



CORPORACIÓN HMENTOR
Informe de resultados de la auditoría
de seguridad

Confidencialidad empresarial

Fecha: 20 de abril del 2023

Proyecto: Versión 001

Tabla de Contenidos

Tabla de Contenidos.....	2
Declaración de confidencialidad	3
Descargo de responsabilidad.....	3
Información de Contacto	3
Componentes de la evaluación	4
Prueba de penetración interna	4
Limpieza interna	5
Índices de severidad de los hallazgos	6
Factores de riesgo	6
Probabilidad	6
Impacto	6
Alcance.....	7
Exclusiones del alcance	7
Prestaciones del cliente.....	7
Resumen Ejecutivo	8
Alcance y limitaciones de tiempo	8
Resumen de las pruebas	8
Notas y recomendaciones de las pruebas.....	10
Puntos Fuertes y débiles.....	11
Resumen e Informe de Vulnerabilidades	12
Resultados de la prueba de penetración interna.....	12
Hallazgos Técnicos	14
Resultados de la prueba de penetración interna.....	14
Migrar a protocolos protegidos por TLS.	31
Escaneos e informes adicionales.....	32

Declaración de confidencialidad

Este documento es propiedad exclusiva de Corporación HMENTOR y Hacker Mentor. Este documento contiene información propietaria y confidencial. La reproducción, redistribución o utilización, total o parcial, en cualquier forma, requiere el consentimiento tanto de Corporación HMENTOR como de Hacker Mentor.

Corporación HMENTOR puede compartir este documento con auditores bajo acuerdos de no divulgación para demostrar el cumplimiento de los requisitos de las pruebas de penetración.

Descargo de responsabilidad

Una prueba de penetración se considera un snapshot en el tiempo. Las conclusiones y recomendaciones reflejan la información recopilada durante la evaluación y no los cambios o modificaciones realizados fuera de este período.

Una auditoría de seguridad limitada en su duración no permite una evaluación completa de todos los controles de seguridad. Hacker Mentor priorizó la evaluación para identificar los controles de seguridad más débiles que un atacante podría explotar. Hacker Mentor recomienda llevar a cabo evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito ininterrumpido de los controles.

Información de Contacto

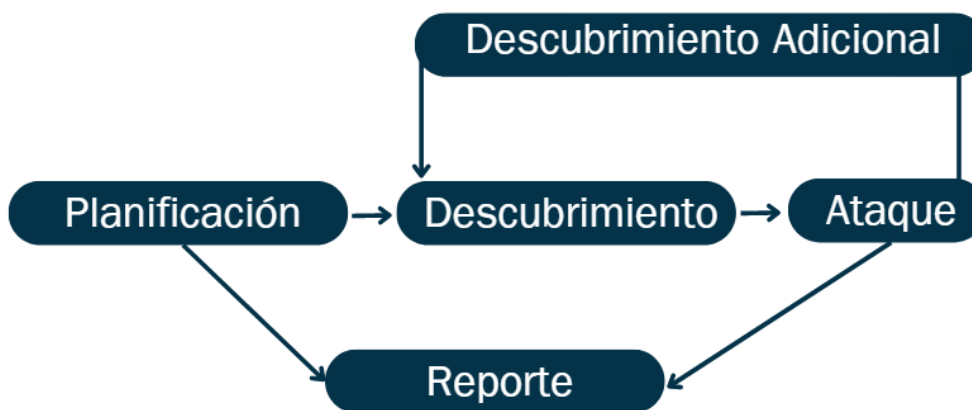
Name	Title	Contact Information
Corporación HMENTOR		
Jon Ramírez	Vicepresidente de Seguridad de la Información (CISO)	Email: jramirez@corporacionHMENTOR.com
Ana Rodríguez	Directora de TI	Email: arodriguez@corporacionHMENTOR.com
Hacker Mentor		
Cristian Vasco	Pentester Líder	Email: cvasco@hacker-mentor.com

Evaluación general

Del 25 de marzo de 2023 al 14 de abril de 2023, Corporación HMENTOR contrató a Hacker Mentor para evaluar el estado general de seguridad de su infraestructura en comparación con las mejores prácticas actuales del sector, que incluían una prueba de penetración en la red interna. Todas las pruebas realizadas se basan en la Guía técnica de pruebas y evaluación de seguridad de la información NIST SP 800-115, la Guía de pruebas OWASP (v4) y marcos de pruebas personalizados.

Las fases de las actividades de pruebas de penetración realizadas se incluyen a continuación:

- Planificación – Se reunieron los objetivos del cliente y se obtuvieron las reglas de compromiso
- Descubrimiento – Se realizaron escaneos y enumeraciones para identificar vulnerabilidades potenciales, áreas débiles, y exploits.
- Ataque – Se confirmaron las vulnerabilidades potenciales a través de la explotación y se realizaron descubrimientos adicionales tras un nuevo acceso.
- Reporte – Se documentaron todas las vulnerabilidades y explotaciones encontradas, los intentos fallidos y los puntos débiles y fuertes de la organización.



Componentes de la evaluación

Prueba de penetración interna

Una prueba de penetración interna emula el papel de un atacante que intenta acceder a la información y los dispositivos ubicados en la red interna sin consentimiento. Se realizó esta prueba desde dentro de la red interna emulando que el adversario ya hubiera encontrado un punto inicial

de acceso en una máquina interna con pocos privilegios. En una prueba de penetración el ingeniero escanea la red para identificar posibles vulnerabilidades del host objetivo y realiza ataques comunes y avanzados a la red interna, tales como: Envenamiento LLMNR/NBT-NS y otros ataques de man-in-the-middle, suplantación de token, kerberoasting, pass the hash, Golden ticket, etc. El ingeniero tratará de obtener acceso a los hosts a través del movimiento lateral, comprometer las cuentas de usuario de dominio y de administrador, y filtrar datos sensibles. Todos los pasos para reproducir y evaluar las vulnerabilidades encontradas se explicarán en este informe.

Limpieza interna

La parte de limpieza al finalizar la auditoría garantiza la eliminación de los restos de la prueba de penetración. A menudo, quedan fragmentos de herramientas o cuentas de usuario en el ordenador de una organización, producto de la prueba de penetración, lo que podría causar problemas de seguridad en un futuro. Una vez completados con éxito los objetivos, Hacker Mentor eliminó todas las cuentas de usuario y contraseñas, así como los servicios de Meterpreter instalados en el sistema. Corporación HMENTOR no debería tener que eliminar ninguna cuenta de usuario o servicio de ninguno de los sistemas causados por la auditoría de seguridad.

