registro a la que se hace referencia en la Figura 29, ya que esta configuración permitiría a los proveedores tspkgs/CredSSP almacenar contraseñas de texto claro en la memoria:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Credssp\PolicyDefaults

Figura 29: Llave de registro CredSSP

Como KB2871997 (detallado arriba) no es aplicable para Windows XP, Windows Server 2003 y Windows Server 2008, para deshabilitar la autenticación WDigest en estas plataformas, antes de reiniciar el sistema, WDigest debe eliminarse de la lista de paquetes de seguridad LSA dentro de la registro (Figura 30 y Figura 31).

HKLM\System\CurrentControlSet\Control\Lsa\Security Packages

Figura 30: Llave de registro para modificar los paquetes de seguridad de LSA

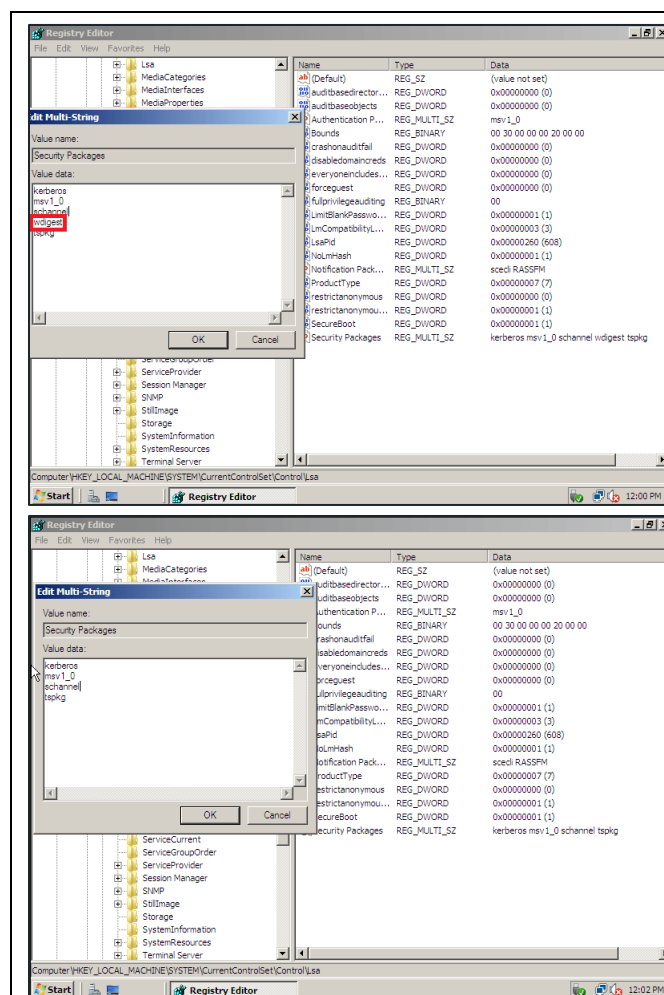


Figura 31: Llave de registro del paquete de seguridad LSA antes y después de la eliminación de la autenticación WDigest de la lista de proveedores

Nota: Incluso con WDigest desactivado, todavía existen formas de que un atacante obtenga credenciales de texto claro de la memoria. El módulo del proveedor de seguridad del sistema Kerberos (SSP) almacena las contraseñas "cifradas" en la memoria. Para valores cifrados, el SSP almacena la contraseña mediante las funciones de Win32 LsaProtectMemory y LsaUnprotectMemory. Mimikatz puede extraer las credenciales cifradas del módulo SSP de Kerberos y descifrarlas utilizando la función LsaUnprotectMemory, generando el valor de la contraseña de texto claro.

Las mitigaciones adicionales para esto incluyen:

- Reducir los permisos asignados a los usuarios estándar de los puntos finales
- Credential Guard (aplicable sólo a Windows 10 / Windows Server 2016+)
- Proceso protegido por LSA

Justificación

Con las contraseñas de texto claro almacenadas en la memoria, esto proporciona al atacante un medio para capturar contraseñas, independientemente de sus requisitos de longitud y complejidad. Sin controles adicionales implementados, la contraseña se puede utilizar para la escalación de privilegios y el movimiento lateral dentro de una organización.

Nota: Incluso con la autenticación WDigest deshabilitada en las plataformas de sistemas operativos más nuevos, se recomienda imponer de manera centralizada la configuración para deshabilitar la autenticación WDigest por medio de un GPO que se evalúa y se vuelve a imponer a un punto final en función de una frecuencia predefinida, ya que los atacantes a menudo modificarán la configuración predeterminada en los puntos finales para explotar y obtener acceso a credenciales de texto claro. La configuración específica para imponer el reprocesamiento automatizado de políticas de grupo se proporciona en una recomendación separada.

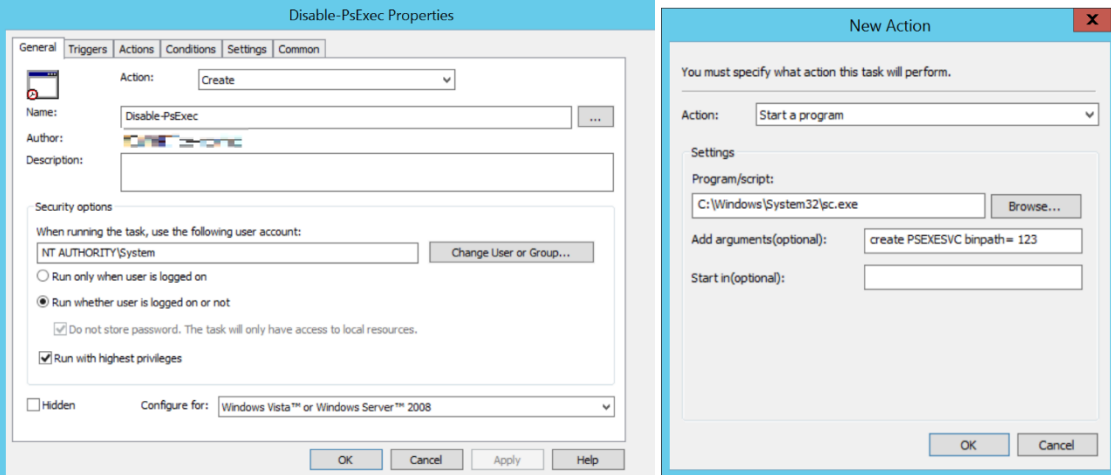
Acción propuesta	Categorización	Flujo de trabajo
1.2.6 Deshabilitar la autenticación WDigest en los puntos finales	Fortalecimiento	Punto final – Fortalecimiento
Detalles de la recomendación		
<p>PsExec es una herramienta de Microsoft Sysinternals que los atacantes suelen utilizar para moverse lateralmente y distribuir malware en un entorno empresarial.</p> <p>Una forma de limitar el uso de PsExec, por parte de los atacantes, es romper la funcionalidad de PsExec configurándolo previamente como un servicio de Windows con un argumento binpath no válido. De forma predeterminada, PsExec crea un servicio llamado PSEXESVC, aunque esto se puede cambiar.</p> <p>Esto se puede ejecutar rápidamente, a escala, ejecutando el comando <code>sc.exe</code> mediante una Tarea programada (Figura 32) que se configura e inicia mediante la Política de grupo. Cuando PsExec se ejecuta como un servicio de Windows, requiere que se especifique una ruta de archivo ejecutable para el servicio PsExec. Si esta ruta de archivo no es válida (apunta a un archivo que no existe), cualquier intento de conectarse utilizando los parámetros PsExec predeterminados a un punto final de destino no tendrá éxito.</p> <p>Nota: Para que se imponga la configuración de la política de grupo de tareas programadas, será necesario invocar un reinicio o gpupdate para los sistemas de punto final. Si no es posible reiniciar o gpupdate, la tarea programada se puede crear utilizando PowerShell (https://devblogs.microsoft.com/scripting/use-powershell-to-create-scheduled-tasks/).</p> <ul style="list-style-type: none">• Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks > New > Scheduled Task (at least Windows 7)		
		

Figura 32: Opciones de configuración de tareas programadas para un servicio PSEXESVC falso

Una vez que se ha iniciado la tarea programada en un punto final, la consulta de los servicios mostrará el servicio PSEXESVC falso (Figura 33). Además, la bitácora de eventos del sistema registrará el ID de evento 7045 para el servicio falso que se está registrando (Figura 34).

```
c:\Users\da-mcwhirt\Desktop>sc queryex type= service state= all | find /i "PSEXESVC"
SERVICE_NAME: PSEXESVC
DISPLAY_NAME: PSEXESVC
```

Figura 33: Servicio PSEXESVC falso

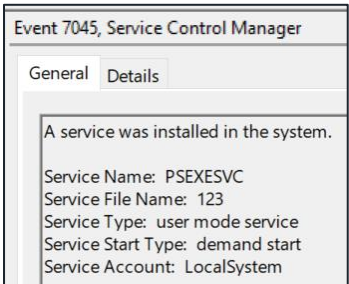


Figura 34: Bitácora de eventos de SYSTEM - EID 7045

Cualquier intento de utilizar la funcionalidad PsExec predeterminada para conectarse a un punto final donde se registró el servicio falso fallará silenciosamente (Figura 35). Además, la bitácora de eventos del sistema registrará el ID de evento 7000 para el error de invocación del servicio PSEXESVC (Figura 36). Sugerencia: El EID 7000 con los parámetros detallados en la Figura 36 puede constituir un caso de uso de monitoreo SIEM interesante.

```
c:\Users\da-mcwhirt\Desktop>PsExec.exe \\win10-domain ipconfig

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

Figura 35: No se pudo aprovechar con éxito PsExec para conectarse a un punto final remoto

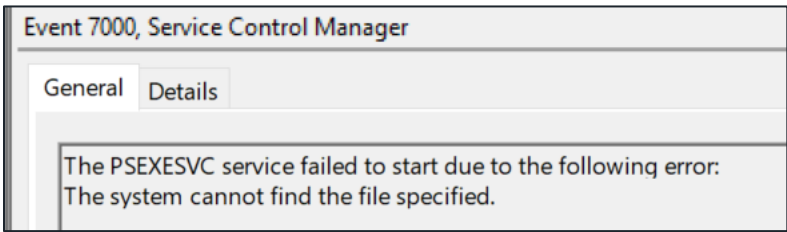


Figura 36: Bitácora de eventos del SISTEMA - EID 7000

Nota: Este método hará que PsExec no se pueda utilizar para la actividad administrativa legítima en los puntos finales. Si PsExec es una herramienta que se utiliza para administrar una empresa, este método (si se implementa) deberá revertirse (Figura 37) una vez que se contenga el malware.

```
sc delete PSEXESVC
```

Figura 37: Comando de ejemplo para eliminar el registro PSEXESVC falso

¹ <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>

Justificación

Limitar las capacidades de PSEXEC evitará que los atacantes aprovechen esta herramienta administrativa heredada y proporcionará alertas de alta fidelidad en caso de que PSEXEC se vuelva a utilizar.

Fortalecimiento: Puntos finales

Acción propuesta	Categorización	Flujo de trabajo
1.3.1 Restringir las comunicaciones de salida de los servidores	Fortalecimiento	Servidor - Fortalecimiento
Detalles de la recomendación		
<p>BanCoppel debe verificar si las comunicaciones de salida de los servidores y los sistemas críticos se pueden denegar de forma predeterminada. Las restricciones de acceso a Internet deben configurarse idealmente para DENEGAR TODO, con cualquier excepción documentada y aprobada por el equipo de seguridad de la información, el cual debe implementar los controles para inhibir y detectar cualquier actividad sospechosa asociada con la excepción.</p> <p>Todo el tráfico de salida de red aprobado bajo excepción debe registrarse, continuar enrutado por medio de un proxy web y restringirse a un conjunto específico de direcciones IP, puertos y protocolos.</p> <p>Si no se pueden bloquear eficazmente todas las comunicaciones de salida de los servidores, BanCoppel deberá considerar (como mínimo) restringir el acceso a sitios externos por medio de FTP, HTTP, HTTPS y SSH. Además, BanCoppel debe considerar bloquear el acceso a sitios de almacenamiento en la nube externos (ej. OneDrive, Dropbox, SendSpace, ShareFile) para que no sean accesibles desde todos los servidores. Con un proxy web o un filtro de contenido web, denegar el acceso a los sitios de almacenamiento en la nube debería ser factible mediante la configuración de categorización del sitio (en lugar de tener que definir cada sitio por separado).</p> <p>Además, las comunicaciones de salida directamente a direcciones IP (donde un FQDN no es parte de la solicitud) deben denegarse explícitamente.</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.3.2 Fortalecer las rutas comunes de la conectividad del movimiento lateral	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Nota: Para las siguientes configuraciones, se recomienda NO aplicarlas para controladores de dominio o servidores Exchange. Además, restringir SMB y WinRM no es práctico para todos los puntos finales dentro del entorno, especialmente para servidores de archivos, controladores de dominio que ejecutan Server Core y servidores que alojan archivos e impresoras compartidas.</p>		

Mediante la configuración de GPO, BanCoppel puede aprovechar la imposición y gestión centralizada de las políticas del cortafuegos de Windows para dispositivos de punto final asignados a usuarios finales, específicamente aquellos que se pueden utilizar fuera de la infraestructura administrada de BanCoppel (ej. computadoras portátiles).

BanCoppel debe considerar la aplicación y estandarización de las siguientes configuraciones dentro del contexto de un GPO para los puntos finales de Nivel 2, incluidos los puntos finales de back-office en las ubicaciones de las tiendas:

- Computer Configuration > Políticas > Windows Settings > Security Settings > Windows Firewall with Advanced Security
 - Configuración del perfil de dominio
 - Estado del cortafuegos
 - Encendido
 - Conexiones entrantes
 - Bloqueado
 - Registrar paquetes descartados
 - Sí
 - Registrar conexiones exitosas
 - Sí
 - Ruta del archivo de bitácora
 - %systemroot%\system32\LogFiles\Firewall\pfirewall.log
 - Tamaño máximo del archivo de bitácora (KB)
 - 4096

Para cualquier aplicación específica que pueda requerir conectividad entrante a los puntos finales del usuario final, la política del cortafuegos local debe configurarse con excepciones de direcciones IP específicas o reglas de evasión de autenticación para usuarios de origen y/o sistemas autorizados para iniciar conexiones entrantes a dichos dispositivos.

Para administrar cualquier controlador de dominio que ejecute Server Core, BanCoppel aún puede deshabilitar WinRM y sólo permitir conexiones desde direcciones IP predefinidas, usuarios o sistemas por medio de una política de reglas del cortafuegos de Windows.

Si bloquear la conectividad entrante para los puntos finales de nivel 2 no es práctico, como mínimo, las siguientes restricciones deben imponerse mediante un GPO (*Computer Configuration > Políticas > Windows Settings > Security Settings > Windows Firewall with Advanced Security*) o por medio de la imposición de la línea de comandos (Tabla 8 y Tabla 9)

Protocolo / Puerto	Regla del cortafuegos de Windows	Imposición de línea de comandos
SMB TCP/445, TCP/139, TCP/135	Regla predefinida: <ul style="list-style-type: none"> • Compartir archivos e impresoras 	netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no
Protocolo de escritorio remoto	Regla predefinida: <ul style="list-style-type: none"> • Escritorio remoto 	netsh advfirewall firewall set rule group="Remote Desktop" new enable=no

TCP/3389		
WMI	Regla predefinida: <ul style="list-style-type: none"> Instrumentación de gestión de Windows (WMI) 	netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=no
Gestión remota de Windows / PowerShell remoto TCP/80, TCP/5985, TCP/5986	Regla predefinida: <ul style="list-style-type: none"> Gestión remota de Windows Gestión remota de Windows (compatibilidad) Regla de puerto: <ul style="list-style-type: none"> 5986 	netsh advfirewall firewall set rule group="Windows Remote Management" new enable=no Por medio de PowerShell: Disable-PSRemoting -Force

Tabla 8: Reglas de bloqueo sugeridas por el cortafuegos de Windows

Ajustes de perfil	Estado del cortafuegos	Conexiones entrantes	Bitácora de paquetes descartados	Bitácora de conexiones exitosas	Tamaño máximo del archivo de bitácora (KB)
Dominio	Encendido	Bloquear todas las conexiones que no coincidan con una regla preconfigurada	Si	Si	4,096
Privado	Encendido	Bloquear todas las conexiones	Si	Si	4,096
Público	Encendido	Bloquear todas las conexiones	Si	Si	4,096

Tabla 9: Estado de configuración recomendado del cortafuegos de Windows



Figura 38: Imposición del cortafuegos de Windows - Captura de pantalla de configuración recomendada

Además, para garantizar que sólo se impongan las reglas del cortafuegos administradas de forma centralizada (y que no puedan ser anuladas por un actor infame), la configuración de "Apply local firewall rules" y "Apply local connection security rules" debe establecerse como "No" para todos los perfiles. (Figura 39).

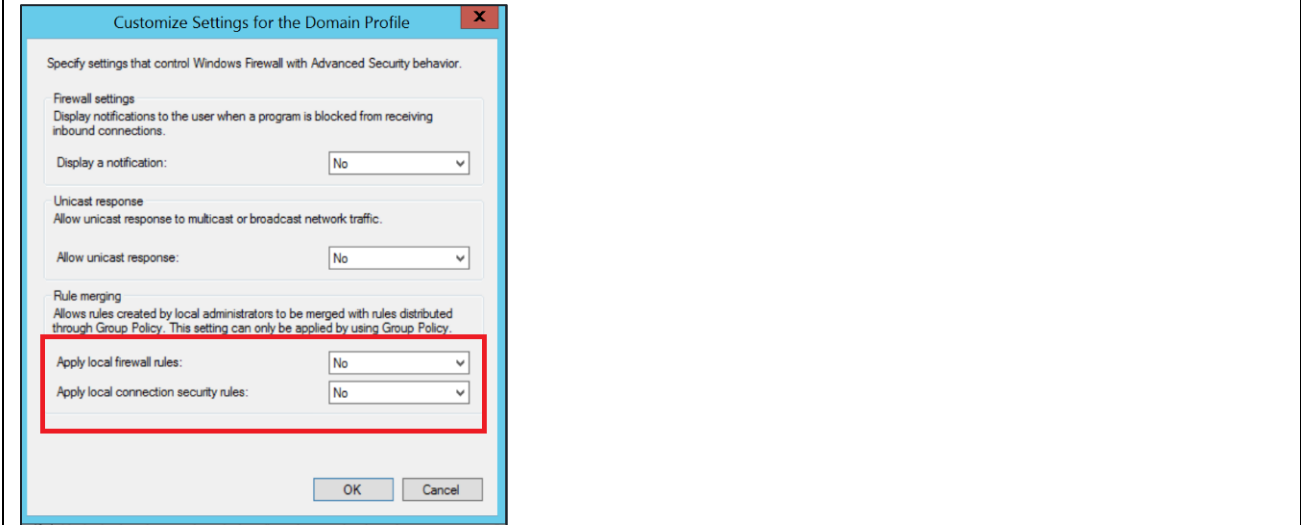


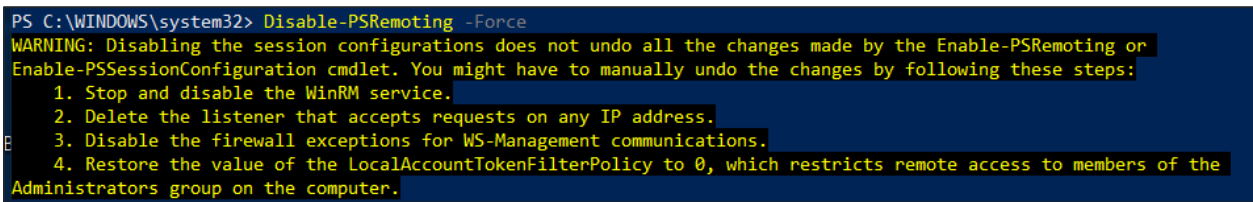
Figura 39: Configuración personalizada del perfil de dominio del cortafuegos de Windows

Para obtener información adicional, consultar:
[https://technet.microsoft.com/en-us/library/cc754274\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc754274(v=ws.11).aspx)
<https://technet.microsoft.com/en-us/library/bb490626.aspx>

Justificación

Imponer las reglas del cortafuegos de Windows centralizado en los puntos finales puede proteger contra un atacante que explota las rutas laterales comunes utilizando puertos y protocolos estándar de Windows.

Acción propuesta	Categorización	Flujo de trabajo
------------------	----------------	------------------

1.3.3 Fortalecimiento de comunicación remota de WinRM/PowerShell	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Nota: Para la siguiente configuración de GPO, se recomienda NO imponer esta configuración para controladores de dominio o servidores Exchange. La configuración de GPO debe probarse primero en una unidad organizativa que contenga un subconjunto de servidores para garantizar que no se observen problemas operativos o de compatibilidad.</p> <p>WinRM está habilitado de forma predeterminada en todos los sistemas operativos de Windows Server (desde Windows Server 2012 y superior) pero deshabilitado en todos los sistemas operativos del cliente (Windows 7 y Windows 10) y plataformas de servidor más antiguas (Windows Server 2008 R2).</p> <p>PowerShell Remoting (PS Remoting) es una función de ejecución de comandos remota nativa de Windows que se basa en el protocolo WinRM.</p> <p>Las plataformas del sistema operativo de cliente Windows (no servidor) donde WinRM está deshabilitado indican:</p> <ul style="list-style-type: none"> No se ha configurado ningún WinRM de escucha No se ha configurado ninguna excepción del cortafuegos de Windows <p>De forma predeterminada, WinRM utiliza los puertos TCP/5985 y TCP/5986, los cuales pueden desactivarse por medio del cortafuegos de Windows o configurarse para que dicho subconjunto específico de direcciones IP pueda autorizarse para conectarse a puntos finales mediante WinRM.</p> <p>WinRM y PowerShell Remoting se pueden deshabilitar explícitamente en el punto final mediante un comando de PowerShell (Figura 40) o una configuración de GPO específica.</p> <p>PowerShell:</p> <p>Disable-PSRemoting -Force</p> <p><i>Figura 40: Comando de PowerShell para deshabilitar la comunicación remota de PowerShell en un punto final</i></p> <p>Nota: La ejecución de Disable-PSRemoting -Force no impide que los usuarios locales creen sesiones de PowerShell en el equipo local o para sesiones destinadas a equipos remotos.</p> <p>Después de ejecutar el comando, se mostrará el mensaje registrado en la Figura 41. Estos pasos proporcionan un refuerzo adicional, pero después de ejecutar el comando Disable-PSRemoting -Force, las sesiones de PowerShell destinadas al punto final de destino no se realizarán correctamente.</p>  <p><i>Figura 41: Mensaje de advertencia después de deshabilitar PSRemoting</i></p> <p>Para imponer los pasos adicionales para deshabilitar WinRM por medio de PowerShell (Figura 42 a Figura 45):</p> <p><i>Detener y deshabilitar el servicio WinRM</i></p> <p>Stop-Service WinRM -PassThruSet-Service WinRM -StartupType Disabled</p> <p><i>Figura 42: Comando de PowerShell para detener y deshabilitar el servicio WinRM</i></p>		

<i>Deshabilitar el oyente que acepta solicitudes en cualquier dirección IP</i>
<pre>dir wsman:\localhost\listener Remove-Item -Path WSMan:\Localhost\listener\<Listener name</pre>
<i>Figura 43: Comandos de PowerShell para eliminar un agente de escucha de WSMAN</i>
<i>Deshabilitar las excepciones del cortafuegos para las comunicaciones de WS-Management</i>
<pre>Set-NetFirewallRule -DisplayName 'Windows Remote Management (HTTP-In)' -Enabled False</pre>
<i>Figura 44: Comando de PowerShell para deshabilitar las excepciones del cortafuegos para WinRM</i>
<i>Restaurar el valor LocalAccountTokenFilterPolicy a 0, el cual restringe el acceso remoto a los miembros del grupo Administrators en la computadora.</i>
<pre>Set-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system -Name LocalAccountTokenFilterPolicy -Value 0</pre>
<i>Figura 45: Comando de PowerShell para configurar la llave de registro para LocalAccountTokenFilterPolicy</i>
<p>Política de grupo:</p> <ul style="list-style-type: none"> Computer Configuration > Políticas > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service > Allow remote server management through WinRM <ul style="list-style-type: none"> Deshabilitado <p>Si esta opción está configurada como "Deshabilitado", el servicio WinRM no responderá a las solicitudes de una computadora remota, independientemente de si se configuraron o no WinRM de escucha.</p> <ul style="list-style-type: none"> Computer Configuration > Políticas > Administrative Templates > Windows Components > Windows Remote Shell > Allow Remote Shell Access <ul style="list-style-type: none"> Deshabilitado <p>Esta configuración de política administrará la configuración del acceso remoto a todos los shells admitidos para ejecutar guiones y comandos.</p> <p>Si sistemas de confianza específicos (ej. hosts de salto administrativos) necesitan establecer una conexión con puntos finales utilizando WinRM, se puede configurar una regla del cortafuegos de Windows, que sólo permite solicitudes entrantes de WinRM desde direcciones IP de origen específicas.</p> <ol style="list-style-type: none"> Computer Configuration > Políticas > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Inbound Rules New Rule > Predefined > Windows Remote Management > Allow the connection Scope tab – Definir la(s) dirección(es) IP de origen específicas donde las conexiones deben originarse por medio de la pestaña "Remote IP address" (Figura 46).

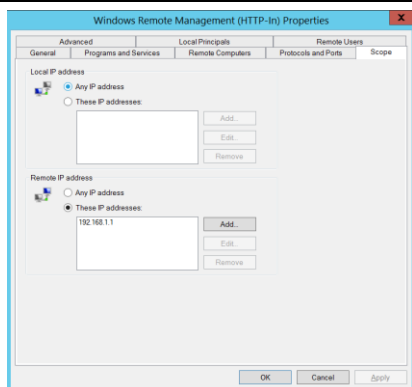


Figura 46: Opción de configuración para restringir WinRM de direcciones IP de origen específicas

Reglas de evasión de autenticación (IPsec) para restringir WinRM:

Además, en un entorno basado en dominio, se puede aprovechar una regla de evasión de autenticación para anular una regla de bloqueo explícita y sólo permitir la conectividad desde los puntos finales y cuentas de origen específicos que utilicen IPsec.

Los siguientes ejemplos de reglas de GPO permitirán la conectividad de WinRM sólo desde un subconjunto específico de cuentas de origen o puntos finales de origen. Además, debe existir una “Regla de seguridad de conexión” predefinida tanto en los puntos finales de origen como en los de destino para solicitar o imponer la autenticación entrante y saliente mediante Kerberos v5 (Figura 47).

Reglas de seguridad de conexión:

- Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Connection Security Rules
- Paso 1: Regla de seguridad de la conexión - Punto final de destino (al que se accederá mediante WinRM)
 - Tipo de regla: Personalizado
 - Punto final 1: Cualquiera
 - Punto final 2: Cualquiera
 - Requisitos - Modo de autenticación: Solicitud de autenticación para configuraciones entrantes y salientes
 - “Require Inbound and Request Outbound” también se puede utilizar en el punto final de destino al que se accederá una vez que se hayan completado las pruebas.
 - Opciones del método de autenticación:
 - Computadora y usuario (Kerberos v5): Sólo debe utilizarse si tanto las computadoras remotas como los usuarios remotos se definirán dentro de una regla del cortafuegos entrante
 - Computadora (Kerberos v5): Sólo debe utilizarse si sólo se definirán computadoras remotas dentro de una regla del cortafuegos entrante
 - Usuario (Kerberos v5): Sólo debe utilizarse si sólo se definirán usuarios remotos dentro de una regla del cortafuegos entrante. Para que los usuarios remotos se autenticuen, la conexión intentará autenticar al usuario actualmente conectado en el punto final de origen. Si se proporcionan credenciales alternativas, la conexión no se realizará correctamente.
 - Tipo de protocolo: TCP
 - Puerto del punto final 1: 5985, 5986

- El punto final 1 debe reflejar los puertos de escucha a los que accederán los sistemas de origen.
- Puerto del punto final 2: Todos los puertos
- Alcance (local): Cualquier dirección IP
- Alcance (remoto): Cualquier dirección IP
- Perfil: Todos
- Nombre: WinRM-Specific-Endpoints

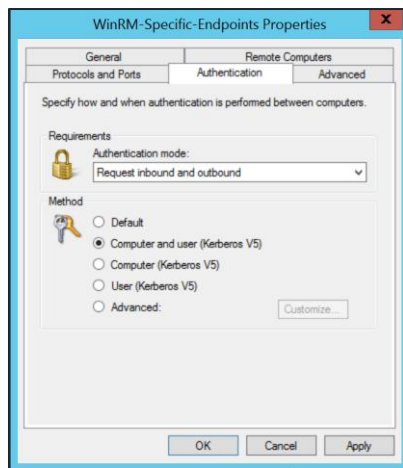


Figura 47: Configuración de autenticación recomendada para la regla de seguridad de conexión si tanto las computadoras como los usuarios se definirán dentro de una regla de entrada para WinRM

- Paso 2: Regla de seguridad de conexión - Punto final de origen (que será un sistema de origen aprobado para conexiones WinRM)
 - Tipo de regla: Personalizado
 - Punto final 1: Cualquiera
 - Punto final 2: Cualquiera
 - Requisitos - Modo de autenticación: Solicitud de autenticación para configuraciones entrantes y salientes
 - Si el lado de destino se configuró como "require", entonces se requerirá la autenticación para la conexión.
 - Opciones del método de autenticación:
 - La opción seleccionada debe coincidir con la opción que se configuró en la regla para el punto final de destino (paso 1 anterior).
 - Tipo de protocolo: TCP
 - Puerto del punto final 1: Todos los puertos
 - Puerto del punto final 2: 5985, 5986
 - El punto final 2 debe reflejar los puertos de destino a los que accederán los sistemas de origen.
 - Alcance (local): cualquier dirección IP
 - Alcance (remoto): cualquier dirección IP
 - Perfil: Todo
 - Nombre: WinRM-Specific-Endpoints
- Paso 3: Crear una regla de entrada para el punto final de destino (a la que se accederá mediante WinRM)

- Computer Configuration > Políticas > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Inbound Rules
 - New Rule > Predefined > Windows Remote Management
 - Seleccionar las casillas de verificación de las casillas Dominio, Privado y Público

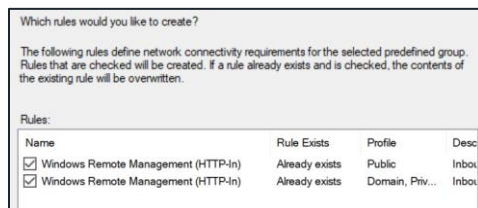


Figura 48: Casillas de verificación de opciones de regla

- Permita la conexión si es segura
 - Customize button – Seleccionar:
 - Permitir la conexión si está autenticada y protegida por integridad
 - Anular reglas de bloqueo

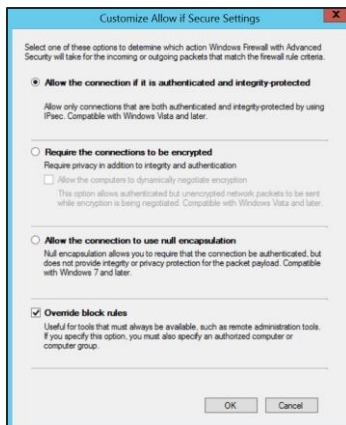


Figura 49: Opciones de configuración recomendadas para la regla WinRM del cortafuegos de Windows

- Seleccionar el alcance de los usuarios autorizados que la regla permitirá para la conectividad por medio de la pestaña "Only allow connections from these users".
 - Estos se enlistarán en la pestaña "Remote Users" de la regla del cortafuegos.
- Seleccionar el alcance de los puntos finales de origen autorizados desde los que la regla permitirá la conectividad por medio de la pestaña "Only allow connections from these computers".
 - Estos se enlistarán en la pestaña "Remote Computers" de la regla del cortafuegos.

Una vez configuradas las reglas, se pueden probar desde un punto final de origen (Figura 50).

Nota: Si se seleccionó la autenticación "user" o "computer and user" en las Reglas de seguridad de conexión, se intentará la autenticación utilizando las credenciales del usuario que ha iniciado sesión

actualmente en el sistema de origen. Si se proporcionan credenciales alternativas, la conexión autenticada fallará.

Enter-PSSession -ComputerName <Destination Endpoint>

Figura 50: Comando para probar WinRM desde un punto final de origen específico

Justificación

Limitar el acceso para cuentas con privilegios y el servicio de gestión remota de Windows (WinRM) puede limitar la propagación del malware y el movimiento lateral en un entorno.

Acción propuesta	Categorización	Flujo de trabajo
1.3.4 Fortalecer el uso del cliente del escritorio remoto en puntos finales	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Si el punto final de un cliente no requiere la capacidad de acceder mediante el escritorio remoto, el cliente de escritorio remoto puede fortalecerse administrativamente para un punto final.</p> <p>Nota: El uso fortalecido del cliente del escritorio remoto mediante la configuración de GPO a la que se hace referencia a continuación no impedirá necesariamente que la capacidad del punto final se utilice para establecer conexiones de escritorio remoto salientes a sistemas adicionales; más bien, el método de GPO deshabilitará al cliente para que los intentos de conectividad de escritorio remoto entrantes no estén permitidos en un punto final.</p> <p>Con una configuración de GPO, las sesiones de escritorio remoto entrantes se pueden evitar en un punto final.</p> <ul style="list-style-type: none">• Computer Configuration > Políticas > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections > Allow users to connect remotely using Remote Desktop Services<ul style="list-style-type: none">○ Deshabilitado <p>Imponer esta configuración dará como resultado que la configuración del registro el cual se indica en la Figura 51 se configure en un punto final.</p>		
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services DWORD Name = fDenyTSConnection Value = "1"		
<p>Figura 51: Valor de registro cuando los servicios de escritorio remoto entrantes están deshabilitados en un punto final</p> <p>Si BanCoppel necesita restringir el acceso al binario integrado de Windows (mstsc.exe) el cual proporciona conectividad de escritorio remoto (ej. saliente a un punto final de destino), AppLocker podría aprovecharse para restringir el acceso para que el binario sea invocado en un punto final.</p> <ol style="list-style-type: none">1. Computer Configuration > Políticas > Windows Settings > Security Settings > Application Control Policies > AppLocker > Executable Rules2. Create New Rule<ol style="list-style-type: none">a. Action: Deny (Everyone user or group)		

b. Path

i. %SYSTEM32%\mstsc.exe

Después de crear la ruta ejecutable y la regla de denegación (y aceptar las reglas de permisos predeterminadas), la configuración representada en la Figura 52 debe estar presente.





Action	User	Name	Condition
 Deny	Everyone	%SYSTEM32%\mstsc.exe	Path
 Allow	Everyone	(Default Rule) All files located in the Windows folder	Path
 Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path
 Allow	BUILTIN\Ad...	(Default Rule) All files	Path

Figura 52: Regla de AppLocker para denegar el acceso al binario mstsc.exe

Después de configurar la regla de AppLocker, si se intenta invocar el binario en un punto final, el resultado debe ser el mensaje que se indica en la Figura 53.