Índices de severidad de los hallazgos

La siguiente table define los niveles de gravedad y el rango de puntuación CVSS correspondiente que se utilizan en todo el documento para evaluar la vulnerabilidad y el impacto del riesgo.

Severidad	CVSS V3 Escala de puntuación	Definición
Crítica	9.0-10.0	La explotación es sencilla y suele resultar en un compromiso a nivel de sistema. Se aconseja elaborar un plan de acción y parchear inmediatamente.
Alta	7.0-8.9	La explotación es más difícil, pero podría causar privilegios elevados y potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda elaborar un plan de acción y parchear lo antes posible.
Moderada	4.0-6.9	Existen vulnerabilidades, pero no son explotables o requieren pasos adicionales como la ingeniería social. Se aconseja elaborar un plan de acción y aplicar parches una vez resueltos los problemas de alta prioridad.
Baja	0.1-3.9	Las vulnerabilidades no son explotables, pero reducirían la superficie de ataque de una organización. Se aconseja elaborar un plan de acción y parchear durante la próxima ventana de mantenimiento.
Informativa	N/A	No existe ninguna vulnerabilidad. Se proporciona información adicional sobre los elementos detectados durante las pruebas, los controles estrictos y la documentación adicional.

Factores de riesgo

El riesgo se mide por dos factores: Probabilidad e Impacto:

Probabilidad

La probabilidad mide el potencial de explotación de una vulnerabilidad. Las puntuaciones se otorgan en función de la dificultad del ataque, las herramientas disponibles, el nivel de habilidad del atacante y el entorno del cliente.

Impacto

El impacto mide el efecto potencial de la vulnerabilidad en las operaciones, incluyendo la confidencialidad, integridad y disponibilidad de los sistemas y/o datos del cliente, el daño a la reputación y las pérdidas financieras.

Alcance

Assessment	Details
Prueba de penetración interna	192.168.190.x/24

Exclusiones del alcance

A petición del cliente, Hacker Mentor no realizó ninguno de los siguientes ataques durante las pruebas:

- Denegación de servicio (DoS)
- Phishing/Ingeniería social

Todos los demás ataques no especificados anteriormente fueron permitidos por Corporación HMENTOR.

Prestaciones del cliente

Corporación HMENTOR no proporcionó a Hacker Mentor ninguna prestación para ayudar en las pruebas de penetración.

Resumen Ejecutivo

Hacker Mentor evaluó el estado general de seguridad interna de Corporación HMENTOR mediante pruebas de penetración del 25 de marzo de 2023 al 14 de abril de 2023. Las siguientes secciones proporcionan una visión general de alto nivel de las vulnerabilidades descubiertas, los intentos exitosos y fallidos, y las fortalezas y debilidades.

Alcance y limitaciones de tiempo

El alcance durante la evaluación no permitió la denegación de servicio ni la ingeniería social en ningún componente de las pruebas.

Se establecieron limitaciones de tiempo para las pruebas. Las pruebas de penetración en la red interna se permitieron durante quince (15) días laborables.

Resumen de las pruebas

La evaluación de la red valoró el estado general de seguridad de la red interna de Corporación HMENTOR. Desde una perspectiva interna, el equipo de Hacker Mentor realizó un escaneo de vulnerabilidades contra todas las IP proporcionadas por Corporación HMENTOR para evaluar los parches de seguridad implementados en la red. El equipo también realizó ataques comunes basados en Active Directory, como envenenamiento de resolución de nombres de multidifusión local y enlace (LLMNR), retransmisión SMB, retransmisión IPv6 man-in-the-middle y Kerberoasting. Además de la exploración de vulnerabilidades y los ataques al Directorio Activo, Hacker Mentor evaluó otros riesgos potenciales, como archivos compartidos abiertos en la red, credenciales predeterminadas en servidores/dispositivos y divulgación de información confidencial para obtener una imagen completa de la postura de seguridad de la red.

El equipo de Hacker Mentor descubrió que LLMNR estaba habilitado en la red (hallazgo PPI-001), lo que permitía la interceptación de hashes de usuario mediante envenenamiento LLMNR. Estos hashes fueron tomados fuera de línea y descifrados a través de ataques de diccionario, lo que indica una débil política de contraseñas (hallazgo PPI-005). Utilizando las contraseñas crackeadas, el equipo Hacker Mentor obtuvo acceso a varias máquinas dentro de la red, lo que indica cuentas de usuario excesivamente permisivas.

Con el acceso a las máquinas, y el uso de sistemas operativos antiguos en la red (hallazgo PPI-008), el equipo fue capaz de aprovechar WDigest (hallazgo PPI-003) para recuperar las credenciales en texto claro de las cuentas. El equipo también fue capaz de volcar hashes de cuentas locales en cada máquina a la que se accedía. El equipo de Hacker Mentor descubrió que los hashes de las cuentas locales se reutilizaban en distintos dispositivos (hallazgo PPI-002), lo que permitió acceder a más máquinas mediante ataques pass-the-hash.

Finalmente, el equipo de Hacker Mentor fue capaz de aprovechar las cuentas capturadas a través de WDigest y hash dumps para moverse lateralmente a través de la red hasta aterrizar en una máquina que tenía una credencial de administrador de dominio en texto claro a través de WDigest. El equipo de pruebas pudo utilizar esta credencial para iniciar sesión en el controlador de dominio y comprometer todo el dominio.

Además de las vulnerabilidades enumeradas anteriormente, el equipo de Hacker Mentor descubrió que se podía suplantar la identidad de los usuarios mediante ataques de delegación (hallazgo PPI-004), por lo que era posible realizar ataques de retransmisión SMB debido a que la firma SMB estaba desactivada (hallazgo PPI-007) y que el tráfico IPv6 no estaba restringido, lo que podía dar lugar a la retransmisión LDAPS y al compromiso del dominio (hallazgo PPI-006).

El resto de hallazgos críticos están relacionados con la gestión de parches, ya que se detectó la presencia en la red de sistemas operativos obsoletos (hallazgo PPI-008) y vulnerabilidades RCE de Microsoft (hallazgos PPI-009, PPI-010, PPI-011, PPI-012).

El resto de los hallazgos fueron altos, moderados, bajos o informativos. Para más información sobre los hallazgos, consulte la sección de hallazgos técnicos.