```
C:\WINDOWS\system32>mstsc
This program is blocked by group policy. For more information, contact your system administrator.
```

Figura 53: Intento de ejecución de un binario bloqueado por AppLocker

Nota: Dependiendo del nivel de permisos que se proporciona a una cuenta y en un punto final, se pueden aprovechar los métodos y las herramientas adicionales para crear un túnel o establecer una sesión de escritorio remoto. El ejemplo simple de la regla de AppLocker, proporcionado anteriormente, podría evitarse si un atacante utiliza herramientas adicionales que no se basan en el binario mstsc.exe.

Justificación

Limitar el acceso para cuentas privilegiadas y el servicio de protocolo de escritorio remoto (RDP) puede limitar las capacidades laterales en todo el entorno.

Acción propuesta	Categorización	Flujo de trabajo
1.3.5 Imponer el reprocesamiento automatizado de las políticas de grupo	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Bancoppel debe imponer el reprocesamiento automatizado de las políticas de grupo para todos los puntos finales. Esta función se puede habilitar por medio de la configuración de GPO (a continuación) después de la prueba para comprender los posibles impactos en los dispositivos.</p> <ul style="list-style-type: none">• Computer Configuration > Políticas > Administrative Templates > System > Group Policy > Configure security policy processing<ul style="list-style-type: none">○ Habilitado - Proceso incluso si los objetos de la política de grupo no han cambiado• Computer Configuration > Políticas > Administrative Templates > System > Group Policy > Configure registry policy processing<ul style="list-style-type: none">○ Habilitado - Proceso incluso si los objetos de la política de grupo no han cambiado		

- Computer Configuration > Políticas > Administrative Templates > System > Group Policy > Configure scripts policy processing
 - Habilitado - Proceso incluso si los objetos de la política de grupo no han cambiado

Una vez impuestas, las siguientes llaves de registro, las cuales se indican en la Figura 54, deben configurarse en un punto final.

“Configure security policy processing - Process even if the Group Policy objects have not changed”

HKLM\Software\Policies\Microsoft\Windows\Group Policy\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}

Value Name: NoGPOListChanges

REG_DWORD: “0”

“Configure registry policy processing - Process even if the Group Policy objects have not changed”

HKLM\Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}

Value Name: NoGPOListChanges

REG_DWORD: “0”

“Configure scripts policy processing - Process even if the Group Policy objects have not changed”

HKLM\Software\Policies\Microsoft\Windows\Group Policy\{42B5FAAE-6536-11d2-AE5A-0000F87571E3}

Value Name: NoGPOListChanges

REG_DWORD: “0”

Figura 54: Llaves de registro para aplicar el reprocesamiento automatizado de las políticas de grupo

De forma predeterminada, la configuración de la política de grupo sólo se vuelve a procesar y se vuelve a aplicar si la política de grupo real se modificó antes del intervalo predeterminado de actualización.

Justificación

De forma predeterminada, la configuración de la política de grupo sólo se reprocesa y se vuelve a aplicar si la política de grupo real se modificó antes del intervalo predeterminado de actualización. Una excepción a esta regla son los ajustes de GPO que se configuran dentro de la Extensión de seguridad del lado del cliente (CSE) {827D319E-6EAC-11D2-A4EA-00C04F79F83A}, el cual volverá a aplicar automáticamente TODOS los ajustes configurados cada 16 horas (independientemente de si la política ha cambiado o no).

La configuración de seguridad CSE incluye cualquier cosa configurada dentro de:

- Computer Configuration > Políticas > Windows Settings > Security Settings
- User Configuration > Políticas > Windows Settings > Security Settings

El intervalo de fortalecimiento automático de seguridad CSE (predeterminado 16 horas) se puede configurar mediante la llave de registro, la cual se indica en la Figura 55. El valor decimal de la llave se refleja en minutos (valor predeterminado = 960).

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions

```
\{827D319E-6AC-11D2-A4EA-00C04F79F83A}\MaxNoGPOListChangesInterval
```

Figura 55: Llave de registro del intervalo de refuerzo de seguridad CSE

Un atacante podría, esencialmente, revertir una configuración que se administra de manera centralizada por medio de la Política de grupo (ej. modificando una configuración de registro), y esta configuración no autorizada permanecería efectiva en un punto final hasta que la Política de grupo real la cual controlaba la configuración fuese modificada por un administrador.

Acción propuesta	Categorización	Flujo de trabajo
1.3.6 Deshabilitar SMB v1.0	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>BanCoppel deberá deshabilitar SMB v1.0 en los puntos finales de Windows. SMB v1.0 se puede deshabilitar en los puntos finales mediante PowerShell, una modificación del registro o mediante la plantilla de la política de grupo de la Guía de seguridad de Microsoft.</p>		
<p>La desactivación de SMB v1.0 debe probarse en un pequeño subconjunto de sistemas antes de deshabilitarla en una gama más amplia de sistemas en toda la empresa.</p>		
<p>PowerShell: Para deshabilitar SMB v1.0 en un sistema, ejecutar el cmdlet de PowerShell que se indica a continuación</p>		
<pre>Set-SmbServerConfiguration -EnableSMB1Protocol \$false</pre>		
<p><i>Figura 56: Comando de PowerShell para deshabilitar SMB v1.0</i></p>		
<p>Registro: SMB v1.0 también se puede deshabilitar mediante la modificación del registro, que se puede aplicar de forma centralizada mediante un GPO (Figura 57, Figura 58 y Figura 59).</p>		
<pre>HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters Registry entry: SMB1 REG_DWORD: 0 = Disabled</pre>		
<p><i>Figura 57: Comando de PowerShell para deshabilitar el servidor SMB v1.0 mediante la modificación de la llave del registro</i></p>		
<pre>HKLM\SYSTEM\CurrentControlSet\services\mrxsmb10 Registry entry: Start REG_DWORD: 4 = Disabled</pre>		
<p><i>Figura 58: Comando de PowerShell para deshabilitar el cliente SMB v1.0 mediante la modificación de la llave del registro</i></p>		

```
HKLM\SYSTEM\CurrentControlSet\services\mrxsmb10
Registry entry: Start
REG_DWORD: 4 = Disabled

HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation
Registry entry: DependOnService
REG_MULTI_SZ: "Bowser","MRxSmb20","NSI"
```

Figura 59: Comando de PowerShell para deshabilitar el cliente SMB v1.0 por medio de la llave de registro

Política de grupo:

Con la plantilla de directiva de grupo de la Guía de seguridad de Microsoft, SMB v1.0 se puede deshabilitar por medio de la configuración de GPO (Figura 60 a Figura 62):

- Computer Configuration > Políticas > Administrative Templates > MS Security Guide > Configure SMB v1 Server
 - Deshabilitado

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

Figura 60: Deshabilitar el servidor SMB v1 por medio de la plantilla de la política de grupo de la Guía de seguridad de MS

- Computer Configuration > Políticas > Administrative Templates > MS Security Guide > Configure SMB v1 Client Driver
 - Habilitado
 - Configurar el controlador MrxSMB10
 - Deshabilitar el controlador

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

Figura 61: Deshabilitar el controlador de cliente SMB v1 por medio de la plantilla de la política de grupo de la Guía de seguridad de MS

Configure SMB v1 client driver

☐ Not Configured

Comment:

☒ Enabled

☐ Disabled

Supported on:

At least Windows

Options:

Configure MrxSmb10 driver

Disable driver (recommended)

Figura 62: Deshabilitar el controlador de cliente SMB v1 por medio de la plantilla de la política de grupo de la guía de

seguridad de MS, configuración adicional

- Computer Configuration > Policies > Administrative Templates > MS Security Guide > Configure SMB v1 Client (configuración adicional necesaria para versiones anteriores a Win8.1/2012R2)
 - Habilitado
 - Configurar las dependencias de LanmanWorkstation
 - Bowser
 - MrxSMB20
 - NSI

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

Figura 63: Deshabilitar la configuración adicional del cliente SMB v1 por medio de la plantilla de la política de grupo de la Guía de seguridad de MS

Para habilitar la auditoría de SMB, seguir la siguiente guía:

<https://blogs.technet.microsoft.com/leesteve/2017/05/11/detecting-and-remediating-smbv1/>

Para obtener información adicional, consultar:

<https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012>

Debido a las aplicaciones heredadas y a la tecnología más antigua que pueden estar presentes en el entorno, la desactivación global de SMB v1.0 podría generar impactos operativos dentro del entorno administrado.

Microsoft ahora proporciona una plantilla de GPO, la cual se puede aprovechar para deshabilitar SMB v1.0. El GPO puede dirigirse a un nivel específico de puntos finales para realizar pruebas. Esto puede reducir el nivel de esfuerzo necesario para aplicar esta configuración de forma eficaz en los puntos finales por medio de un mecanismo centralizado.

Justificación

SMB v1.0 proporciona un vector de ataque y está sujeto a varias vulnerabilidades que se han liberado públicamente.

Fortalecimiento: Red Hat Enterprise Linux

Acción propuesta	Categorización	Flujo de trabajo
1.4.1 Habilitar el registro centralizado	Fortalecimiento de Linux	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>BanCoppel debe configurar los sistemas Linux para reenviar las bitácoras a una ubicación centralizada y segura. Los servicios más comunes de registro basados en Linux son rsyslog, syslog y syslog-ng.</p> <p>Se deben considerar los siguientes puntos para garantizar que el registro se implemente de manera adecuada</p> <ul style="list-style-type: none"> Debe asegurarse de que en el archivo de configuración respectivo de cada bitácora, la fuente de datos esté configurada correctamente y que las bitácoras se reenvíen al lugar correcto La plataforma de registro centralizada debe configurarse para recibir las bitácoras. El análisis y la normalización de las bitácoras deben configurarse adecuadamente Las reglas basadas en lo que BanCoppel busca encontrar deben configurarse en la plataforma de registro y alerta. Por ejemplo, un enfoque beneficioso puede ser crear alertas para la creación de cron jobs o múltiples intentos fallidos de ejecutar comandos como root. <p>La siguiente lista proporciona algunas de las bitácoras que deben recolectarse y revisarse:</p> <ul style="list-style-type: none"> Intentos de autenticación exitosos y fallidos, con prioridad en los servicios de red los cuales pueden proporcionar acceso administrativo, como SSH Uso de cuentas con privilegios de root, como el comando "su" (ej. Registro de "sudoers") Conexiones entrantes denegadas (ej. aquellas bloqueadas por iptables) Historial de comandos (ej. bitácoras del historial shell) <p>El servicio rsyslog incorporado de RHEL se puede utilizar para configurar y administrar el registro centralizado para los sistemas RHEL.</p> <p>Rsyslog admite tres formatos de configuración diferentes: básico, avanzado y obsoleto. Se recomienda encarecidamente que sólo se utilice el formato de configuración avanzada, siempre que sea posible, y que la versión de rsyslog se actualice al menos a la v7 si es compatible.</p> <p>La siguiente configuración de muestra está en formato avanzado y se proporciona para rsyslog versión 7.0 y superior. La configuración se proporciona como muestra y debe adaptarse al entorno.</p> <p>Rsyslog debe ejecutarse y configurarse tanto en el servidor del registro central el cual recibe los mensajes de bitácora como en el servidor del cliente donde se originan los mensajes de bitácora.</p> <p>El siguiente comando se puede utilizar para instalar rsyslog en una máquina RHEL:</p> <pre># yum install rsyslog</pre>		

Figura 64: Instalar rsyslog

Se puede configurar un cliente para enviar bitácoras a un servidor central configurando los ajustes en un archivo de configuración creado en el directorio `/etc/rsyslog.d`¹ en el sistema del cliente.

```

*. * action(type="omfwd"
    queue.type="linkedlist"
    queue.filename="<filename for queue> "
    action.resumeRetryCount="-1"
    queue.saveOnShutdown="on"
    target="<ServerIP>" port="<Port Num>" protocol="tcp"
)

```

Figura 65: Ejemplo de configuración del cliente rsyslog

El servicio rsyslog también debe configurarse en el servidor de registro central. Para lograr esto, se puede crear un archivo de configuración rsyslog con extensión `.conf` en el directorio `/etc/rsyslog.d` en el servidor.

Un archivo de configuración rsyslog de servidor puede contener varias secciones de plantilla, un conjunto de reglas y configuraciones de red.

Las plantillas² se pueden declarar en el archivo de configuración para las bitácoras entrantes. La siguiente configuración de muestra se puede utilizar para una declaración de plantilla.

```

template(name="<Template Name>" type="list") {
    constant(value="/var/log/remote/auth/")
    property(name="hostname")
    constant(value="/")
    property(name="programname" SecurePath="replace")
    constant(value=".log")
}

```

Figura 66: Plantilla de definición de configuración de muestra para la configuración del servidor rsyslog

A continuación, se puede definir un conjunto de reglas³ para procesar mensajes en función de las plantillas definidas. A continuación, se proporciona un conjunto de reglas de muestra que puede procesar los archivos de bitácora recibidos según la plantilla definida anteriormente. Un conjunto de reglas puede tener varias entradas asignadas a las plantillas.

```

ruleset(name="<Ruleset Name>"){
    authpriv.*    action(type="omfile" DynaFile="<Template Name>"
}

```

Figura 67: Configuración de muestra el cual define el conjunto de reglas para el servidor rsyslog

Rsyslog admite tanto TCP como UDP para el transporte de bitácoras. Se recomienda TCP ya que TCP es más estable y ofrece una entrega confiable. A continuación, se puede agregar el siguiente

¹ https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/configuring-a-remote-logging-solution_configuring-basic-system-settings

² <https://www.rsyslog.com/doc/v8-stable/configuration/templates.html>

³ https://www.rsyslog.com/doc/v8-stable/concepts/multi_ruleset.html

ajuste para configurar la recepción de syslog TCP en el archivo de configuración rsyslog del servidor el cual proporciona la asignación al conjunto de reglas definido.

```
#Config to load and configure TCP logging
module(load="imtcp")
input(type="imtcp" port="<Port Num>" ruleset="<RuleSet Name>")
```

Figura 68: Configuración de muestra el cual define la recepción de registros TCP para el conjunto de reglas remote1

Aplicabilidad: RHEL 5, 6, 7, 8

Justificación

Es posible que los atacantes con acceso privilegiado en máquinas Linux borren las bitácoras almacenadas localmente. Una solución de registro centralizada envía las bitácoras desde los puntos finales y almacena las bitácoras en un servidor central. Esto dificulta que un atacante elimine las bitácoras de las actividades que realizó en la máquina.

Acción propuesta	Categorización	Flujo de trabajo
1.4.2 Configurar la auditoría del sistema	Fortalecimiento de Linux	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>BanCoppel debería considerar implementar la auditoría del sistema Linux utilizando el sistema de auditoría Linux. La auditoría del sistema se enfoca en detectar cualquier violación de la política de seguridad actual implementada en un sistema Linux.</p> <p>La auditoría del sistema podrá monitorear el sistema para cosas como:</p> <ul style="list-style-type: none"> • Modificación de la configuración de auditoría y archivos de registro de auditoría • Cambios en bases de datos confiables (ej. "/etc/passwd") • Intenta exportar información fuera del sistema • Cambios en los mecanismos de autenticación de usuarios (ej. SSH) <p>Las siguientes referencias se pueden consultar durante la configuración de los servicios de auditoría:</p> <ul style="list-style-type: none"> • RHEL 5: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/5/html/5.5_technical_notes/audit • RHEL 6.10: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-configuring_the_audit_service • RHEL 7: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/chap-system_auditing • RHEL 8: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/auditing-the-system_security-hardening <p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		
Justificación		

El servicio de auditoría puede mejorar la visibilidad de los defensores en el sistema Linux. Esto podría ayudar a detectar cualquier actividad maliciosa que los adversarios puedan estar realizando en el sistema.

Acción propuesta	Categorización	Flujo de trabajo
1.4.3 Configurar el registro de fecha de la ejecución de la bitácora en el historial Shell	Fortalecimiento de Linux	Registro y monitoreo - Visibilidad
Detalles de la recomendación		
<p>Los sistemas Linux almacenan los comandos ejecutados por un usuario en un archivo oculto ".bash_history" específico del usuario almacenado en el directorio de inicio del usuario. Este archivo puede proporcionar información importante en caso de un incidente de seguridad. Se proporcionan las siguientes recomendaciones para mejorar la función de registro de historial en los sistemas RHEL.</p> <p>Una limitación de la grabación predeterminada del historial shell en Linux es que el archivo del historial no contiene registros de fechas. BanCoppel deberá habilitar esto configurando una variable "HISTTIMEFORMAT" en el sistema. El archivo ".bash_profile" en el directorio de inicio del usuario se puede utilizar para configurar esto cada vez que el usuario inicia sesión.</p>		
<pre>echo 'export HISTTIMEFORMAT="%d/%m/%y %T "' >> ~/.bash_profile</pre>		
<p><i>Figura 69: Comando para configurar la variable \$HISTTIMEFORMAT en el archivo .bash_profile</i></p>		
<p>El tamaño predeterminado del archivo del historial en RHEL es de 1000 líneas. Esto significa que cualquier comando que sea anterior a los últimos 1,000 comandos se eliminará del archivo del historial. Se recomienda aumentar la longitud del archivo histórico; esto se puede realizar configurando las variables HISTSIZE y HISTFILESIZE en el sistema. El siguiente comando configurará las variables en el archivo de perfil de bash del usuario y aumentará el tamaño del archivo del historial a ilimitado.</p>		
<pre>echo 'export HISTSIZE= ' >> ~/.bash_profile echo 'export HISTFILESIZE= ' >> ~/.bash_profile</pre>		
<p><i>Figura 70: Comandos para configurar un tamaño ilimitado de archivo del historial en RHEL</i></p>		
<p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		
Justificación		
<p>Los registros de fechas, en el archivo bash_history, son pruebas muy valiosas las cuales proporcionan información temporal significativa en caso de una investigación. Los comandos en el archivo bash_history pueden sobrescribirse, resultando en la pérdida de evidencia si el tamaño del archivo histórico no es el adecuado.</p>		

Acción propuesta	Categorización	Flujo de trabajo
------------------	----------------	------------------

1.4.4	Habilitar la grabación de sesiones	Fortalecimiento de Linux	Registro y monitoreo - Visibilidad
Detalles de la recomendación			
<p>BanCoppel deberá considerar la posibilidad de habilitar la grabación de sesiones de usuario. La grabación de sesiones de usuario permite a los administradores grabar y reproducir sesiones de terminal de usuario. Todas las grabaciones se capturan y almacenan en formato de texto en el diario del sistema. Estos datos se pueden utilizar para auditar las sesiones de los usuarios o realizar análisis forenses en caso de un incidente de seguridad.</p> <p>Red Hat proporciona documentación⁴ detallada sobre cómo habilitar y configurar la grabación de sesiones en un sistema RHEL.</p> <p>Aplicabilidad: RHEL 8</p>			
Justificación			
<p>Los atacantes a menudo obtienen acceso de terminal a máquinas Linux y realizan actividades maliciosas. Mientras que el archivo ".bash_history" registra todos los comandos que un usuario ha ejecutado en una ventana de terminal, la salida de los comandos no se registra. Además, cuando las empresas de servicios públicos tienen sus propias sesiones, los comandos y las actividades no se registran. En tales casos, la grabación de la sesión puede proporcionar registros detallados de la actividad del usuario o del adversario.</p>			

Acción propuesta	Categorización	Flujo de trabajo
1.4.5 Imponer contraseñas seguras	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Cuentas
Detalles de la recomendación		
<p>BanCoppel deberá considerar la implementación de mecanismos para garantizar que se utilicen contraseñas seguras en todos los sistemas instalados de RHEL.</p> <p>El módulo "Pam_cracklib.so" disponible en RHEL Linux verifica la fuerza de las contraseñas y se puede configurar.</p> <p>Se recomiendan las siguientes configuraciones en el archivo de configuración de autenticación del sistema ("/etc/pam.d/system-auth") y el archivo de autenticación de contraseña ("/etc/pam.d/password-auth").</p> <p>Se sugiere la siguiente configuración para establecer los requisitos mínimos de contraseña para todos los usuarios; Se recomienda configurar la longitud de la contraseña con un mínimo de 14 caracteres.</p> <pre>password requisite pam_cracklib.so try_first_pass retry=3 minlen=14 dcredit=- 1 ucredit=-1 ocredit=-1 lcredit=-1</pre>		

⁴https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/recording_sessions/index

Figura 71: Configuración para la aplicación de contraseña en RHEL

Se recomiendan las siguientes configuraciones para habilitar el bloqueo de contraseña para intentos fallidos de contraseña. La siguiente configuración establecerá el bloqueo de la cuenta en cinco inicios de sesión fallidos.