Notas y recomendaciones de las pruebas

Los resultados de las pruebas de la red de Corporación HMENTOR son indicativos de una organización que se somete a su primera prueba de penetración, como es el caso. Muchos de los hallazgos descubiertos son vulnerabilidades dentro de Active Directory que vienen activadas por defecto, como LLMNR, IPv6 y Kerberoasting.

Durante las pruebas, destacaron dos constantes: una política de contraseñas débil y un parcheado débil. La política de contraseñas débiles condujo al compromiso inicial de las cuentas y suele ser uno de los primeros puntos de apoyo que un atacante intenta utilizar en una red. La presencia de una política de contraseñas débil está respaldada por la evidencia de que nuestro equipo de pruebas descifró más de 120 contraseñas de cuentas de usuario, incluida la mayoría de las cuentas de administrador de dominio, mediante ataques básicos de diccionario.

Recomendamos que Corporación HMENTOR reevalúe su política de contraseñas actual y considere una política de 15 caracteres o más para sus cuentas de usuario normales y de 30 caracteres o más para sus cuentas de administrador de dominio. También recomendamos que Corporación HMENTOR incluya una lista negra de contraseñas y que evalúe la lista de contraseñas de usuario crackeadas. Por último, debería considerarse utilizar una solución de gestión de privilegios de acceso (PAM).

Los parches débiles y los sistemas operativos obsoletos llevaron a comprometer docenas de máquinas dentro de la red. Creemos que el número de máquinas comprometidas habría sido significativamente mayor, sin embargo, los equipos Hacker Mentor y Corporación HMENTOR acordaron que no era necesario intentar explotar ninguna vulnerabilidad basada en ejecución remota de código (RCE), como MS17-010 (hallazgo PPI-011), ya que el controlador de dominio ya había sido comprometido y los equipos no querían arriesgarse a ninguna denegación de servicio a través de ataques fallidos.

Recomendamos que el equipo de Corporación HMENTOR revise las recomendaciones de parcheo realizadas en la sección de hallazgos técnicos del informe junto con la revisión de los escaneos de Nessus proporcionados para obtener una visión completa de los elementos que deben parchearse. También recomendamos que Corporación HMENTOR mejore sus políticas y procedimientos de gestión de parches para ayudar a prevenir posibles ataques dentro de su red.

Como nota positiva, nuestro equipo de pruebas activó varias alertas durante el compromiso. El equipo de operaciones de seguridad de Corporación HMENTOR descubrió nuestro escaneo de vulnerabilidades y recibió una alerta cuando intentamos utilizar ataques ruidosos en una máquina comprometida. Aunque no se descubrieron todos los ataques durante las pruebas, estas alertas son un comienzo positivo. Se ha proporcionado orientación adicional sobre alertas y detección para los hallazgos, cuando ha sido necesario, en la sección de hallazgos técnicos.

En general, la red de Corporación HMENTOR funcionó como se esperaba para una prueba de penetración realizada por primera vez. Recomendamos que el equipo de Corporación HMENTOR revise a fondo las recomendaciones formuladas en este informe, parchee los hallazgos y vuelva a realizar la prueba anualmente para mejorar su postura general de seguridad interna.

Puntos Fuertes y débiles

A continuación, se identifican los principales puntos fuertes detectados durante la evaluación:

1. Alertas en algunos escaneos de herramientas comunes (Nessus)
2. Mimikatz detectado en algunas máquinas
3. Las cuentas de servicio no se ejecutaban como administradores de dominio
4. La contraseña de cuenta de administrador local de Corporación HMENTOR era única para cada dispositivo.

A continuación, se identifican las principales debilidades detectadas durante la evaluación:

1. Política de contraseñas insuficientes
2. Sistemas operativos críticamente desactualizados y parches débiles
3. Se observaron contraseñas en texto claro debido a WDigest
4. LLMNR está habilitado dentro de la red
5. La firma SMB está habilitada en todos los dispositivos, excepto en servidores.
6. IPv6 se gestiona incorrectamente dentro de la red
7. Las cuentas de usuario pueden ser suplantadas a través de la delegación de tokens
8. Se descubrieron credenciales por defecto en infraestructuras críticas.
9. Se permitía el acceso no autenticado a recursos compartidos
10. Las cuentas de servicio utilizaban contraseñas débiles
11. Cuentas de administrador de dominio con contraseñas débiles

Resumen e Informe de Vulnerabilidades

Las siguientes tablas ilustran las vulnerabilidades encontradas por impacto y las soluciones recomendadas:

Resultados de la prueba de penetración interna

12	2	4	0	0
Crítica	Alta	Moderada	Baja	Informativa

Hallazgo	Severidad	Recomendación
Prueba de penetración interna (PPI)		
PPI-001: Configuración LLMNR insuficiente	Critical	Desactivar la resolución de nombres de multidifusión mediante GPO.
PPI-002: Error de configuración de seguridad - Reutilización de la contraseña de administrador local	Critical	Utilice contraseñas de administrador locales únicas y limite los usuarios administradores locales mediante privilegios mínimos.
PPI-003: Mala configuración de seguridad - Wdigest	Critical	Deshabilite WDigest mediante GPO.
PPI-004: Hardening insuficiente - Suplantación de token	Critical	Restrinja la delegación de token
PPI-005: Complejidad insuficiente de contraseñas	Critical	Implementar los requisitos de contraseña de CIS Benchmark / solución PAM.
PPI-006: Error de configuración - IPv6	Critical	Restringa el tráfico DHCPv6 y los anuncios de router entrantes en el Firewall de Windows a través de GPO.
PPI-007: Hardening insuficiente - Firma SMB deshabilitada	Critical	Habilite la firma SMB en todos los ordenadores del dominio Corporación HMENTOR
PPI-008: Gestión de parches insuficiente - Sistemas operativos	Critical	Actualice los sistemas operativos a la última versión.
PPI-009: Parcheado insuficiente - MS08-067 - ECLIPSEDWING/NETAPI	Critical	Aplice los parches de Microsoft adecuados para remediar el problema.

Hallazgo	Severidad	Recomendación
PPI-010: Parcheado insuficiente - MS12-020 - Remote Desktop RCE	Critical	Aplique los parches de Microsoft adecuados para remediar el problema.
PPI-011: Parcheado insuficiente - MS17-010 - EternalBlue	Critical	Aplique los parches de Microsoft adecuados para remediar el problema.
PPI-012: Parcheado insuficiente - CVE-2019-0708 - BlueKeep	Critical	Aplique los parches de Microsoft adecuados para remediar el problema.
PPI-013: Privilegios insuficientes - Gestión de cuentas - Kerberoasting	Alta	Utilizar cuentas de servicio (GMSA) para servicios privilegiados.
PPI-014: Credenciales por defecto en Servicios Web	Alta	Cambie las credenciales por defecto o desactive las cuentas que se utilicen.
PPI-015: Gestión de parches insuficiente - SMBv1	Moderada	Actualice a SMBv3 y aplique los últimos parches.
PPI-016: Divulgación de Hash IPMI	Moderada	Desactive IPMI sobre LAN si no es necesario.
PPI-017: Complejidad insuficiente de SNMP	Moderada	Deshabilite SNMP si no es necesario.
PPI-018: Cifrado insuficiente de datos en tránsito: Telnet	Moderada	Migre a protocolos protegidos por TLS

Hallazgos Técnicos

Resultados de la prueba de penetración interna

Hallazgo PPI-001: Configuración LLMNR insuficiente (Crítica)

Descripción:	Corporación HMENTOR permite la resolución de nombres multicast en sus redes de usuarios finales. Hacker Mentor capturó 20 hashes de cuentas de usuario envenando el tráfico LLMNR y crackeó 2 con software de cracking comercial.
Riesgo:	<p>Probabilidad: Alta – Este ataque es efectivo en entornos que permiten la resolución de nombres multicast.</p> <p>Impacto: Muy alto – El envenamiento LLMNR permite a los atacantes capturar hashes de contraseñas para crackearlos offline o retransmitirlos en tiempo real y pivotar lateralmente en el entorno.</p>
Sistema:	Todos
Herramientas utilizadas:	Responder, Hashcat
Referencias:	Stern Security - Local Network Attacks: LLMNR and NBT-NS Poisoning NIST SP800-53 r4 IA-3 - Device Identification and Authentication NIST SP800-53 r4 CM-6(1) - Configuration Settings

Evidencia

```
[13/04/23 5:58:48] (hmsstudent@hmsstudent)-[~]
[SMB] NTLMv2-SSP Client : fe80
[SMB] NTLMv2-SSP Username : HMENTOR\
[SMB] NTLMv2-SSP Hash : :: HMENTOR:
```

Figura 1: Hash capturado de "HMENTOR"

```
:: HMENTOR:4856b7e8f3
00000:Pa
```

Figura 2: Hash crackeado de "HMENTOR"

Remediación

Desactive la resolución de nombres de multidifusión mediante GPO. Para obtener una guía completa de mitigación y detección, consulte la guía de MITRE [aquí](#).

Los hashes crackeados demuestran una política de complejidad de contraseñas deficiente. Si se requiere la resolución de nombres de multidifusión, el control de acceso a la red (NAC) combinado con listas blancas de aplicaciones puede limitar estos ataques.

Hallazgo PPI-002: Error de configuración de seguridad - Reutilización de la contraseña de administrador local (Crítica)

Descripción:	<p>Hacker Mentor utilizó hashes de administradores locales para obtener acceso a otras máquinas de la red mediante un ataque "pass-the-hash". Los hashes de administrador local se obtuvieron a través del acceso a máquinas proporcionado por la cuenta crackeada en PPI-001.</p> <p>Los ataques "pass-the-hash" no requieren conocer la contraseña de la cuenta para acceder con éxito a una máquina. Por lo tanto, la reutilización de la misma contraseña de administrador local (y por lo tanto el mismo hash) en varias máquinas permitirá el acceso al sistema de esos equipos.</p> <p>Hacker Mentor aprovechó este ataque para obtener acceso a ~10 máquinas dentro de la red principal. Esto condujo a un mayor acceso a las cuentas y al compromiso final del controlador de dominio.</p>
Riesgo:	<p>Probabilidad: Alta – Este ataque es efectivo en redes grandes con reutilización de contraseñas de administradores locales.</p> <p>Impacto: Muy alto – Pass-the-hash permite a un atacante moverse lateral y verticalmente por toda la red.</p>
Sistema:	Todos
Herramientas utilizadas:	Impacket, Crackmapexec
Referencias:	https://capec.mitre.org/data/definitions/644.html

Evidencia

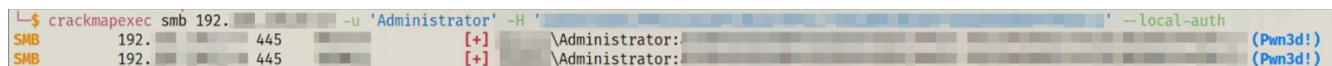


Figura 3: Hash de administrador local usado para obtener acceso a otros equipos

Remediación

Utilice contraseñas de administrador locales únicas. Limite los usuarios administradores locales mediante privilegios mínimos. Considere la implementación de una solución PAM. Para una guía completa de mitigación y detección, consulte la guía de MITRE [aquí](#).

Hallazgo PPI-003: Mala configuración de seguridad - WDigest (Crítica)

Descripción:	<p>Corporación HMENTOR utiliza sistemas operativos obsoletos en su red, incluidos Windows 7, 8, Server 2008 y Server 2012.</p> <p>Estos sistemas operativos, por defecto, permiten WDigest, que almacena todas las contraseñas de los usuarios conectados en texto claro.</p> <p>Hacker Mentor aprovechó el acceso a máquinas obtenidas en PPI-001 e PPI-002 para moverse lateralmente por la red hasta descubrir una máquina con credenciales de administrador de dominio almacenadas en WDigest.</p>
Riesgo:	<p>Probabilidad: Moderada – Este ataque es efectivo en redes con sistemas operativos antiguos</p> <p>Impacto: Muy alto – Las credenciales de WDigest se almacenan en texto claro, lo que puede permitir el robo de cuentas sensibles, como Administradores de Dominio.</p>
Sistema:	Todos los sistemas anteriores a Windows 10 y Server 2016
Herramientas utilizadas:	Metasploit, Kiwi
Referencias:	https://stealthbits.com/blog/wdigest-clear-text-passwords-stealing-more-than-a-hash/

Evidencia

```
meterpreter > creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials

Username      Domain      Password
-----
ar           HMENTOR    Pa
ma           HMENTOR    Pa
```

Figura 4: Contraseñas en texto claro de administradores de dominio

Remediación

Desactive WDigest a través de GPO. Para una guía completa de mitigación y detección, por favor consulte la guía [aquí](#).