```
auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900
auth [success=1 default=bad] pam_unix.so
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900
```

Figura 72: Habilitar bloqueo para intentos fallidos de contraseña

La siguiente configuración evitará el bloqueo de la cuenta raíz como resultado de la configuración del bloqueo de contraseña:

```
"auth required /lib/security/$ISA/pam_tally.so onerr=fail no_magic_root"
```

Figura 73: Configuración para proteger la cuenta raíz del bloqueo

La siguiente configuración garantizará el uso del algoritmo hash sha512 para la configuración de contraseñas

```
password sufficient pam_unix.so sha512
```

Figura 74: Configurar el uso de sha512 para el hash de contraseñas

Las cuentas que están inactivas durante un período prolongado deben auditarse y desactivarse mensualmente. El siguiente comando se puede utilizar para identificar la última fecha de inicio de sesión de un usuario.

```
lastlog
```

Figura 75: Comando para verificar la última fecha de inicio de sesión de todos los usuarios

Se recomienda que la contraseña se cambie, como mínimo, cada año para cualquier cuenta privilegiada.

Justificación

Los atacantes suelen adivinar o descifrar contraseñas para acceder a los sistemas. Las contraseñas seguras pueden proteger contra ataques de descifrado y adivinación de contraseñas.

Aplicabilidad: RHEL 5, 6, 7, 8

Acción propuesta	Categorización	Flujo de trabajo
1.4.6 Cuentas seguras del sistema	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Cuentas
Detalles de la recomendación		
Varias cuentas en sistemas Linux se utilizan para administrar aplicaciones y, por lo tanto, no es necesario que proporcionen un shell interactivo cuando se utilicen. Se recomienda establecer el		

campo shell en el archivo "/etc/passwd" en "/sbin/nologin". Esto deshabilitará el acceso al shell para un usuario configurado. Se recomienda identificar cualquier cuenta que no requiera acceso interactivo al sistema y deshabilitar el acceso shell para las cuentas.

El siguiente comando se puede utilizar para configurar el shell como "/sbin/nologin" para cualquier usuario que se identifique como que no requiere acceso interactivo:

```
usermod -s /sbin/nologin <user>
```

Figura 76: Comando para configurar el shell para un usuario como /sbin/nologin donde <user> es el nombre de usuario

Aplicabilidad: RHEL 5, 6, 7, 8

Justificación

Los atacantes a veces utilizan el shell de cuentas de servicio y sistemas con acceso interactivo a un sistema para interactuar con el sistema. Estas cuentas suelen tener privilegios y las contraseñas rara vez se cambian. Configurar el shell en "/sbin/nologin" no permite a los usuarios realizar un inicio de sesión interactivo en un sistema utilizando cuentas del sistema.

Acción propuesta	Categorización	Flujo de trabajo
1.4.7 Imponer una máscara predeterminada de archivo	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL – Sistema de archivos
Detalles de la recomendación		
<p>El valor predeterminado de umask en el sistema Linux define los permisos de los archivos nuevos que crea el usuario. Se recomienda asegurarse de que el valor umask esté establecido al menos en 0027 o más restrictivo. El valor umask de 0027 permite a los usuarios del mismo grupo leer y ejecutar los archivos, pero mantiene los archivos accesibles para cualquier otro usuario del sistema.</p> <p>El siguiente comando se puede utilizar para revisar el valor umask configurado para un usuario:</p> <pre>umask</pre> <p><i>Figura 77: Comando para revisar la configuración umask</i></p> <p>Se puede ejecutar el siguiente comando, el cual agregará umask 0027 al archivo "bash_profile" específico de un usuario. Esto asegurará que umask se establezca cada vez que un usuario inicie sesión en el sistema si se está utilizando bash shell. Es posible que se requieran otros ajustes de configuración para otros shells que pueden utilizarse en el entorno.</p> <pre>echo 'umask 0027' >> ~/.bash_profile</pre> <p><i>Figura 78: Configuración para establecer el valor umask para un usuario</i></p> <p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		
Justificación		

Un umask no restrictivo puede exponer archivos en el sistema y hacerlos accesibles a cualquier usuario que tenga acceso al sistema. Los atacantes suelen buscar archivos con permisos de archivo no restrictivos como parte de las actividades de reconocimiento y recolección de la información para buscar datos que puedan ayudarlos en el ataque. Un valor umask restrictivo impuesto garantiza que los archivos no puedan ser leídos por todos.

Acción propuesta	Categorización	Flujo de trabajo
1.4.8 Habilitar funciones anti explotación	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - SO
Detalles de la recomendación		
<p>La aleatorización del diseño del espacio de direcciones (ASLR) garantiza que la dirección base de un ejecutable y otras áreas de proceso de datos clave de un proceso en ejecución sean aleatorias. ASLR protege contra una serie de técnicas de explotación que tienen como objetivo la corrupción de la memoria. Se recomienda habilitar ASLR para proteger mejor los sistemas contra ataques de corrupción de memoria.</p> <p>La siguiente configuración se puede agregar en “/etc/sysctl.conf” para habilitar ASLR en máquinas RHEL. Establecer el valor en “2”, para la variable, habilitará la aleatorización completa para ASLR.</p> <pre>kernel.randomize_va_space = 2</pre> <p><i>Figura 79: Parámetro para habilitar ASLR en RHEL</i></p> <p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		
Justificación		
<p>Los atacantes suelen utilizar explotaciones para obtener acceso o aumentar los privilegios en una máquina Linux. ASLR puede reducir la superficie de ataque para tales ataques y dificultar el trabajo de los atacantes.</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.4.9 Proteger el servicio SSH	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Servicios
Detalles de la recomendación		
<p>Secure Shell (SSH) se utiliza, a menudo, para administrar y acceder a servidores Linux.</p> <p>Se recomienda que BanCoppel defina las políticas y los procedimientos para mitigar las vulnerabilidades significativas las cuales pueden surgir debido a fallas dentro de la implementación y gestión de SSH en el entorno.</p>		

Se debe habilitar el acceso con privilegios mínimos para todas las cuentas y grupos accesibles por SSH, especialmente para procesos automatizados y acceso remoto.

También se recomienda limitar el acceso al servidor por medio de SSH sólo a cuentas de usuarios autenticados ajenos a root. La autenticación criptográfica basada en llaves públicas se puede configurar junto con la contraseña para habilitar la autenticación multi factor y proteger el acceso al servicio SSH configurado en el sistema.

La directiva de configuración "AuthenticationMethods" en el archivo "/etc/ssh/sshd_config" se puede utilizar para especificar los métodos de autenticación que se deben utilizar. <CLIENTE> debe considerar definir más de un método de autenticación para lograr la autenticación de múltiples factores en el sistema.

Todos los usuarios requerirán la creación de pares de llaves públicas-privadas, y las llaves deberán agregarse al servidor antes de que la autenticación basada en llaves sea obligatoria en un servidor. La siguiente entrada en el archivo "/etc/ssh/sshd_config" requerirá que el usuario realice una autenticación basada en llave pública y contraseña, implementando la autenticación multi factor en el sistema:

```
AuthenticationMethods publickey,password
```

Figura 80: Habilitar la autenticación basada en llaves y contraseñas

Los métodos anteriores también deben habilitarse en el archivo de configuración sshd agregando las siguientes líneas:

```
PubkeyAuthentication yes
PasswordAuthentication yes
```

Figura 81: Habilitación de la autenticación basada en llaves y contraseñas

Se deben considerar los cortafuegos basados en el host para limitar los hosts que pueden conectarse al servicio SSH en un servidor. Esto se recomienda encarecidamente para cualquier servidor que tenga un servicio SSH expuesto a Internet. Iptables o nftables son utilerías de Linux disponibles en varios sistemas Linux los cuales se pueden utilizar para configurar el filtrado de paquetes IP y limitar el acceso SSH desde un conjunto limitado de sistemas. Se debe registrar cualquier intento de conexión que no esté autorizado.

Alternativamente, las coberturas TCP podrán utilizarse para implementar sistemas de filtrado y limitación las cuales pueden acceder al servicio SSH. La cobertura TCP funciona con dos archivos: "/etc/hosts.allow" y "/etc/hosts.deny". Se recomienda agregar "TODOS" los hosts al archivo "deny" y sólo los hosts autorizados al archivo "hosts.allow".

Los servidores SSH expuestos públicamente a menudo son objetivos de ataques de adivinación de contraseñas. Los servidores SSH internos deben tener un mayor grado de criticidad asociado. Si existe algún inicio de sesión fallido o intentos de conexión a un servidor SSH interno, debe investigarse.

Se recomienda deshabilitar la capacidad de los administradores para iniciar sesión como root directamente utilizando SSH. Un administrador debe iniciar sesión como usuario normal y, posteriormente, ejecutar comandos que requieran acceso con privilegios utilizando el comando "sudo" para obtener derechos elevados. La directiva "PermitRootLogin" se puede establecer como "No" en el archivo "/etc/ssh/sshd_config" para imponer esto.

```
PermitRootLogin No
```

Figura 82: Deshabilitar la capacidad para que un usuario root inicie sesión directamente utilizando SSH

<CLIENTE> debe deshabilitar el uso de contraseñas vacías para cualquier usuario SSH. Esto se puede configurar estableciendo la directiva "PermitEmptyPasswords" en el archivo "/etc/ssh/sshd_config", como se indica a continuación.

```
PermitEmptyPasswords No
```

Aplicabilidad: RHEL 5, 6, 7, 8

Justificación

Secure Shell (SSH) es un método de uso común para permitir el acceso interactivo con el fin de interactuar y administrar servidores Linux. Los atacantes a menudo utilizan SSH para obtener acceso inicial, mantener persistencia y moverse lateralmente.

Acción propuesta	Categorización	Flujo de trabajo
1.4.10 Limitar los puertos abiertos y los servicios	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Servicios
Detalles de la recomendación		
<p>Cualquier servicio de red que no sea necesario en un sistema debe desactivarse. Los procesos de escucha en la red se pueden enlistar ejecutando el siguiente comando con privilegio de root:</p> <pre>netstat -pantu grep LISTEN</pre> <p><i>Figura 83: Comando para enlistar los servicios de escucha</i></p> <p>Algunas de las posibles formas de deshabilitar servicios en sistemas Linux se enlistan a continuación. Si un servicio es administrado por inetd, el puerto puede cerrarse buscando la línea relevante en el archivo de configuración "/etc/inetd.conf" para el servicio y comentándolo.</p> <p>Xinetd fue creado como reemplazo de inetd. Tiene funciones de seguridad integradas, por lo que ya no se requiere un software adicional. El servidor Xinetd utiliza el directorio "/etc/xinetd.d", el cual contiene archivos relacionados con los diferentes servicios que administra el servidor. Cada archivo debe modificarse para administrar los servicios que se ejecutan con Xinetd.</p> <p>También se recomienda utilizar un cortafuegos basado en host como iptables para restringir el acceso a servicios que no son necesarios como parte del negocio en RHEL 6 y 7. En el caso de RHEL 8, el marco nftables ha reemplazado a iptables como la función de filtrado de paquetes predeterminado y deberá ser utilizado.</p> <p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		
Justificación		
<p>Los atacantes a menudo buscan servicios de escucha en un sistema y acceden o explotan estos para obtener acceso al sistema.</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.4.11 Revisar los Cron Jobs	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL – Servicios
Detalles de la recomendación		
<p>Los cron jobs se utilizan para establecer tareas programadas. Se recomienda que BanCoppel enliste y revise periódicamente todos los cron jobs configurados en la máquina y se asegure de que estén autorizados.</p> <p>El siguiente comando se puede utilizar para enlistar todos los cron jobs enlistados en una máquina para un usuario específico:</p> <pre>crontab -u <username> -l</pre> <p><i>Figura 84: Listado de Cronjobs para un usuario</i></p> <p>El siguiente comando se puede utilizar para enlistar todos los cron jobs configurados en el sistema:</p> <pre>ls -al /etc/cron.d</pre> <p><i>Figura 85: Enlistar todos los cron jobs enlistados en un sistema</i></p> <p>Estos cron jobs deben revisarse para ver el binario que ejecutan al ver el contenido de los archivos cron. Deben identificarse los archivos que se están ejecutando mediante cron jobs; estos archivos sólo deben ser modificables por el usuario root. Los permisos completos para el archivo ejecutable se pueden enlistar utilizando el siguiente comando:</p> <pre>ls -al <Full path of the binary></pre> <p><i>Figura 86: Listado completo de permisos para un binario</i></p> <p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		
Justificación		
<p>Los adversarios suelen utilizar los cron jobs para persistir en una máquina Linux. Los cron jobs también se pueden utilizar para realizar una escalación de privilegios en el sistema.</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.4.12 Revisar y documentar cuentas privilegiadas	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Cuentas
Detalles de la recomendación		
<p>BanCoppel debe revisar y documentar las cuentas configuradas en los sistemas RHEL Server. Las cuentas en Linux se enlistan en el archivo “/etc/passwd”. Este archivo debe revisarse para asegurarse de que todas las cuentas estén autorizadas.</p>		

El sistema Linux utiliza el valor UID (identificador de usuario) para identificar a un usuario. Cualquier cuenta de usuario que tenga el valor UID establecido en 0 tendrá privilegios de root. BanCoppel debe asegurarse de que el único usuario configurado en un sistema con UID 0 sea la cuenta predeterminada de root. El siguiente comando se puede utilizar para identificar cuentas que tienen un valor UID establecido en 0:

```
cat /etc/passwd | awk -F: '($3 == 0) { print $1 }'
```

Figura 87: Identificar usuarios con UID 0

El comando Sudo permite a los usuarios ejecutar programas con los privilegios de seguridad de otro usuario; de forma predeterminada, sudo ejecuta comandos con privilegios de super usuario. El acceso al privilegio sudo se gestiona por medio del archivo "/etc/sudoers". De manera alternativa, las entradas de archivo también se pueden crear en la carpeta "/etc/sudoers.d" para proporcionar acceso sudo a un usuario. BanCoppel debe revisar el archivo sudoers y la carpeta sudoers.d para identificar cualquier grupo que pueda tener acceso a sudo. Se debe revisar la pertenencia a cualquier grupo que tenga acceso a sudo.

En RHEL, el grupo "wheel" tiene acceso sudo en la configuración predeterminada. El siguiente comando se puede utilizar para identificar a todos los miembros de un grupo en el sistema RHEL:

```
grep '<groupname>' /etc/group
```

Figura 88: Lista de todos los miembros del grupo wheel

Aplicabilidad: RHEL 5, 6, 7, 8

Justificación

Para realizar la remediación y garantizar la completa erradicación, es imperativo identificar las cuentas privilegiadas en los servidores. Esta actividad ayudará a BanCoppel a identificar las cuentas que no son necesarias y que se pueden eliminar del sistema.

Si un atacante tiene un acceso shell limitado en un sistema, este puede abusar de los derechos de sudo para escalar privilegios en el sistema. Los derechos de sudo deben controlarse estrictamente y no proporcionarse si no es necesario.

Acción propuesta	Categorización	Flujo de trabajo
1.4.13 Identificar y revisar los ejecutables SUID	Postura	Fortalecimiento del servidor RHEL - Cuentas
Detalles de la recomendación		
SUID (Establecer ID de usuario de propietario en ejecución) es un permiso de archivo que se puede configurar. Cuando se establece, el archivo se ejecutará con los permisos del propietario. BanCoppel deberá revisar todos los archivos del sistema para el conjunto de bits SUID.		
El siguiente comando se puede utilizar para buscar ejecutables SUID en un sistema:		
<pre>find / -perm -u=s -type f 2>/dev/null</pre>		
<i>Figura 89: Comando para buscar ejecutables SUID</i>		

La lista de archivos identificados debe revisarse para cualquier programa que pudiese permitir que un usuario escape a un shell. También se debe revisar cualquier editor, compilador o intérprete de archivos que pueda utilizarse para leer o sobrescribir un archivo. Los permisos deben eliminarse para dichos archivos.

Aplicabilidad: RHEL 5, 6, 7, 8

Justificación

Los atacantes suelen utilizar los archivos SUID para escalar los privilegios y realizar actividades maliciosas en el sistema.

Acción propuesta	Categorización	Flujo de trabajo
1.4.14 Monitoreo de integridad de archivos (FIM)	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL – Sistema de archivos
Detalles de la recomendación		
<p>BanCoppel deberá considerar implementar el monitoreo de la integridad de los archivos. El monitoreo de la integridad de los archivos se puede utilizar para realizar un seguimiento y auditar las modificaciones de los archivos. Esto debe implementarse para archivos críticos del sistema y de la empresa.</p> <p>Algunas de las carpetas y archivos del sistema las cuales se pueden monitorear para cualquier modificación de archivo son:</p> <ul style="list-style-type: none"> • /bin • /boot • /etc • /sbin • /usr/bin • /usr/local/bin • /usr/local/sbin • /usr/sbin • /usr/share/keyrings • /var/spool/cron <p>BanCoppel debe implementar FIM para cualquier directorio o archivo que sea crítico para el sistema o el negocio. RHEL admite la solución de monitoreo de integridad de archivos Tripwire⁵</p> <p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		
Justificación		

⁵ <https://www.redhat.com/sysadmin/security-monitoring-tripwire>

Los atacantes a menudo modifican los archivos del sistema para realizar sus objetivos. Los sistemas de monitoreo de integridad de archivos pueden monitorear archivos críticos para detectar cualquier cambio y alertar si se detecta algún cambio. Esto puede ayudar a identificar cualquier cambio malicioso en el sistema.

Acción propuesta	Categorización	Flujo de trabajo
1.4.15 Eliminar los shells innecesarios o no utilizados de los sistemas Linux	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - SO
Detalles de la recomendación		
<p>Para cada binario de shell instalado en el servidor, BanCoppel debe evaluar los requisitos comerciales y el riesgo que representa para la red. Si se encuentra que un binario shell excede el requisito, BanCoppel deberá eliminar el binario shell del sistema en cuestión.</p> <p>BanCoppel debe verificar si el shell predeterminado de la cuenta root ha sido reemplazado por otro binario de shell. Esto podría causar un daño irreparable a la cuenta de root si el shell en cuestión fuera eliminado del sistema afectado.</p> <p>Esto se puede verificar ejecutando el siguiente comando en un sistema Linux y verificando el valor de shell configurado para la cuenta raíz:</p> <pre>\$ grep '^root' /etc/passwd</pre> <p><i>Figura 90: Comando para verificar la entrada del shell para la cuenta root</i></p>		
Justificación		
<p>Puede que no sea necesario tener varios binarios separados de shell instalados en un servidor. Tener varios shells en un sistema aumenta el riesgo para un sistema y una red más amplia. Un actor de amenazas podría obtener acceso a una instancia de shell en un sistema comprometido y borrar el historial de shell y cualquier actividad del atacante de instancias separadas de shell.</p> <p>Si bien esta configuración se considera una amenaza de bajo impacto, esta podría permitir que un actor de amenazas oculte sus acciones dentro de la red.</p> <p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		

Acción propuesta	Categorización	Flujo de trabajo
1.4.16 Implementar SELinux	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - SO
Detalles de la recomendación		

Security Enhanced Linux (SELinux) es un módulo de kernel cargable que ha sido diseñado para la seguridad; implementa el control de acceso obligatorio y permite un control granular sobre a qué pueden acceder los usuarios en un sistema Linux. SELinux verifica los permisos cuando una aplicación o proceso realiza una solicitud para acceder a un objeto. SELinux puede entonces auditar o imponer dicha solicitud.

SELinux requiere una configuración detallada y un esfuerzo considerable durante la fase de implementación y debe tenerse en cuenta si existe varios usuarios que utilizan el mismo sistema. También se recomienda implementar SELinux en modo permisivo, que sólo registrará los mensajes. Una vez que se ha probado el modo permisivo de SELinux, la implementación se puede mover al modo de aplicación.

Red Hat proporciona documentación detallada sobre cómo se puede configurar e implementar SELinux en un servidor Red Hat. Este documento se puede consultar mientras se configura SELinux.

Aplicabilidad: RHEL 5, 6, 7, 8

Justificación

SELinux puede mejorar las soluciones de seguridad existentes implementadas en el sistema Linux. También mejora enormemente la protección contra ataques de escalación de privilegios. Si un atacante puede comprometer un proceso, el atacante tendrá acceso limitado a archivos y funciones a los que sólo puede acceder el proceso.

Acción propuesta	Categorización	Flujo de trabajo
1.4.17 Implementar la gestión centralizada de identidad	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - Cuentas
Detalles de la recomendación		
<p>BanCoppel deberá considerar implementar una solución de gestión centralizada de identidad (IdM) para administrar dominios basados en Linux. IdM reduciría significativamente la sobrecarga de administrar diferentes servicios y cuentas individualmente. Esto mejorará la estandarización y facilitará la gestión del estado de TI de Linux en el entorno de BanCoppel.</p> <p>Se pueden considerar las siguientes soluciones para implementar la gestión de identidad centralizada</p> <ul style="list-style-type: none"> • Solución de gestión de identidades de Red Hat6 • Free IPA7 (Solución de gestión de identidad de código abierto) <p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		
Justificación		

⁶ <https://access.redhat.com/products/identity-management>

⁷ https://www.freeipa.org/page/Main_Page

Los sistemas Linux a menudo tienen una gestión descentralizada y, por lo tanto, son más propensos a errores de configuración. La implementación de una solución de gestión de identidad aumentará la uniformidad y permitirá el inicio de sesión único, lo que eliminará la necesidad de recordar varias contraseñas y, por lo tanto, aumentará la seguridad, la productividad y la usabilidad.

Acción propuesta	Categorización	Flujo de trabajo
1.4.18 Actualizar el sistema operativo a la última versión, instalar parches de seguridad	Fortalecimiento de Linux	Fortalecimiento del servidor RHEL - SO
Detalles de la recomendación		
<p>BanCoppel debe actualizar los servidores a la última versión compatible del sistema operativo e instalar parches de seguridad para evitar la explotación de vulnerabilidades conocidas del sistema operativo.</p> <p>Aplicabilidad: RHEL 5, 6, 7, 8</p>		
Justificación		
<p>El entorno de BanCoppel tiene servidores que ejecutan sistemas operativos más antiguos con vulnerabilidades conocidas. Los atacantes frecuentemente explotan software antiguo con herramientas públicas conocidas que no requieren el uso de vulnerabilidades de día cero o métodos elaborados, ya que a menudo están bien documentados y armados de manera eficiente.</p>		

Contención: Erradicación

Acción propuesta	Categorización	Flujo de trabajo
2.1.1 Bloquear las direcciones IP, los puertos y los sinkholes de nombres de dominio maliciosos de los atacantes	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Los administradores deben bloquear el tráfico a las direcciones IP, los puertos y los sinkholes de nombres de dominio que hayan sido identificados como aprovechados por un atacante. El monitoreo se puede configurar para alertar inmediatamente al equipo de investigación cuando cualquier host intenta comunicarse con uno de los recursos de red identificados.</p> <p>Se puede desarrollar un proceso para permitir a la organización bloquear o hundir rápidamente los recursos adicionales según lo solicite el equipo de investigación. Se recomienda que este proceso permanezca después de la remediación, para que lo utilice el equipo de seguridad de la información para cualquier evento de seguridad futuro.</p> <p>Al bloquear direcciones IP, considerar bloquear el tráfico hacia y desde los bloques de red que rodean estas direcciones IP; una organización deberá evaluar primero cada bloque de red/organización para asegurarse de que las operaciones no se vean interrumpidas por el bloqueo de la comunicación con un sitio remoto legítimo dentro de esos rangos de IP.</p> <p>Para implementar el sinkhole de DNS en servidores DNS de Windows, considerar utilizar la herramienta Sinkhole-DNS disponible en el siguiente enlace: http://cyber-defense.sans.org/blog/2010/08/31/windows-dns-server-blackhole-blacklist</p>		
Justificación		
<p>Imponer esta recomendación bloqueará el tráfico entre la red de una organización y los recursos de los atacantes conocidos. El bloqueo de esta comunicación inhibirá la capacidad del atacante para conectarse directamente a su infraestructura de comando y control desde el entorno, además de alertar al equipo de investigación sobre cualquier host comprometido que no haya sido identificado previamente.</p>		

Acción propuesta	Categorización	Flujo de trabajo
2.1.2 Habilitar "Password is Required" en cuentas identificadas	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Los administradores deben habilitar "Password is Required" en las cuentas identificadas. Las cuentas de usuario con el atributo "PasswordNotRequired" establecido como "True" se pueden utilizar para acceder a los recursos del dominio sin la necesidad de proporcionar una contraseña, independientemente de las políticas de todo el dominio que se apliquen. Para que esto suceda, la cuenta deberá configurarse con una contraseña en blanco.</p>		

Revisar la lista de cuentas en el archivo adjunto vinculado a esta recomendación para asegurarse de que las cuentas de usuario estén configuradas para requerir una contraseña configurando el atributo "PasswordNotRequired" en una configuración "False".

Esto se puede configurar ejecutando el comando de PowerShell (Figura 91) desde un controlador de dominio, utilizando una cuenta que tenga acceso privilegiado basado en el dominio.

```
set-ADAccountControl -Identity <accountname> -
PasswordNotRequired $False
```

Figura 91: Comando de PowerShell para deshabilitar la función "PasswordNotRequired" para cuentas de usuario

Nota: Si una cuenta tiene una contraseña en blanco, cuando el atributo "Password Not Required", se establece como "False"; se producirá el error que se muestra en la Figura 92. Se deberá establecer una contraseña para la cuenta antes de continuar.

The password does not meet the length, complexity, or history requirement of the domain

Figura 92: Error al intentar eliminar la configuración del atributo "PasswordNotRequired" en una cuenta con una contraseña en blanco

Adjuntos:



Justificación

Se deben solicitar contraseñas para todas las cuentas; los atacantes a menudo aprovechan estas cuentas vulnerables para realizar un mayor reconocimiento y mantener el acceso.

Acción propuesta	Categorización	Flujo de trabajo
2.1.3 Habilitar "Sensitive account and cannot be delegated" para todas las cuentas privilegiadas identificadas	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Los administradores deben habilitar "Sensitive account and cannot be delegated" para todas las cuentas privilegiadas identificadas.</p> <p>Las cuentas confidenciales que están protegidas por "AdminSDHolder" y que no tienen seleccionada la opción "Account is sensitive and cannot be delegated" podrán ser aprovechadas por un atacante para propósitos de delegación si las cuentas están expuestas en un sistema donde la delegación Kerberos está configurada.</p> <p>Si las cuentas identificadas no requieren explícitamente que se configure una opción para la delegación, la delegación debe deshabilitarse para las cuentas que utilizan Usuarios y equipos del directorio activo marcando la casilla "Account is sensitive and cannot be delegated" dentro de la pestaña "Account" (Figura 93).</p>		

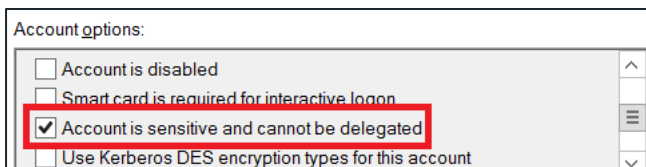


Figura 93: Opción de cuenta para deshabilitar la delegación para una cuenta privilegiada

Justificación

Las cuentas privilegiadas deben tener sus delegaciones restringidas tanto como sea posible. La delegación permite a un atacante aprovechar los derechos y permisos de una cuenta administrativa para sus propias necesidades.

Acción propuesta	Categorización	Flujo de trabajo
2.1.4 Eliminar el atributo "Admin SDHolder" de todas las cuentas que no están en grupos privilegiados	Fortalecimiento	Punto final - Fortalecimiento

Detalles de la recomendación

BanCoppel deberá revisar la lista de las cuentas identificadas para tener establecido el atributo "AdminSDHolder" y determinar si ya no se considera que las cuentas tienen una asociación privilegiada dentro del dominio. Una vez que se ha identificado el alcance preciso de las cuentas en las que se puede eliminar el atributo, el proceso se puede programar con un guion de PowerShell.

Revisar las cuentas identificadas y, para las cuentas sin privilegios, borrar el valor del atributo "AdminSDHolder" de las cuentas. Si una cuenta era anteriormente una cuenta privilegiada y se le asignó el atributo "AdminSDHolder", la cuenta aún retendrá este atributo, incluso si se elimina de una asociación del grupo privilegiado.

Para mitigar las cuentas que ya no deberían tener establecido el atributo "AdminSDHolder":

- Por medio de Usuarios y equipos del directorio activo, eliminar la cuenta de cualquier grupo privilegiado integrado y, mediante la pestaña "Attribute Editor" de la cuenta, establecer el valor del atributo "adminCount".

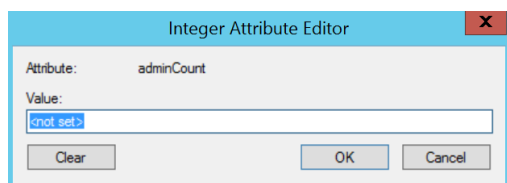


Figura 94: Campo de atributo adminCount

- De manera alternativa, para eliminar el valor del atributo "adminCount" e imponer explícitamente la herencia para cualquier cuenta sin privilegios que todavía estuviera protegida por "AdminSDHolder", se puede aprovechar el siguiente guion de PowerShell (Figura 95):

```
set-aduser <username> -remove @{adminCount=1}
$user = get-aduser <username> -properties ntsecuritydescriptor
$user.ntsecuritydescriptor.SetAccessRuleProtection($false,$true)
set-aduser <username> -replace
@{ntsecuritydescriptor=$user.ntsecuritydescriptor}
```

Figura 95: Comandos de PowerShell para imponer la herencia para los permisos de ACL en cuentas con privilegios heredados protegidas por AdminSDHolder

- Después de que se haya eliminado el valor del atributo "adminCount", utilizando Usuarios y computadora del directorio activo (ADUC), se puede habilitar la herencia de seguridad para la cuenta (Figura 96).
 - ADUC > Account > Security Tab > Advanced > Enable Inheritance

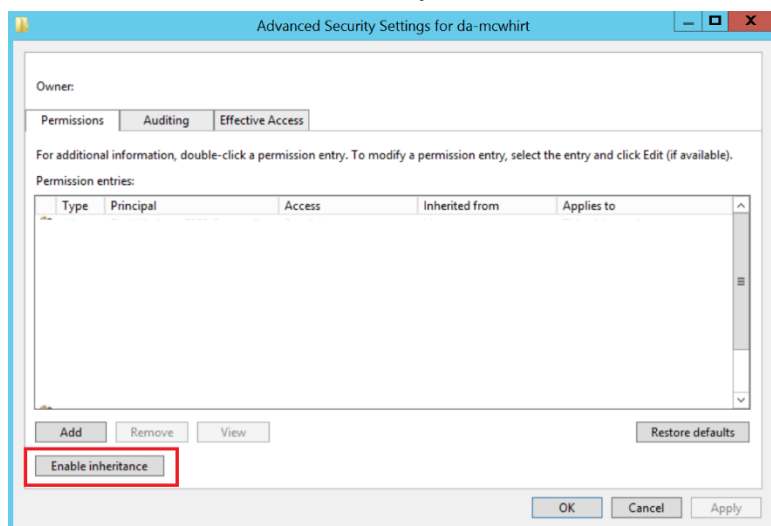


Figura 96: Opción para "Enable Inheritance" para una cuenta en ADUC

Adjuntos:



Justificación

El atributo Admin SDHolder permite derechos administrativos cuando se aplica a una cuenta. Las cuentas no administrativas deben tener este permiso eliminado para garantizar que no se aproveche en caso de que la cuenta se vea comprometida.

Acción propuesta	Categorización	Flujo de trabajo
2.1.5 Restablecer las contraseñas e imponer la caducidad de la contraseña en cuentas privilegiadas	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Los administradores deben restablecer las contraseñas e imponer la caducidad de las contraseñas en las cuentas privilegiadas. Esto se puede realizar mediante un restablecimiento de contraseña empresarial.</p> <p>Para realizar un restablecimiento de contraseña empresarial:</p> <ol style="list-style-type: none"> 1. Cambiar la contraseña de todas las cuentas que pertenecen a usuarios las cuales tenían una cuenta comprometida (identificadas como utilizadas activamente por un atacante). <ul style="list-style-type: none"> ○ Por ejemplo, si la cuenta del directorio activo de un usuario se vio comprometida y un atacante la utilizó, se deben cambiar las contraseñas del directorio activo, LDAP y RADIUS del usuario. 		

2. Configurar nuevas cuentas para usuarios privilegiados. Si esto no es posible, cambiar como mínimo la contraseña de todas las cuentas privilegiadas del directorio activo.
 - Esto incluye administradores de empresas, administradores de dominio, administradores de Exchange, cuentas de servicio con privilegios y cualquier cuenta que sea miembro del grupo de “local administrators” en una cantidad significativa de sistemas.
3. Cambiar la contraseña de todas las cuentas en los sistemas Linux donde se identificó evidencia de compromiso. Además, determinar si otros sistemas tienen las mismas contraseñas (ej. administradores que utilizan la misma contraseña en varios sistemas).
4. Cambiar la contraseña de todas las cuentas que tengan acceso shell a la infraestructura de los sistemas Linux. Asegurarse de que la contraseña de root sea única en cada sistema.
5. Configurar las cuentas del directorio activo y LDAP de los usuarios para que requieran que el usuario elija una nueva contraseña en el siguiente inicio de sesión.
 - Después de una semana, los usuarios que no han establecido nuevas contraseñas deben tener sus cuentas deshabilitadas hasta que se comuniquen con el help desk para reactivarlas.
6. 8Cambiar la contraseña de la cuenta Kerberos “KRBtgt” dos veces. Consultar la guía de Microsoft para obtener instrucciones y guiones:
 - <https://blogs.microsoft.com/cybertrust/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/>
 - *Nota: Para los controladores de dominio de sólo lectura (RODC), las cuentas "krbtgt" para estos sistemas deberán cambiarse manualmente por medio de Usuarios y equipos del directorio activo.*
7. Deshabilitar y volver a activar la opción "Smart Card is required" para todas las cuentas de tarjetas inteligentes. Si una cuenta está configurada para requerir una tarjeta inteligente para el inicio de sesión interactivo, el hash NT para esa cuenta se deriva de un valor generado aleatoriamente. Este hash no cambiará cuando se restablezca la contraseña y, si un atacante lo roba, se puede utilizar para ataques de pass-the-hash como cualquier otro conjunto de credenciales NTLM.
 - o Para forzar la creación de un nuevo hash NT, Simpson Strong-Tie debe alternar (deshabilitar y, posteriormente, volver a habilitar) el atributo “Smart Card is required for interactive logon” para cada cuenta de tarjeta inteligente.
8. Restablecer la contraseña de confianza para cada dominio de confianza.
 - <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-reset-trust>

Si no se puede imponer un restablecimiento de contraseña empresarial totalmente coordinado en un breve período de tiempo, una organización puede imponer el restablecimiento de contraseña para las cuentas que cumplan las siguientes condiciones, en el orden específico que se describe a continuación:

1. Cuentas privilegiadas - Incluidas las cuentas basadas en dominios a las que se les asignan los siguientes permisos:
 - Administradores de dominio
 - Administradores de empresas
 - Administradores de esquemas
 - Administradores
 - Operadores de cuentas
 - Operadores de respaldo
 - Editores de certificados
 - Operadores de impresión
2. Cuentas de servicio: comenzando específicamente con aquellas con contraseñas estáticas que no cambian de forma predefinida.

3. Cuentas locales, cuentas de servicio y cualquier cuenta de dominio identificable que comúnmente interactúe con sistemas etiquetados como comprometidos y accedidos (referencia 2.3 y 2.4 arriba)
4. Cuentas de dominio que pueden no formar parte del grupo de administradores de dominio, administradores de empresa o administradores de esquema, pero que tienen permisos administrativos en una gran variedad de puntos finales (ej. Administradores de servidor, cuentas de soporte de escritorio/asistencia técnica, cuentas de SCCM, cuentas de dominio utilizadas para administrar y ejecutar herramientas específicas [AV] en puntos finales)

Después de iniciar restablecimientos para el alcance de las cuentas identificadas anteriormente, una organización puede coordinar un proceso para forzar un cambio de contraseña para las cuentas de dominio (usuario) restantes. Para limitar y controlar el impacto potencial en las operaciones, esto se puede lograr pronosticando y ejecutando un restablecimiento para las cuentas que residen en una OU/sitio específico, único para cada día hasta que el proceso se haya completado en su totalidad.

- Día 1 – Todas las cuentas en OU / Sitio A
- Día 2 – Todas las cuentas en OU / Sitio B
- Día 3 – Todas las cuentas en OU / Sitio C



Enterprise Password
Reset Preparation Gui

Adjuntos:



Justificación

Restablecer todas las contraseñas en un corto período de tiempo garantizará que el acceso de un atacante sea limitado.

Acción propuesta	Categorización	Flujo de trabajo
2.1.6 Fortalecer los permisos para la persistencia de los puntos finales	Fortalecimiento	Punto final - Fortalecimiento
<p>Detalles de la recomendación</p> <p>Los atacantes aprovecharán la persistencia en un punto final para garantizar que el malware aún esté presente y pueda ejecutarse incluso si se reinicia el punto final. Una investigación exhaustiva arrojará evidencia de los diversos mecanismos de persistencia que puede utilizar una variante, aunque puede ser necesario imponer temporalmente permisos fortalecidos los cuales reducen los riesgos relacionados con la configuración de sistemas adicionales con un mecanismo persistente para la invocación de malware.</p> <p>El registro de Windows contiene varias llaves que a menudo se aprovechan para la persistencia. La Figura 97 proporciona una lista de alto nivel de llaves comunes de registro las cuales a menudo se aprovechan para la persistencia en un punto final.</p> <p>HKLM\Software\Microsoft\Windows\CurrentVersion\Run HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</p>		

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
```

Figura 97: Llaves comunes de registro utilizadas para la persistencia

Al utilizar una configuración fortalecida de política de grupo, una organización puede reducir de forma centralizada el alcance de los permisos asignados a una llave de registro específica y denegar explícitamente el acceso de escritura o modificación para cuentas privilegiadas o cuentas que se observe que son aprovechadas por una variante de malware para propagación y persistencia.