Hallazgo PPI-004: Hardening insuficiente –Suplantación de token (Crítica)

Descripción:	Hacker Mentor suplantó el token de "arivadeneira" para obtener privilegios de Administrador de Dominio.
Riesgo:	<p>Probabilidad: Alta– El auditor de seguridad vio y suplantó tokens con el uso de herramientas de código abierto</p> <p>Impacto: Muy alto – Si se explota, un atacante obtiene acceso de administrador de dominio.</p>
Sistema:	Todos
Herramientas utilizadas:	Metasploit, Incognito
Referencias:	<p>NIST SP800-53 r4 CM-7 - Least Functionality</p> <p>NIST SP800-53 r4 AC-6 - Least Privilege</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts</p>

Evidencia

```
meterpreter > impersonate_token [redacted] \\ariv [redacted]
[+] Delegation token available
[+] Successfully impersonated user [redacted] \\ariv [redacted]
```

Figura 5: Suplantación de "ariv"

```
meterpreter > shell
Process 284 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
[redacted] \\ariv [redacted]
```

Figura 6: Acceso por Shell como Administrador de Dominio "ariv"

Remediación

Restringir la delegación de tokens. Para obtener una guía completa de mitigación y detección, consulte la guía de MITRE [aquí](#).

Hallazgo PPI-005: Complejidad insuficiente de contraseñas (Crítica)

Descripción:	<p>Hacker Mentor volcó los hashes del controlador de dominio y procedió a intentar ataques de crackeo de contraseñas contra todos los usuarios.</p> <p>Hacker Mentor descifró 123 contraseñas utilizando ataques de diccionario y ataques de fuerza bruta de bajo esfuerzo. 2 cuentas crackeadas tenían derechos de administrador de dominio.</p>
Riesgo:	<p>Probabilidad: Alta– Las contraseñas sencillas son susceptibles de ataques de descifrado de contraseñas. El cifrado proporciona cierta protección, pero los ataques de diccionario basados en listas de palabras comunes suelen descifrar las contraseñas débiles.</p> <p>Impacto: Muy alto –Las cuentas de administrador de dominio con contraseñas débiles podrían llevar a un adversario a afectar críticamente la capacidad de Corporación HMENTOR para operar.</p>
Sistema:	Todos
Herramientas utilizadas:	Hashcat
Referencias:	<p>NIST SP800-53 IA-5(1) - Authenticator Management</p> <p>https://www.cisecurity.org/white-papers/cis-password-policy-guide/</p>

Evidencia

Cuenta	Contraseña
HMENTOR\usermonitoreo	s1st3m4s0l4r!
HMENTOR\pparrales	Masterweb*1
HMENTOR\adminfcme	S3GUR1D4D*
HMENTOR\prugel	Abcd1234
HMENTOR\emalvarado	Qwer1234
HMENTOR\jarauz	211Mikaela
HMENTOR\falcivar	Asdf4321
HMENTOR\ntenecela	Mamita1212
HMENTOR\jlopez	qweR1234
HMENTOR\mespinoza	Marce1988
HMENTOR\auditoriasbs3	cesantia

Figura 7: Extracto de hashes de dominio crackeados

Remediación

Implementar los requisitos de contraseña de CIS Benchmark / solución PAM. Hacker Mentor recomienda que Corporación HMENTOR aplique las mejores prácticas de la industria en torno a la complejidad y gestión de contraseñas. También se recomienda un filtro de contraseñas para evitar que los usuarios utilicen contraseñas comunes y fáciles de adivinar. Además, Hacker Mentor recomienda que Corporación HMENTOR aplique requisitos de contraseña más estrictos para el administrador del dominio y otras cuentas sensibles.

Hallazgo PPI-006: Error de configuración –IPV6 (Crítica)

Descripción:	Mediante el envenenamiento de DNS IPv6, el equipo de Hacker Mentor fue capaz de transmitir con éxito las credenciales al controlador de dominio de Corporación HMENTOR.
Riesgo:	<p>Probabilidad: Alta - IPv6 está activado por defecto en las redes Windows. Las herramientas y técnicas necesarias para realizar esta tarea son triviales.</p> <p>Impacto: Muy alto – Si se explota, un atacante puede obtener acceso de administrador de dominio.</p>
Sistema:	Todos
Herramientas utilizadas:	Mitm6, Impacket
Referencias:	https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/

Evidencia

```
[*] Authenticating against ldaps://192.168.1.100 as Administrator VA$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] Authenticating against ldaps://192.168.1.100 as Administrator VA$ SUCCEED
```

Figura 8: Transmisión con éxito de credenciales LDAP a través de mitm6

Remediación

1. El envenenamiento IPv6 abusa del hecho de que Windows busca una dirección IPv6 incluso en entornos sólo IPv4. Si no utilizas IPv6 internamente, la forma más segura de prevenir el mitm6 es bloquear el tráfico DHCPv6 y los anuncios entrantes del router en el Firewall de Windows a través de la directiva de grupo. Deshabilitar IPv6 por completo puede tener efectos secundarios no deseados.
2. Si WPAD no se utiliza internamente, desactívelo mediante la directiva de grupo y desactivando el servicio WinHttpAutoProxySvc.
3. La retransmisión a LDAP y LDAPS sólo se puede mitigar habilitando tanto la firma LDAP como la vinculación de canal LDAP.

Considere la posibilidad de administrar usuarios al grupo “Usuarios protegidos” o marcarlos como “Cuenta es confidencial y no se pueda delegar”, lo que impedirá cualquier suplantación de ese usuario mediante delegación.

Hallazgo PPI-007: Hardening insuficiente – Firma SMB deshabilitada (Crítica)

Descripción:	Corporación HMENTOR no implementó la firma SMB en varios dispositivos. La ausencia de firma SMB podría dar lugar a ataques de retransmisión SMB, que permitirían acceder a shell a nivel de sistema sin necesidad de una contraseña de usuario.
Riesgo:	<p>Probabilidad: Alta - La retransmisión de hashes de contraseñas es una técnica básica que no requiere crackeo offline.</p> <p>Impacto: Muy alto – Si se explota, un adversario obtiene la ejecución de código, lo que conduce a un movimiento lateral a través de la red.</p>
Sistema:	Todos
Herramientas utilizadas:	MultiRelay, Responder
Referencias:	CIS Microsoft Windows Server 2012 R2 v2.2.0 (Page 180) https://github.com/Igandx/Responder/blob/master/tools/MultiRelay.py

Evidencia

```
[*] SMBD-Thread-9: Received connection from 192.168.1.100, attacking target smb://192.168.1.100
[*] Authenticating against smb://192.168.1.100 as Administrator \z SUCCEED
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11003
```

Figura 8: Retransmisión SMB satisfactoria

Remediación

Habilite la firma SMB en todos los equipos del dominio Corporación HMENTOR. Como alternativa, dado que la firma SMB puede causar problemas de rendimiento, desactivar la autenticación NTLM, aplicar la jerarquización de cuentas y limitar los usuarios administradores locales puede ayudar a mitigar eficazmente los ataques. Para obtener orientación completa sobre la mitigación y la detección, consulte la guía de MITRE [aquí](#).