- *Computer Configuration > Políticas > Windows Settings > Security Settings > Registry*

La Figura 98 proporciona un ejemplo de una política de grupo que ha configurado permisos explícitos de denegación para el grupo de administradores de dominio para la llave de registro HKLM\Software\Microsoft\Windows\CurrentVersion\Run.

Policies				hide
Windows Settings				hide
Security Settings				hide
Registry				hide
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				hide
Configure this key then: Propagate inheritable permissions to all subkeys				
Owner				
Permissions				
Type	Name	Permission	Apply To	
Deny	MCWHIRT\Domain Admins	Full control	This key only	
Allow inheritable permissions from the parent to propagate to this object and all child objects				Disabled

Figura 98: Ejemplo de política de grupo para imponer una configuración explícita DENY para una llave de registro específica

Para configurar una política de grupo similar:

1. Navegar a *Computer Configuration > Políticas > Windows Settings > Security Settings > Registry* – y, posteriormente, hacer clic con el botón derecho y seleccionar *Add Key*
2. Navegar hasta la llave de registro que debe protegerse aún más
3. Seleccionar *Advanced* dentro de la ventana **Security Permissions**

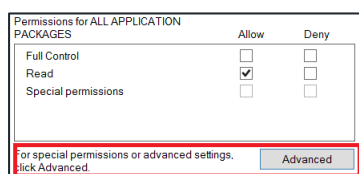


Figura 99: Permisos de seguridad avanzados para editar

4. *Add > Select a Principal* – a continuación, seleccionar la cuenta o el grupo de seguridad adecuado para los que se deben denegar los permisos y seleccionar el ámbito de los permisos adecuados. La Figura 100 proporciona el subconjunto mínimo de permisos que deben incluirse para una denegación explícita.

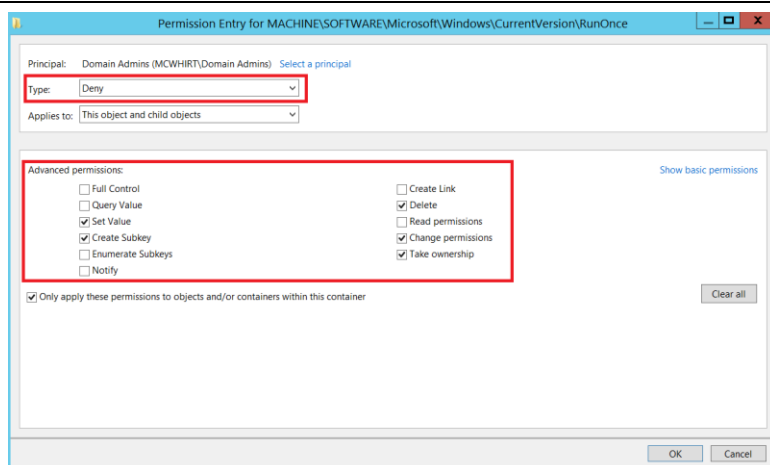


Figura 100: Ventana de entrada de permisos

5. Hacer clic en **OK** – y aparecerá el cuadro “Add Object” (Figura 101). Seleccionar la opción adecuada para la configuración deseada.

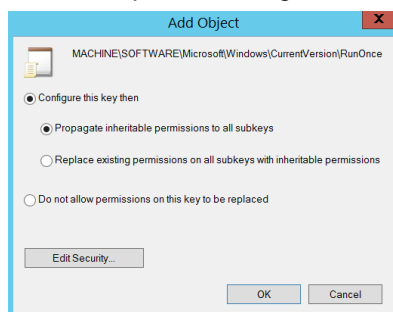


Figura 101: Agregar configuración de objeto

- “Propagate inheritable permissions to all subkeys” fuerza la ACL especificada en todas las subclaves de la llave de destino.
- “Replace existing permissions on all subkeys with inheritable permissions” fuerza sólo la nueva ACL en las subclaves que se **heredan** de la llave de destino.
- Seleccionar la opción “Do not allow permissions on this key to be replaced” indica que los permisos existentes no se pueden modificar.

Una vez que se configura y, la política de grupo está vinculada a un contenedor, cualquier intento de escribir en la llave de registro especificada en un punto final utilizando una cuenta donde se denegó explícitamente el acceso dará como resultado un error (Figura 102).

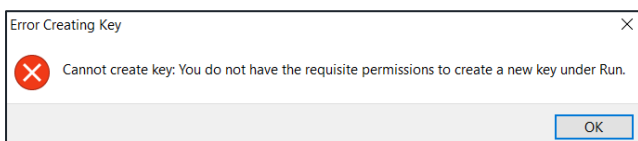


Figura 102: Error al intentar escribir en una llave de registro donde se denegó el acceso

Justificación

La revisión de los privilegios del punto final garantizará que a los usuarios sin privilegios no se les otorguen permisos detallados en los puntos finales que se puedan aprovechar para la persistencia o el movimiento lateral.

Acción propuesta	Categorización	Flujo de trabajo
2.1.7 Mejorar el nivel de autenticación del LAN Manager para putos finales	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Probar y ajustar la configuración del nivel de autenticación del LAN Manager de "Send NTLMv2 responses only" para todos los clientes que admitan NTLMv2. Esto se puede configurar mediante un ajuste de GPO.</p> <p>Para los controladores que no son de dominio, Mandiant recomienda configurar el ajuste en la que los clientes utilizan sólo la autenticación NTLMv2 y utilizar la seguridad de sesión NTLMv2 si el servidor lo admite.</p> <ul style="list-style-type: none"> • <i>Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Network security: LAN Manager authentication level</i> <ul style="list-style-type: none"> ○ "Send NTLMv2 response only. Refuse LM and NTLM." <p>Para los controladores de dominio, configurar inicialmente el ajuste en la que los controladores de dominio aceptan la autenticación LM, NTLM y NTLMv2:</p> <ul style="list-style-type: none"> • <i>Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Network security: LAN Manager authentication level</i> <ul style="list-style-type: none"> ○ "Send NTLMv2 response only" <p>Idealmente, con el tiempo, esta configuración debería fortalecerse para reflejar el mensaje "Send NTLMv2 response only. Refuse LM and NTLM".</p> <p>Además, como mínimo, se debe configurar e imponer el cifrado de 128 bits para la seguridad de NTLM SSP.</p> <ul style="list-style-type: none"> • <i>Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Network security: Minimum session security for NTLM SSP based (including secure RPC) clients</i> <ul style="list-style-type: none"> ○ "Require 128-bit encryption" • <i>Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Network security: Minimum session security for NTLM SSP based (including secure RPC) servers</i> <ul style="list-style-type: none"> ○ "Require 128-bit encryption" 		
Justificación		
<p>Validar que todos los puntos finales estén utilizando cifrados NTLM actualizados garantizará que las contraseñas almacenadas con un cifrado heredado no sean aprovechadas por un atacante para descifrar contraseñas y mantener la persistencia.</p>		

Acción propuesta	Categorización	Flujo de trabajo
2.1.8 Limpiar y verificar los sistemas "accedidos"	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Considerar la posibilidad de limpiar y escanear los sistemas que se han identificado como "accedidos" para asegurarse de que se elimine todo el malware.</p>		

Las recomendaciones específicas de Mandiant para limpiar y verificar los sistemas a los que se accede incluyen:

- Asegurarse de que el sistema esté completamente parcheado
- Asegurarse de que el sistema haya actualizado el antivirus (firmas) y se haya completado un análisis total del disco.
- Asegurarse de que se hayan restablecido todas las contraseñas de las cuentas locales del sistema
 - Esto incluiría no sólo las cuentas de nivel de sistema operativo (SO), sino también las cuentas específicas de la aplicación (ej. SQL, Oracle, aplicación web) que están presentes en cualquier sistema al que se accede
- Verificar si los usuarios se ejecutan dentro de un contexto administrativo en el sistema y si se puede reducir el alcance de los permisos asignados a los usuarios finales en el sistema
- Asegurar que las contraseñas de todos los usuarios del dominio las cuales interactúan con el sistema hayan sido (o serán) cambiadas
- Asegurarse de que se hayan aplicado todas las recomendaciones de fortalecimiento del GPO (para estaciones de trabajo/servidores)

Justificación

Validar que todos los puntos finales estén utilizando cifrados NTLM actualizados garantizará que las contraseñas almacenadas con un cifrado heredado no sean aprovechadas por un atacante para descifrar contraseñas y mantener la persistencia.

Acción propuesta	Categorización	Flujo de trabajo
2.1.9 Asegurarse de que el programa de administración de vulnerabilidades se aplique a todos los hosts	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>BanCoppel debe garantizar que exista un programa integral de gestión de vulnerabilidades en el que se utilicen herramientas de gestión de vulnerabilidades para identificar aplicaciones, sistemas y servicios que supongan un riesgo para el entorno operativo de la organización. Además, se puede aprovechar para identificar activos perdidos o no autorizados.</p> <p>Tener la capacidad de identificar vulnerabilidades antes de que un actor de amenazas pueda explotarlas es sólo el primer paso para prevenir un incidente crítico. Las vulnerabilidades descubiertas deben remediarse de manera oportuna. Un programa de gestión de vulnerabilidades debe estar respaldado por el líder y los recursos para lograr el programa deben estar fácilmente disponibles. Por último, es fundamental para el éxito del programa establecer la responsabilidad de quién está mitigando o remediando cada vulnerabilidad y un cronograma para lograr el cumplimiento total.</p> <p>BanCoppel debe considerar las siguientes guías y pasos para establecer un programa de gestión de vulnerabilidades y los procesos asociados:</p> <p>Personas:</p> <ul style="list-style-type: none"> • Dedicar o asignar una o más personas al programa de gestión de vulnerabilidades para garantizar que los procesos se sigan continuamente. • Asegurar que los recursos de personal dedicados / asignados estén capacitados de acuerdo con los estándares de la industria para la gestión de vulnerabilidades y amenazas. <p>Proceso:</p>		

- BanCoppel debe desarrollar un estándar formal de gestión de vulnerabilidades que incluya lo siguiente:
 - Un conjunto de acuerdos de nivel de servicio (SLA), con el apoyo de TI, los cuales definen los plazos acordados en los que se mitigará o remediará una vulnerabilidad.
 - Un modelo de puntuación de riesgo ya sea integrado en la tecnología de escaneo de vulnerabilidades o desarrollado internamente dentro de BanCoppel, el cual esté alineado con un conjunto definido de SLO para las diversas definiciones de criticidad de la vulnerabilidad (ej. Baja, Media, Alta, Crítica)
 - Un proceso de excepción para las excepciones y todas las demás vulnerabilidades que no se pueden mitigar o remediar. Debe incluir un proceso de aprobación que involucre a las personas y propietarios que son responsables de los activos en particular.
- El equipo de seguridad de la información de BanCoppel debe desarrollar reportes y métricas sobre la gestión de vulnerabilidades las cuales se informen a los equipos de gestión pertinentes en una cadencia predeterminada.

Tecnología:

- BanCoppel deberá utilizar una tecnología de escaneo de vulnerabilidades para realizar escaneos semanales de descubrimiento en todos los rangos de IP y segmentos de red de BanCoppel. Los análisis de descubrimiento ayudan con la identificación de puntos finales no autorizados y faltantes en toda la organización.
- BanCoppel debe tomar los resultados del descubrimiento de activos y priorizar cada activo descubierto en agrupaciones lógicas las cuales sean relevantes para las operaciones comerciales y/o los requisitos de cumplimiento. Una vez que se completan las agrupaciones, BanCoppel también debe determinar el riesgo de cada agrupación de activos para operaciones comerciales únicas. Se debe crear una base inicial para cada agrupación lógica con el fin de identificar fácilmente cuando una vulnerabilidad recientemente identificada desvía el nivel de riesgo aceptable de la base inicial actual.
- BanCoppel deberá crear un cronograma de análisis regular utilizando los datos de la fase de descubrimiento. Tanto los análisis autenticados como los no autenticados deben ejecutarse en toda la organización y en fases escalonadas. El programa de evaluación debe incluir exploraciones periódicas del entorno completo. Un objetivo razonable sería escanear cada activo en busca de vulnerabilidades dos veces al mes.
- Los resultados de las exploraciones deben utilizarse para priorizar los esfuerzos de remediación y proporcionar una comprensión más detallada de la postura de seguridad de BanCoppel. No todos los activos tienen el mismo valor y la gestión de vulnerabilidades debe tener en cuenta las prioridades operativas del negocio.

Relevante para todas las plataformas de los puntos finales y servidores, la aplicación de parches para explotaciones conocidas es una recomendación clave para la contención y la posible remediación de una infección de malware. Muchas variantes utilizan explotaciones conocidas para comprometer sistemas e invocar movimientos laterales dentro de un entorno. Un ejemplo común de esto es la variante de ransomware WannaCrypt, la cual explotó una de las vulnerabilidades que se aborda como parte de la actualización de seguridad de Microsoft MS17-010.

Las organizaciones deben asegurarse de que los parches se prueben y verifiquen antes de imponerlos en los sistemas de producción dentro de un entorno. Además, aprovechar los procesos probados, además de una plataforma centralizada para acelerar la implementación de parches críticos, es vital para garantizar que se puedan invocar las medidas adecuadas de contención y remediación en caso de un brote, a gran escala, dentro de un entorno.

Justificación

Un programa de gestión de vulnerabilidades establecido y maduro proporciona una defensa proactiva contra varios actores de amenazas y brinda a la organización la oportunidad de remediar o mitigar las

vulnerabilidades descubiertas antes de que puedan ser aprovechadas por un actor de amenazas. Si bien sigue siendo susceptible a ataques de día cero, el descubrimiento y la remediación oportuna de vulnerabilidades pueden, como mínimo, proteger contra más ataques comunes y permitir que el equipo de seguridad de la información se concentre en otras medidas proactivas, como la caza de amenazas y los equipos rojo/púrpura.

Acción propuesta	Categorización	Flujo de trabajo
2.1.10 Asegurarse de que los servidores a los que se puede acceder desde el exterior estén fortalecidos	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Validar que todos los servidores a los que se puede acceder desde Internet y las redes externas estén fortalecidos y monitoreados con una solución EDR y que las bitácoras de acceso se reenvíen a un servidor Syslog o SIEM.</p> <p>La autenticación multi factor debe aprovecharse tanto como sea posible para garantizar que sólo los usuarios autorizados puedan acceder a estos recursos y aumentar la postura defensiva de estos servidores externos.</p> <p>Las redes que contienen estos servidores críticos deben segmentarse y tener reglas granulares del cortafuegos las cuales restrinjan el acceso desde la DMZ u otras redes accesibles desde la web con cortafuegos robustos que permitan el registro detallado y la inspección del tráfico. Cualquier servidor basado en la web (ej. una aplicación web) que se comunique con redes externas debe estar completamente fortalecida y tener el acceso registrado y reenviado al servidor Syslog y SIEM.</p> <p>Estos servidores críticos suelen ser el primer punto de infección para muchas interacciones de malware. Centrar los esfuerzos internos en fortalecer, parchear, asegurar y monitorear estos recursos comerciales críticos garantizará que los recursos de remediación se concentren donde tendrán un mayor impacto defensivo y aumentarán la postura defensiva de BanCoppel.</p> <p>Recomendaciones generales del fortalecimiento:</p> <ul style="list-style-type: none"> • Investigar e implementar una herramienta o proceso automatizado que garantice el cumplimiento de la configuración de forma regular. Idealmente, BanCoppel deberá poder escalar los cambios de administración y configuración en toda la empresa de manera más efectiva con una capacidad centralizada y automatizada. • Asegurarse de que los servidores no puedan comunicarse con Internet o redes externas tanto como sea posible. Validar que el tráfico de entrada y salida a estos hosts esté explícitamente definido y limitado, asegurarse de que el tráfico que sale de la red del servidor sea limitado y supervisado. • Asegurarse de que las firmas AV estén actualizadas, AV esté instalado y una solución EDR supervise el acceso y la creación de procesos. Asegurarse también de que los permisos estén limitados en los servidores, sólo se debe permitir la instalación de programas autorizados y se deben restringir los permisos de instalación local. • Deshabilitar explícitamente el uso de protocolos heredados como FTP, Telnet y herramientas de administración remota como PSEXEC. 		

- Actualizar PowerShell a la versión 6 para aumentar las capacidades de registro. Si se utiliza SCCM en BanCoppel, no se debe denegar explícitamente la versión 2 de PowerShell, ya que esto generará errores en SCCM.

Recomendaciones de fortalecimiento de Windows:

- Los controladores de dominio y otros servidores sensibles no deben tener acceso a Internet.
- Los administradores deben tener cuentas dedicadas para las actividades de administración y cuentas separadas, sin privilegios, para las actividades cotidianas. Las cuentas de administrador de dominio sólo deben utilizarse para autenticarse en los controladores de dominio.
- Los administradores deben utilizar plataformas de administración dedicadas o estaciones de trabajo de administración de privilegios (PAWS) para administrar el directorio activo. Estas credenciales administrativas no deben utilizarse en ningún otro sistema.
- Se debe evitar que los sistemas de plataforma de administración utilizados para administrar el directorio activo accedan a Internet y se deben aislar de las comunicaciones entrantes/salientes con otros sistemas dentro de la red.
- Todas las cuentas de administrador local deben tener contraseñas únicas, idealmente administradas por LAPS.
- Deben utilizarse cuentas de dominio separadas para administrar servidores públicos desde cualquier cuenta utilizada para administrar servidores internos.
- Se debe monitorear la siguiente actividad de autenticación:
 - Uso de cuentas privilegiadas
 - Intentos para utilizar cuentas locales con el fin de iniciar sesión de forma remota desde otros sistemas
 - Inicios de sesión del Protocolo de escritorio remoto (RDP)
- Evitar el almacenamiento del hash del LAN Manager para contraseñas.

Recomendaciones de fortalecimiento de Linux:

- Asegurarse de que Linux y los servidores web estén parcheados; los atacantes también se enfocarán en estos hosts.
 - Spacewalk es una aplicación de parcheo gratuita para Linux; la dificultad con muchas herramientas de código abierto es asegurarse de que estén configuradas correctamente.
- Poner en funcionamiento los estándares de configuración de Linux:
 - Imponer y administrar el cifrado de disco
 - Imponer los ajustes de configuración del sistema operativo, los cuales incluyen:
 - Requisitos de firma de la aplicación
 - Privilegios de sudo
 - Restricciones de uso de la cuenta root
 - Acceso SSH
 - Deshabilitar servicios inseguros o innecesarios (ej. Telnet, ftp)
 - Implementar e imponer los controles de seguridad de los puntos finales, los cuales incluyen:
 - Antivirus
 - Sistemas de prevención de intrusión del host (HIPS)
 - Agentes de detección y respuesta de los puntos finales (EDR)
 - ACL del cortafuegos del host

- Agentes de prevención de pérdida de datos (DLP)
 - Implementación de parches
 - Centralizar la gestión de identidades y accesos, especialmente para cuentas privilegiadas

Justificación

Fortalecer adecuadamente los servidores Windows y Linux, dirigidos a redes externas, es un elemento crítico para limitar las capacidades de los atacantes y proteger el perímetro de la red. Los servidores web, los servidores de aplicaciones y otros servidores alojados en DMZ suelen ser los primeros objetivos de los atacantes los cuales buscan obtener acceso no autorizado y requieren un fortalecimiento adicional para evitar que se vean comprometidos y se utilicen como un punto de pivote para obtener acceso a las redes internas.

Mejoras estratégicas

Acción propuesta	Categorización	Flujo de trabajo
3.1.1 Verificar si se pueden aprovechar las reglas de reducción de la superficie del ataque (ASR)	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Las reglas de Reducción de la superficie del ataque (ASR) de Microsoft pueden proporcionar una capa adicional de protección contra ataques comunes a los sistemas de punto final.</p> <p>Para aprovechar ASR, los siguientes requisitos son necesarios:</p> <ul style="list-style-type: none"> El punto final debe estar ejecutado: <ul style="list-style-type: none"> Windows 10 (v1709+) Windows Server 2016 (v1803+) Windows Server 2019 Se requiere una licencia de Windows 10 Enterprise E3 (o superior). ASR depende de que el antivirus de Windows Defender esté habilitado en el punto final. Además, la función de protección, en tiempo real de Microsoft Defender, debe estar habilitada. <p>Las siguientes reglas de ASR están disponibles y podrían ayudar a fortalecer los terminales dentro del entorno empresarial de BanCoppel.</p> <ul style="list-style-type: none"> Bloquear el contenido ejecutable del cliente de correo electrónico y el correo web. Bloquear todas las aplicaciones de Office para que no creen procesos secundarios Impedir que la aplicación de comunicación de Office cree procesos secundarios Impedir que las aplicaciones de Office creen contenido ejecutable Impedir que las aplicaciones de Office inyecten código en otros procesos Bloquear JavaScript o VBScript para que no inicien contenido ejecutable descargado Bloquear la ejecución de guiones potencialmente ofuscados Bloquear las llamadas a la API de Win32 desde la macro de Office Bloquear la ejecución de archivos ejecutables a menos que cumplan con un criterio de prevalencia, edad o lista de confianza Utilizar protección avanzada contra ransomware Bloquear el robo de credenciales del subsistema de autoridad de seguridad local de Windows (lsass.exe) Bloquear las creaciones de procesos que se originan a partir de comandos PSEXEC y WMI Bloquear procesos no confiables y sin firmar que se ejecutan desde USB Impedir que Adobe Reader cree procesos secundarios Bloquear la persistencia por medio de la suscripción a eventos de WMI 		
Justificación		
<p>Si BanCoppel puede aprovechar las reglas de ASR, esto puede proporcionar un medio práctico y escalable para proteger los puntos finales de los métodos de explotación comunes, además de proteger contra las técnicas comunes de movimiento lateral.</p>		

Acción propuesta	Categorización	Flujo de trabajo
3.1.2 Revisar los objetos de la política de grupo	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>Los agentes que aprovechan la persistencia del malware pueden modificar o crear objetos de política de grupo (GPO) para la implementación continua masiva de malware dentro de un entorno. BanCoppel debe revisar y verificar que los GPO recientemente modificados o creados son esperados, además de revisar su entorno en busca de un GPO que contenga configuraciones específicas relevantes para guiones de inicio de sesión o tareas programadas (las cuales a menudo son aprovechadas por los actores de amenazas para la implementación masiva de malware).</p> <p>Para revisar todos los GPO configurados, incluidos los registros de fechas para la creación de un GPO y los últimos atributos modificados, utilizar el siguiente cmdlet de PowerShell:</p>		
get-gpo -all		
<p><i>Figura 103: Cmdlet de PowerShell para revisar una lista de GPO y atributos específicos</i></p> <p>Para revisar todos los GPO configurados con una referencia de guion de inicio de sesión de usuario o computadora, utilizar el siguiente guion de PowerShell:</p>		
<pre>import-module grouppolicy function LogonScript(\$xmldata){ If ((\$xmldata.GPO.Computer.ExtensionData.Name -contains "Scripts") -or (\$xmldata.GPO.User.ExtensionData.Name -contains "Scripts")){ Return \$true } Return \$false } \$LogonScriptGPOs = @() Get-GPO -All ForEach { \$gpo = \$_ ; \$_ Get-GPOReport -ReportType xml ForEach { If(LogonScript([xml]\$_)){ \$LogonScriptGPOs += \$gpo } }} If (\$LogonScriptGPOs.Count -eq 0) { "No GPO's Configured with a Logon Script Found" } Else{ \$LogonScriptGPOs Select-object DisplayName,ID,Owner,CreationTime,ModificationTime</pre>		
<p><i>Figura 104: Guion de PowerShell para enlistar todos los GPO configurados con una referencia de guion de inicio de sesión</i></p> <p>Para revisar todos los GPO configurados con una referencia de tarea programada, utilizar el siguiente guion de PowerShell:</p>		
<pre>import-module grouppolicy function SchedTask(\$xmldata){</pre>		


```

    If (($xmldata.GPO.Computer.ExtensionData.Name -contains "Scheduled Tasks") -or
($xmldata.GPO.User.ExtensionData.Name -contains "Scheduled Tasks")){
        Return $true
    }

    Return $false
}

$SchedTaskGPOs = @()

Get-GPO -All | ForEach { $gpo = $_ ; $_ | Get-GPOReport -ReportType xml | ForEach {
If(SchedTask([xml]$_)){ $SchedTaskGPOs += $gpo } }}

If ($SchedTaskGPOs.Count -eq 0) {
    "No GPO's Configured with a Scheduled Task Found"
}
Else{
    $SchedTaskGPOs | Select-object DisplayName,ID,Owner,CreationTime,ModificationTime
| Export-CSV -path $outputdir\GPOs-SchedTask.csv -NoTypeInfoation
}

```

Figura 105: Guion de PowerShell para enlistar todos los GPO configurados con una referencia de tarea programada

Justificación

BanCoppel debe validar que los GPO están libres de mecanismos de persistencia para garantizar un evento de remediación exitoso.

Acción propuesta	Categorización	Flujo de trabajo
3.1.3 Implementar estaciones de trabajo de acceso privilegiado para administradores	Fortalecimiento	Punto final - Fortalecimiento
Detalles de la recomendación		
<p>BanCoppel deberá considerar que el personal administrativo aproveche las estaciones de trabajo de acceso privilegiado (PAW) dedicadas para que los administradores gestionen los servidores críticos, como controladores de dominio. Los PAW son estaciones de trabajo fortalecidas que prohíben el acceso a Internet y otras actividades generales del usuario, como ver el correo electrónico. Los PAW sólo deben tener acceso a los recursos que deben administrar de forma remota. Las listas de control de acceso (ACL) deben configurarse para servidores críticos, de modo que el acceso remoto a estos servidores sólo esté disponible desde el respectivo PAW de administrador y/o el host de salto al que sólo se puede acceder desde el PAW.</p> <p>Existen varios métodos que BanCoppel puede considerar para implementar un PAW, los cuales incluyen:</p> <ul style="list-style-type: none"> • Opción 1: Dos computadoras portátiles físicas separadas, una para usuarios generales y otra para acceso privilegiado y uso de administración remota 		

- **Opción 2:** Un solo PAW físico fortalecido con una máquina virtual bloqueada que se utilizará para las actividades generales del usuario
- **Opción 3:** Una estación de trabajo física segura que tiene acceso a un SO administrativo virtual y una máquina virtual para las actividades generales del usuario; esto se puede lograr por medio de VDI

Cada opción tiene ventajas y desventajas, tal y como describe Microsoft en el siguiente enlace:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts>

Como mínimo, asegurarse de que un PAW cumpla con los siguientes requisitos:

- Ejecutar Windows 10 o Server 2016
- Implementar Credential Guard, Device Guard y Windows Defender Remote Credential Guard
- Si se prefiere el uso de máquinas virtuales, considerar implementar máquinas virtuales blindadas como se describe en el siguiente enlace:
<https://blogs.technet.microsoft.com/datacentersecurity/2017/11/29/why-use-shielded-vms-for-your-privileged-access-workstation-paw-solution/>
- Los PAW deben ser los únicos sistemas que tienen permisos para acceder a un host de salto (bloqueados mediante ACL en la red o en la capa de punto final o mediante tunelización IPSEC entre puntos finales).
- Aprovechar el cifrado total del disco
- Los usuarios que acceden a los PAW deben formar parte del grupo del directorio activo "Protected Users".
- Se tiene un paquete de seguridad, como un antivirus, instalado
Tener en cuenta que todas las herramientas o aplicaciones instaladas en un PAW pueden suponer un riesgo adicional para el PAW. Las herramientas de administración las cuales están instaladas en los PAW deben estar en el mismo nivel o en un nivel superior. Las herramientas de seguridad (ej. plataformas EDR, protección de punto final de Symantec, Nessus) deben administrarse desde un PAW, siempre que sea posible.
- Se actualiza de forma periódica y automática.
- No puede acceder a los sitios de Internet o intranet que no están relacionados con el trabajo del Administrador asignado.
- Se deben imponer un GPO el cual restrinjan la configuración de "User Rights Assignment", minimizando el alcance de las cuentas que tienen acceso explícito para autenticarse en un PAW.

Al implementar un PAW, considerar aprovechar un enfoque de múltiples fases. Los administradores de dominio deben tener prioridad para aprovechar un PAW, seguidos de otros administradores que administran servicios críticos como vCenter, Hyper-V y otros servicios básicos que admiten el dominio.

Para que la infraestructura del directorio activo admita un PAW, se deben considerar los siguientes parámetros:

- Se deben configurar nuevos grupos globales con seguridad habilitada para albergar las cuentas de usuario que se aprovecharán para administrar y autenticarse en los PAW.
- Deben crearse unidades organizativas dedicadas (OU) para albergar los distintos alcances de los PAW, en correlación con los niveles específicos en los que se utilizarán los PAW para administrar sistemas y aplicaciones.
 - Se debe imponer la delegación para las distintas unidades organizativas para garantizar que sólo los grupos de seguridad autorizados (Figura 106) tengan acceso a las unidades organizativas donde se alojarán los PAW.
 - La herencia de GPO debe bloquearse para las unidades organizativas específicas (ej. dispositivos) donde se alojarán los objetos informáticos para cada PAW bajo niveles.

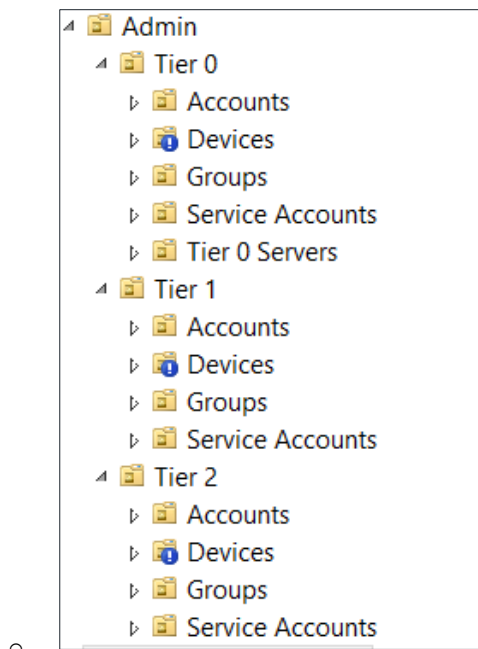


Figura 106: Estructura de OU recomendada para niveles de administración y PAW

- En el caso de las unidades organizativas en las que se alojarán los objetos de la computadora para cada PAW bajo niveles, la siguiente configuración del equipo de GPO debe imponerse y vincularse a las unidades organizativas en las que se bloqueó la herencia de GPO (ej. dispositivos):
 - Restrict and centrally manage Local Group Membership
 - i. Computer Configuration > Preferences > Control Panel Settings > Local Users and Groups
 - ii. Hacer clic derecho > All Tasks > AddAction: Update
 - Group Name: Administrators (built-in)
 - Delete All member users (Checked)
 - Delete all member groups (Checked)
 - iii. Volver a agregar la cuenta de administrador integrada y especificar un grupo de dominio (si es necesario) para que forme parte del grupo de administradores locales. Este grupo debe correlacionarse con un grupo con seguridad habilitada que sólo se aprovecha para administrar un PAW (ej. "PAW Maintenance"), y NO debe incluir las mismas cuentas de usuario que se aprovechan para autenticarse en el PAW para uso normalizado.
 - iv. Se debe aprovechar el mismo proceso (arriba) para garantizar que ninguna cuenta sea miembro de los siguientes grupos integrados en los PAW:
 - Operadores de respaldo
 - Operadores criptográficos
 - Administradores de Hyper-V
 - Operadores de configuración de red
 - Usuarios avanzados
 - Replicadores
 - Restrict and centrally manage Local Group Membership
 - i. Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment > Allow log on locally

- Grupo de seguridad que contiene cuentas de usuario de PAW
 - Grupo de seguridad que contiene cuentas de mantenimiento de PAW
- Block Inbound Network Traffic
 - i. *Computer Configuration > Políticas > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security*
 - Recomendado para importar el archivo Microsoft PAWFirewall.wfw y ajustarlo según sea necesario (<https://gallery.technet.microsoft.com/Privileged-Access-3d072563>).
- Configure WSUS for Windows Updates
 - i. *Computer Configuration > Políticas > Administrative Templates > Windows Components > Windows Updates*
 - Habilitar la política *Configure Automatic Updates*.
 - Seleccionar la opción 4 - *Auto download and schedule the install*.
 - Cambiar la opción de *Scheduled install day* a 0 - *Every Day* y la opción *Scheduled install time* según las preferencias de la organización.
 - Activar la opción *Specify Intranet Microsoft update service location policy* y especificar en ambas opciones la URL del servidor WSUS preferido.
- Para las unidades organizativas donde se alojarán los objetos de la computadora para cada PAW bajo niveles, la siguiente configuración de usuario de GPO debe imponerse y vincularse a las unidades organizativas donde se bloqueó la herencia de GPO (ej. dispositivos).
 - a. Block Internet browsing and access

La *configuración* (a continuación en la Figura 107) establecerá una dirección de proxy en una dirección de bucle invertido (127.0.0.1).