Hallazgo PPI-008: Gestión de parches insuficiente – Sistemas operativos (Crítica)

Descripción:	<p>Corporación HMENTOR utiliza varios sistemas obsoletos en su red. Esto incluye:</p> <ul style="list-style-type: none">- Windows Server 2003 (fin de vida el 14 de julio de 2015)- Windows Server 2008 R2 (fin de su vida útil el 14 de enero de 2020)- Windows XP (fin de su vida útil el 8 de abril de 2014)- Windows 7 (fin de su vida útil el 14 de enero de 2020)- Ubuntu 11 (fin de vida útil el 9 de mayo de 2013) <p>Los sistemas al final de su vida útil son susceptibles a multitud de vulnerabilidades. Hacker Mentor no intentó ningún ataque contra estos servidores debido al riesgo de denegación de servicio, que está fuera de su alcance.</p>
Riesgo:	<p>Probabilidad: Alta - Un atacante puede descubrir estas vulnerabilidades con herramientas básicas.</p> <p>Impacto: Alto - Si se explota, un atacante podría obtener la ejecución remota completa de código o denegar el servicio a un sistema.</p>
Sistema:	192.168.190.x
Herramientas utilizadas:	Nessus
Referencias:	<p>NIST SP800-53 r4 MA-6 – Timely Maintenance</p> <p>NIST SP800-53 r4 SI-2 – Flaw Remediation</p>

Remediación

Actualice los sistemas operativos a la última versión.

Hallazgo PPI-009: Parcheado insuficiente - MS08-067 - ECLIPSEDWING/NETAPI (Crítica)

Descripción:	Corporación HMENTOR utiliza un sistema sin parches en la red interna que es vulnerable a MS08-067. Hacker Mentor confirmó que la vulnerabilidad probablemente existe, pero no intentó lanzar el exploit para evitar cualquier denegación de servicio.
Riesgo:	<p>Probabilidad: Alta - Considerada una de las vulnerabilidades más explotadas en Microsoft Windows, ya que se distribuye de forma nativa con Windows XP.</p> <p>Impacto: Muy alto - Si se explota, un atacante obtiene la ejecución de código como usuario del sistema del sistema. Un adversario necesitará técnicas adicionales para obtener acceso de administrador de dominio.</p>
Sistema:	192.168.190.x
Herramientas utilizadas:	Nessus, Nmap
Referencias:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidencia

```

$ nmap -p 445 192.168.190.x --script smb-vuln-ms08-067
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-14 19:07 EDT
Nmap scan report for 192.168.190.x
Host is up (0.00046s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs: CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_

```

Figura 9: MS08-067 sin parchear

Remediación

Aplique los parches de Microsoft adecuados para solucionar el problema. Encontrará más información sobre el parche MS08-067 aquí: <https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067>

Hallazgo PPI -010: Parcheado insuficiente - MS12-020 – Remote Desktop RCE (Crítica)

Descripción:	Corporación HMENTOR utiliza un sistema sin parches en la red interna que es vulnerable a MS12-020. Hacker Mentor confirmó que la vulnerabilidad probablemente existe, pero no intentó lanzar el exploit para evitar cualquier denegación de servicio.
Riesgo:	<p>Probabilidad: Alta - La vulnerabilidad es fácilmente descubrible y explotable con herramientas de código abierto.</p> <p>Impacto: Muy alto - Si se explota, un atacante obtiene la ejecución de código como el sistema del sistema. Un adversario necesitará técnicas adicionales para obtener acceso de administrador de dominio.</p>
Sistema:	192.168.190.x
Herramientas utilizadas:	Nessus, Nmap
Referencias:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidencia

```

$ nmap -p 3389 192.168.190.x --script rdp-vuln-ms12-020
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-14 19:19 EDT
Nmap scan report for 192.168.190.x
Host is up (0.00049s latency).

PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
| rdp-vuln-ms12-020:
| VULNERABLE:
| MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|   State: VULNERABLE
|   IDs: CVE:2012-0152
|   Risk factor: Medium CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
| MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|   State: VULNERABLE
|   IDs: CVE:2012-0002
|   Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|   Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
|
| Disclosure date: 2012-03-13
| References:
|   http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_

```

Figura 10: MS12-020 sin parchear

Remediación

Aplique los parches de Microsoft adecuados para solucionar el problema. Puede encontrar más información sobre el parche MS12-020 aquí: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-020>

Hallazgo PPI -011: Parcheado insuficiente - MS17-010 – EternalBlue (Crítica)

Descripción:	Corporación HMENTOR utiliza varios sistemas sin parches en la red interna que son vulnerables a MS17-010. Hacker Mentor confirmó que la vulnerabilidad probablemente existe, pero no intentó lanzar el exploit para evitar cualquier denegación de servicio.
Riesgo:	<p>Probabilidad: Alta - Actores maliciosos han utilizado exploits de SMB como EternalBlue en brechas recientes.</p> <p>Impacto: Muy alto - Si se explota, un atacante obtiene la ejecución de código como el sistema del sistema. Un adversario necesitará técnicas adicionales para obtener acceso de administrador de dominio.</p>
Sistema:	192.168.190.x
Herramientas utilizadas:	Nessus, Metasploit, AutoBlue
Referencias:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidencia

```
[14/04/23 7:53:26] (hmstudent@hmstudent)-[/opt/exploits/AutoBlue-MS17-010]
$ python eternal_checker.py 192.168.190.x
[*] Target OS: Windows 7 Ultimate 7601 Service Pack 1
[!] The target is not patched
== Testing named pipes ==
[*] Done
```

Figura 11: MS17-010 sin parchear

Remediación

Aplique los parches de Microsoft adecuados para solucionar el problema. Puede encontrar más información sobre el parche MS17-010 aquí: <https://docs.microsoft.com/en-us/securityupdates/securitybulletins/2017/ms17-010>

Hallazgo-012: Parcheado insuficiente – CVE-2019-0708 –BlueKeep (Crítica)

Descripción:	Corporación HMENTOR utiliza varios sistemas sin parches en la red interna que son vulnerables a CVE-2019-0708 (BlueKeep). Hacker Mentor confirmó que la vulnerabilidad probablemente existe, pero no intentó lanzar el exploit para evitar cualquier denegación de servicio.
Riesgo:	<p>Probabilidad: Alta - La vulnerabilidad es fácilmente descubrible y explotable con herramientas de código abierto.</p> <p>Impacto: Muy alto - Si se explota, un atacante obtiene la ejecución de código como el sistema del sistema. Un adversario necesitará técnicas adicionales para obtener acceso de administrador de dominio.</p>
Sistema:	192.168.190.x
Herramientas utilizadas:	Nessus, Nmap
Referencias:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidencia

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run
[*] Started reverse TCP handler on 192.168.190.139:4444
[*] 192.168.190.139:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.190.139:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.190.139:3389 - The target is vulnerable. The target attempted cleanup of the incor
```

Figura 12: CVE-2019-0708 sin parchear

Remediación

Aplique los parches de Microsoft adecuados para solucionar el problema. Puede encontrar más información sobre el parche CVE-2019-0708 aquí: <https://support.microsoft.com/en-us/topic/customer-guidance-for-cve-2019-0708-remote-desktop-services-remote-code-execution-vulnerability-may-14-2019-0624e35b-5f5d-6da7-632c-27066a79262e>

Hallazgo-013: Privilegios insuficientes - Gestión de cuentas - Kerberoasting (Alta)

Descripción:	<p>Hacker Mentor recuperó todos los nombres principales de servicio (SPN) de usuario del controlador de dominio de Corporación HMENTOR utilizando una cuenta de nivel de usuario de dominio (PPI-001) en un ataque Kerberoasting. La recuperación de estos SPN de usuario permitió a Hacker Mentor descifrar 1 contraseña de cuenta.</p> <p>No se observaron cuentas de servicio ejecutándose como administradores de dominio. Se observaron cuentas de usuario ejecutándose como servicio, lo cual no es una buena práctica.</p>
Riesgo:	<p>Probabilidad: Alta - Cualquier cuenta unida al dominio puede solicitar SPNs de usuario.</p> <p>Impacto: Alto - Usando SPNs, es posible recuperar hashes de contraseñas de cuentas sensibles y crackearlas offline.</p>
Herramientas utilizadas:	Impacket, Hashcat
Referencias:	Kerberoasting details: https://adsecurity.org/?p=2293 Group Managed Service Accounts Overview

Evidencia

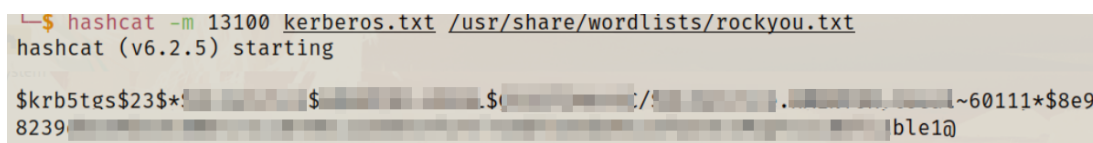


Figura 13: Servicio de cuenta crackeado

Remediación

Utilice cuentas de servicio gestionadas por grupo (GMSA) para los servicios privilegiados. Las cuentas GMSA pueden utilizarse para garantizar que las contraseñas son largas, complejas y cambian con frecuencia. Cuando GMSA no sea aplicable, proteja las cuentas utilizando una solución de bóveda de contraseñas.

Hacker Mentor recomienda configurar el registro de alertas en los controladores de dominio para el evento de Windows ID 4769 siempre que se solicite un ticket de servicio Kerberos. Estas alertas son propensas a altas tasas de falsos positivos, pero son un control de detección complementario. Adapte una herramienta de gestión de eventos e información de seguridad (SIEM) para alertar sobre solicitudes excesivas de SPN de usuario.

Hallazgo-014: Credenciales por defecto en Servicios Web (Alta)

Descripción:	Las credenciales predeterminadas validadas de Hacker Mentor funcionaron en múltiples aplicaciones web dentro del entorno de Corporación HMENTOR.
Riesgo:	<p>Probabilidad: Alta - Se publican credenciales para estos dispositivos y un atacante realiza el primer intento de autenticación.</p> <p>Impacto: Alto - Los atacantes pueden controlar dispositivos, destruir datos o apagar sistemas.</p>
Sistema:	Las credenciales predeterminadas se probaron en un conjunto de aplicaciones web.
Herramientas utilizadas:	Comprobación manual
Referencias:	NIST SP800-53 IA-5(1) - Authenticator Management

Evidencia

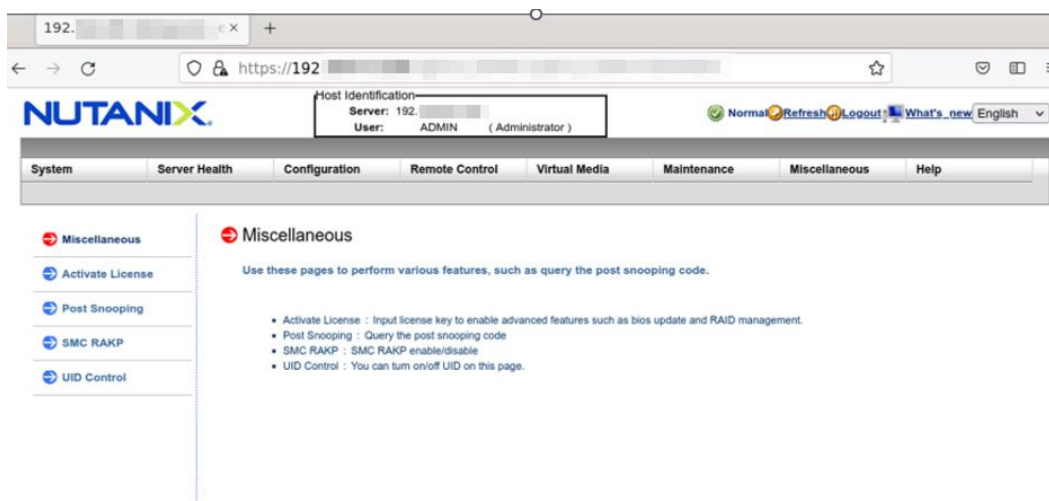


Figura 14: Acceso a NUTANIX cluster mediante credenciales predeterminadas

Remediación

Cambia las credenciales por defecto o desactive las cuentas que no utilices.

Hallazgo-015: Gestión de parches insuficiente – SMBv1 (Moderada)

Descripción:	Corporación HMENTOR no parchó SMBv1. Esta versión es vulnerable a múltiples ataques de denegación de servicio y ejecución remota de código. Hacker Mentor confirmó que la vulnerabilidad probablemente existe, pero no intentó el exploit para evitar cualquier denegación de servicio.
Riesgo:	<p>Probabilidad: Moderada - Los escaneos básicos identificarían la versión SMB pero requerirían que un adversario estuviera en la red interna e identificara un exploit.</p> <p>Impacto: Moderado - Si se explota, un atacante obtiene denegación de servicio y capacidad de ejecución de código.</p>
Sistema:	192.168.190.x
Herramientas utilizadas:	Nessus, Nmap
Referencias:	https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ NIST SP800-53 r4 SI-2 - Flaw Remediation

Evidencia