 - i. *User Configuration > Preferences > Windows Settings > Registry*
 - ii. *New > Registry Item*
 - iii. *General* tab
 - Action: Replace
 - Hive: HKCU
 - Key Path: Software\Microsoft\Windows\CurrentVersion\Internet Settings
 - Value Name: ProxyEnable
 - Value Type: REG_DWORD
 - Value Data: 1

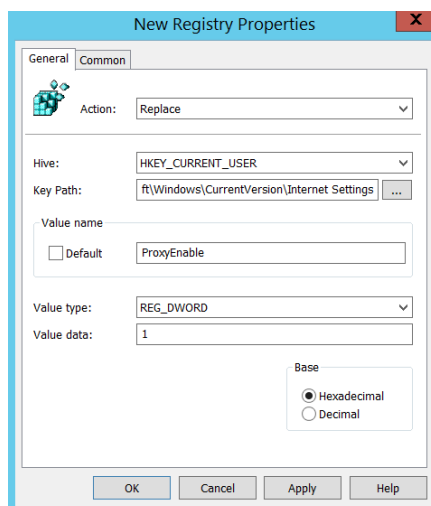


Figura 107: Configuración de registro de pestaña general

iv. Common tab

- Seleccionar *Remove this item when it is no longer applied*.
- Seleccionar *Item level targeting* y hacer clic en *Targeting*.
- Hacer clic en *New Item* y seleccionar *Security group*.
- Seleccionar el botón "..." y buscar el grupo de seguridad de usuarios del PAW apropiado.
- Hacer clic en *OK* en la ventana objetivo.
- Hacer clic en *OK* para completar la configuración de la política de grupo "ProxyServer".

v. *User Configuration > Preferences > Windows Settings > Registry*vi. *New > Registry Item*

vii. General tab

- Action: Replace (a continuación en la Figura 108)
- Hive: HKCU
- Key Path: Software\Microsoft\Windows\CurrentVersion\Internet Settings
- Value Name: ProxyServer
- Value Type: REG_SZ
- Value Data: 127.0.0.1:80

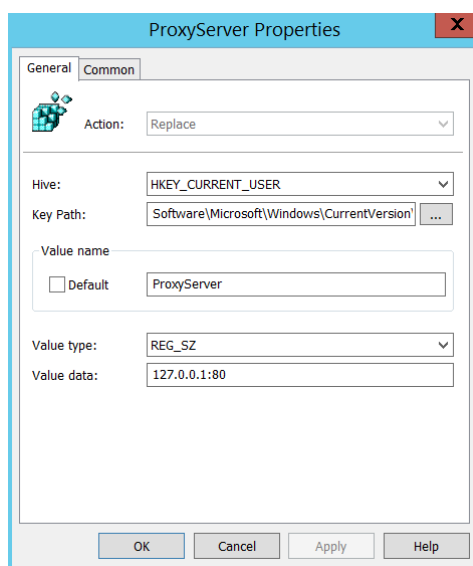


Figura 108: Configuración de registro de pestaña general

viii. Common tab

- Seleccionar *Remove this item when it is no longer applied*.
- Seleccionar *Item level targeting* y hacer clic en *Targeting*.
- Hacer clic en *New Item* y seleccionar *Security group*.
- Seleccionar el botón "..." y buscar el grupo de seguridad de usuarios del PAW apropiado.
- Hacer clic en *OK* en la ventana objetivo.
- Hacer clic en *OK* para completar la configuración de la política de grupo "ProxyServer".

ix. *User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer*

- Habilitar la opción para “*Disable changing Automatic Configuration settings*”.
- Habilitar la opción para “*Prevent changing proxy settings*”.

b. Block Internet browsing and access – except for cloud services

Si será necesario aprovechar el PAW para administrar servicios externos en la nube (ej. Azure), se puede utilizar el siguiente método para restringir la navegación en Internet sólo a los sitios específicos en un archivo proxy.pac (el archivo de muestra se puede descargar desde <https://gallery.technet.microsoft.com/Privileged-Access-3d072563>)

i. *User Configuration > Preferences > Windows Settings > Registry*

ii. *New > Registry Item*

iii. *General tab*

- Action: Replace (a continuación en la Figura 109)
- Hive: HKCU
- Key Path: Software\Microsoft\Windows\CurrentVersion\Internet Settings
- Value Name: AutoConfigUrl
- Value Type: REG_SZ
- Value Data: Ingresar la URL completa del archivo *proxy.pac*, incluido *http://* y el nombre del archivo (ej. <http://proxy.testdomain.local/proxy.pac>)

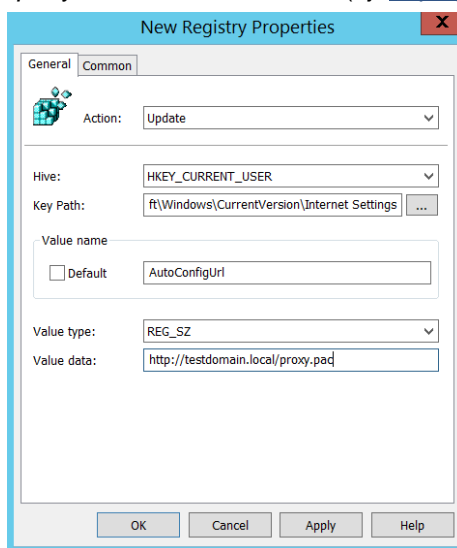


Figura 109: Configuración de registro de pestaña general

iv. *Common tab*

- Seleccionar *Remove this item when it is no longer applied*.
- Seleccionar *Item level targeting* y hacer clic en *Targeting*.
- Hacer clic en *New Item* y seleccionar *Security group*.
- Seleccionar el botón “...” y buscar el grupo de seguridad de usuarios del PAW apropiado.
- Hacer clic en *OK* en la ventana objetivo.
- Hacer clic en *OK* para completar la configuración de la política de grupo “ProxyServer”.

Para obtener información adicional sobre cómo configurar un PAW y la infraestructura de apoyo, consultar:

<https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations>

Justificación

BanCoppel deberá aprovechar un PAW para mejorar la seguridad de la gestión remota en los puntos finales y servidores.

APÉNDICE A: PLANTILLAS DE POLÍTICAS DE GRUPO - DATASTORE CENTRALIZADO

BanCoppel debe configurar y aprovechar un almacenamiento centralizado para archivos de plantilla de política de grupo. Muchas de las recomendaciones de configuración de GPO se basan en el uso de archivos ADMX y ADML los cuales están presentes en la última versión del Kit de herramientas de cumplimiento de seguridad de Microsoft (<https://www.microsoft.com/en-us/download/details.aspx?id=55319>).

Opción 1: Importación descentralizada de archivos de plantilla de GPO (No es preferible)

Si una organización necesita configurar un GPO utilizando la configuración almacenada en archivos ADMX y ADML específicos, y no se aprovechará un almacén de datos de GPO centralizado, los archivos ADMX y ADML respectivos deben copiarse en las siguientes ubicaciones en un punto final donde se configurará el GPO (Figura 110).

```
ADMX files = c:\Windows\PolicyDefinitions
ADML files = c:\Windows\PolicyDefinitions\EN-US
```

Figura 110: Ubicación para copiar archivos de políticas ADMX y ADML

Opción 2: Almacenamiento centralizado de datos (recomendado)

Un almacenamiento centralizado de datos de política de grupo es una ubicación centralizada para almacenar todos los archivos de plantilla de la política de grupo, lo que elimina la necesidad de que los administradores carguen y administren archivos de plantilla de política de grupo en varios puntos finales utilizados para administrar la política de grupo. Los beneficios de un almacenamiento centralizado de datos de política de grupo incluyen:

- Imposición sobre que todos los administradores utilizan los mismos archivos de plantilla de política de grupo.
- La capacidad de cargar los mismos archivos de plantilla desde cualquier computadora utilizada para administrar la configuración de la política de grupo.
- Facilidad de administración para gestionar y actualizar los archivos de plantilla

Para aprovechar un almacenamiento centralizado de datos de políticas de grupo, si aún no existe en un controlador de dominio, crear una carpeta titulada "PolicyDefinitions" dentro de la carpeta C:\Windows\SYSVOL\sysvol\<domain>\Policies. La carpeta "PolicyDefinitions" se utilizará para albergar archivos de plantilla ADMX y ADML.

- De manera alternativa, si la carpeta "PolicyDefinitions" ya existe, copiar los nuevos archivos ADMX y ADML en los directorios apropiados dentro de la carpeta "PolicyDefinitions".
 - Los archivos ADMX se colocarán en la raíz de la carpeta "PolicyDefinitions".
 - Los archivos ADML se colocarán dentro de la subcarpeta "EN-US" dentro de la carpeta "PolicyDefinitions".

Para verificar que el almacenamiento centralizado de datos de políticas de grupo funciona correctamente, abrir la Consola de administración de políticas de grupo (GPMC) y navegar a *Computer Configuration > Policies > Administrative Templates*, el cual deberían indicar que se hace referencia a las definiciones desde el almacenamiento centralizado (Figura 111).

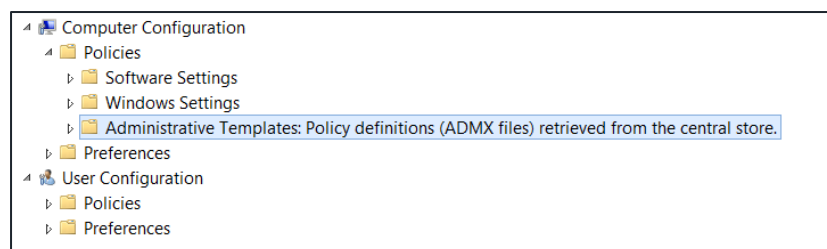


Figura 111: Archivos de plantilla de GPO - Referenciados desde el almacenamiento centralizado de datos

APÉNDICE B: ESTRATEGIA DE REMEDIACIÓN

La respuesta eficaz a incidentes requiere dos componentes críticos. La investigación busca comprender el alcance, el cronograma y el impacto de la intrusión. Los esfuerzos de remediación eliminan al atacante del entorno y posicionan a la organización para prevenir, detectar y responder a futuras amenazas de manera más efectiva.

Actividades de remediación

Cuatro grupos principales de actividades comprenden un esfuerzo de remediación efectivo: postura, contención, erradicación y estrategia. Estas actividades no deben verse como un modelo en cascada; más bien, los planes de remediación efectivos organizan las actividades de estos grupos en etapas basadas en la intrusión y las brechas de capacidad de la organización.

Postura

Estas actividades preparan a la organización para ejecutar acciones de remediación. La necesidad más urgente de adoptar una postura típicamente se relaciona con las acciones de contención y erradicación; sin embargo, también puede ser necesario adoptar una postura para actividades estratégicas como la inclusión de aplicaciones en listas blancas. Por ejemplo, una acción de contención puede ser bloquear el tráfico a los servidores de comando y control del atacante. La ejecución de esa acción requeriría que la organización comprenda dónde deben implementarse dichos bloqueos y describir instrucciones de trabajo detalladas para los equipos relevantes de TI.

Las actividades de postura más comunes incluyen:

- Prepararse para restablecer las contraseñas de una manera que minimice las interrupciones operativas.
- Determinar cómo y dónde implementar eficazmente los bloques de red.
- Construir previamente servidores para reemplazar los servidores comprometidos.
- Planificar cómo entregar nuevas PC a los usuarios con sistemas comprometidos.

Contención

Estas actividades están diseñadas para interrumpir la capacidad del atacante para ejecutar su misión dentro del entorno.

Las actividades de contención más importantes en una intrusión dirigida típica incluyen:

- Bloquear la infraestructura de comando y control del atacante.
- Deshabilitar las cuentas que el atacante esté utilizando activamente.
- Restringir el acceso a los sistemas a los que apunta el atacante.

Erradicación

Las acciones de erradicación eliminan la capacidad del atacante para acceder al entorno. Aunque la contención y la erradicación a menudo se realizan simultáneamente, Mandiant distingue entre ellas porque en algunos casos puede ser apropiado contener de inmediato un ataque en el que la erradicación inmediata no se puede implementar ya que la investigación aún está en curso.

Las actividades de erradicación más importantes incluyen:

- Reconstruir los sistemas infectados con malware.
- Restablecer las contraseñas de las cuentas comprometidas.

Estrategia

La experiencia ha demostrado que los atacantes avanzados lograrán penetrar en los entornos a los que apuntan. Los equipos de seguridad exitosos detectan y responden rápidamente a los atacantes antes de que el atacante robe datos o se incruste en el entorno. La planeación estratégica eficaz extrae las lecciones aprendidas del incidente actual, aumentadas con la experiencia de Mandiant, para mejorar las capacidades de la organización de manera integral.

La mejora de la postura de seguridad de la organización generalmente requiere cambios que afectan los procesos de TI y que pueden afectar los procesos comerciales. Los ejemplos incluyen una protección más eficaz de los autenticadores de cuentas privilegiadas y una segmentación mejorada de la red. Si bien estos proyectos tienen componentes tácticos, representan un esfuerzo de planeación estratégica con objetivos a corto y largo plazo.

Adaptación del plan

Los planes de remediación deben personalizarse para reflejar las complejidades operativas únicas de la organización. Lo que funcionó bien para un incidente puede no ser aconsejable en otro.

Una de las consideraciones clave es el momento de las actividades de contención y erradicación. En algunos casos, la organización debe ejecutar actividades de contención y erradicación de inmediato, aunque no se comprenda completamente el alcance del incidente. En otros casos, dicho cronograma es contraproducente y, de hecho, puede prolongar la intrusión y aumentar el riesgo de robo de datos de la organización.

Al planear las actividades de remediación, se debe considerar el impacto que tendrá la Acción propuesta en función el ciclo de vida del ataque dirigido. Las capacidades que mejoran la capacidad de las organizaciones para detectar y responder ante ataques no deben pasarse por alto, ya que la prevención no siempre se puede lograr.

La Figura 112 ilustra el ciclo de vida común de los ataques dirigidos. La Tabla 10 contiene ejemplos de acciones de remediación comúnmente recomendadas como una forma de ilustrar la utilidad del enfoque enfocado en el ciclo de vida del ataque para la planeación de la remediación.

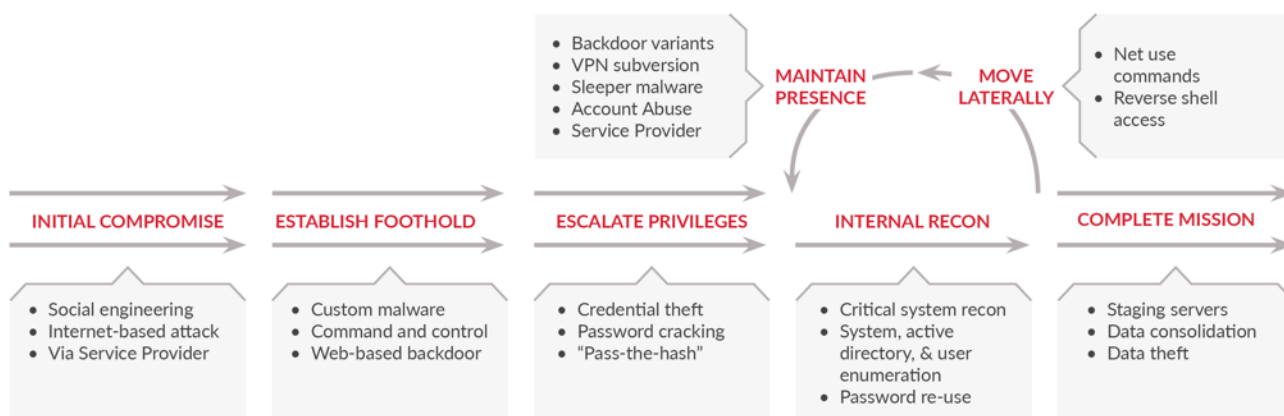


Figura 112: Ciclo de vida del ataque dirigido

	Compromiso inicial	Establecer un punto inicial / Mantener presencia	Escalar privilegios	Reconocimiento interno	Movimiento lateral	Completar la misión
Inhibir	Aplicación de parches para el usuario final Conciencia del usuario	Reducciones de privilegios del usuario final	Lista blanca de aplicaciones Huella reducida de cuentas privilegiadas	Restringir, internamente, la disponibilidad de la información de TI	Segmentación de la red Bloquear la comunicación entre estaciones de trabajo	Restringir los servidores que inician conexiones salientes

	Gestión de vulnerabilidades de los sistemas conectados a Internet					Advertencia de clic para sitios no categorizados
Detectar	ID de red	Anti-malware de última generación Apilamiento del mecanismo de persistencia	Análisis de anomalías de procesos	Análisis de anomalías de autenticación	Análisis de conexión de red	
Responder	Proceso urgente de parche Manual de restablecimiento de contraseña del usuario	Manuales de contención rápida Actividades de caza	Plan de respuesta a incidentes			

Tabla 10: Mitigar el ciclo de vida del ataque dirigido

APÉNDICE C: EXPLICACIÓN DEL CICLO DE VIDA DEL ATAQUE DIRIGIDO

La siguiente sección proporciona más contexto sobre el ciclo de vida de los ataques dirigidos el cual se muestra en la Figura 112.

Reconocimiento inicial: El atacante realiza una investigación sobre un objetivo. El atacante identifica objetivos (tanto sistemas como personas) y determina su metodología de ataque. El atacante puede buscar servicios de Internet o personas para explotar. La investigación del atacante también puede involucrar las siguientes actividades:

- Identificar sitios web que pueden ser vulnerables a las vulnerabilidades de las aplicaciones web.
- Analizar las actividades comerciales actuales o proyectadas de la organización objetivo
- Comprender la organización interna y los productos de la organización objetivo.
- Conferencias de investigación a las que asisten los empleados
- Navegar por sitios de redes sociales para identificar a los empleados y realizarles ingeniería social de manera más efectiva.

Compromiso inicial: El atacante ejecuta con éxito código malicioso en uno o más sistemas. Lo más probable es que esto ocurra por medio de la ingeniería social (la mayoría de las veces, el spear phishing), al explotar una vulnerabilidad en un sistema conectado a Internet o por cualquier otro medio necesario.

Establecer un punto inicial: El atacante se asegura de mantener un control continuo sobre un sistema recientemente comprometido. Esto ocurre inmediatamente después del compromiso inicial. Por lo general, el atacante establece un punto inicial instalando una puerta trasera persistente o descargando utilerías adicionales o malware en el sistema de la víctima.

Escalar privilegios: El atacante obtiene un mayor acceso a los sistemas y datos. Los atacantes a menudo escalan sus privilegios mediante el volcado de hash de contraseñas (seguido de ataques de craqueo de contraseñas o pass-the-hash); registro de pulsaciones de teclas/credenciales, obtención de certificados PKI, aprovechamiento de los privilegios de una aplicación o explotación de una pieza de software vulnerable.

Reconocimiento interno: El atacante explora el entorno de la víctima para obtener una mejor comprensión del entorno, los roles y responsabilidades de las personas clave y para determinar dónde una organización almacena información de interés.

Movimiento lateral: El atacante utiliza su acceso para moverse de un sistema a otro dentro del entorno comprometido. Los métodos comunes de movimiento lateral incluyen acceder a recursos compartidos de red, utilizar el Programador de tareas de Windows para ejecutar programas, utilizar herramientas de acceso remoto como PsExec o utilizar clientes de escritorio remoto como Remote Desktop Protocol (RDP), DameWare o Virtual Network Computing (VNC) para interactuar con los sistemas de destino mediante una interfaz gráfica de usuario.

Mantener presencia: El atacante garantiza el acceso continuo al entorno. Los métodos comunes para mantener una presencia incluyen la instalación de múltiples variantes de puertas traseras de malware o la obtención de acceso a servicios de acceso remoto como la Red Privada Virtual (VPN) corporativa.

Completar la misión: El atacante logra su objetivo. A menudo, esto significa robar propiedad intelectual, datos financieros, información sobre fusiones y adquisiciones o información de identificación personal (PII). Una vez que se ha completado la misión, la mayoría de los atacantes objetivo no abandonan el entorno, pero mantienen el acceso en caso de que se realice una nueva misión.

APÉNDICE D: DESCRIPCIÓN GENERAL DE SYSMON



Monitoreo de
seguridad (SYSMON).



FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2020 FireEye, Inc. All rights reserved. FireEye and Mandiant are registered trademarks of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