```

$ nmap -p 445 192.168.190.x --script smb-protocols
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-14 21:29 EDT
Nmap scan report for 192.168.190.x
Host is up (0.00034s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0.2
|     2.1
|_

```

Figura 15: Versión obsoleta de SMB

Remediación

Actualice a SMBv3 y aplique los últimos parches.

Hallazgo-016: Divulgación de Hash IPMI (Moderada)

Descripción:	Corporación HMENTOR ha desplegado un host remoto que soporta IPMI v2.0. El protocolo (IPMI) se ve afectado por una vulnerabilidad de divulgación de información debido al soporte de la autenticación RMCP+ Authenticated Key-Exchange Protocol (RAKP). Un atacante remoto puede obtener información de hash de contraseña para cuentas de usuario válidas.
Riesgo:	<p>Probabilidad: Alta - Los escaneos básicos de red identificarán esta vulnerabilidad.</p> <p>Impacto: Moderado - Si se explota, un atacante puede obtener acceso a dispositivos de gestión sensibles. Hacker Mentor encontró contraseñas en texto claro.</p>
Sistema:	192.168.190.x
Herramientas utilizadas:	Metasploit
Referencias:	https://blog.rapid7.com/2013/07/02/a-penetration-testers-guide-to-ipmi/

Evidencia

```
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run
[+] 192.168.190.623 - IPMI - Hash found: ADI...
[+] 192.168.190.623 - IPMI - Hash for user 'ADMIN' matches password 'ADMIN'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figura 15: Divulgación de hash IPMI

Remediación

No hay parche para esta vulnerabilidad; es un problema inherente a la especificación para IPMI v2.0. Las mitigaciones sugeridas incluyen:

- Deshabilitar IPMI sobre LAN si no es necesario.
- Utilizar contraseñas seguras para limitar el éxito de los ataques de diccionario fuera de línea.
- Utilizar listas de control de acceso (ACL) o redes aisladas para limitar el acceso a las interfaces de gestión IPMI.

Hallazgo PPI-017: Complejidad insuficiente de SNMP (Moderada)

Descripción:	Corporación HMENTOR desplegó SNMP con cadenas de comunidad "públicas" por defecto. Esta configuración exponía el acceso de sólo lectura a la base de información de gestión (MIB) del sistema, incluidas las configuraciones de red.
Riesgo:	<p>Probabilidad: Alta - Los escaneos básicos de red identificarán esta vulnerabilidad.</p> <p>Impacto: Moderado - Si se explota, un atacante puede perfilar el dispositivo y centrar los ataques.</p>
Sistema:	Identificados 12 equipos
Herramientas utilizadas:	Nessus, SNMP-Check, Ettercap
Referencias:	NIST SP800-53 r4 AC-17(2) - Remote Access Protection of Confidentiality/Integrity using Encryption

Evidencia

```
[*] System information:
Host IP      : 
Hostname    : dr
Description  : IBM F
Contact     : 
Location    : 
Uptime snmp : 
Uptime system : 50 days, 15:42:33.00
System date : 
```

Figura 16: Divulgación de información a través de cadenas de comunidad SNMP públicas

Remediación

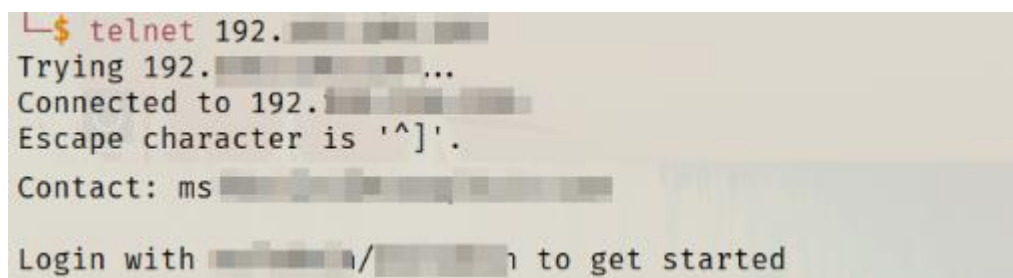
Hacker Mentor recomienda a Corporación HMENTOR considerar las siguientes acciones correctivas:

- Desactivar SNMP si no es necesario
- Filtrar los paquetes UDP que van al puerto UDP - 161
- Evaluar la migración a SNMPv3
- Utilizar directrices de complejidad de contraseña para cadenas de comunidad

Hallazgo PPI-018: Cifrado insuficiente de datos en tránsito: Telnet (Moderada)

Descripción:	Corporación HMENTOR permitía Telnet, el cual no cifra los datos en tránsito. Telnet utiliza autenticación en texto plano y pasa todos los datos (incluidas las contraseñas) en texto claro, por lo que pueden ser interceptados por un atacante.
Riesgo:	<p>Probabilidad: Baja - Un adversario requiere una posición Man-in-the-Middle entre el cliente y el servidor.</p> <p>Impacto: Alto - Si se explota, un adversario puede interceptar credenciales administrativas que pueden utilizarse en otros ataques.</p>
Sistema:	Identificados 9 equipos
Herramientas utilizadas:	Telnet
Referencias:	NIST SP800-53 r4 AC-17(2) - Remote Access Protection of Confidentiality / Integrity Using Encryption

Evidencia



```

L$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Contact: ms
Login with user/Password to get started
  
```

Figura 16: Divulgación de información a través de cadenas de comunidad SNMP públicas

Remediación

Migrar a protocolos protegidos por TLS.

Escaneos e informes adicionales

Hacker Mentor proporciona a sus clientes toda la información recopilada durante las pruebas. Esto incluye archivos Nessus y escaneos completos de vulnerabilidades en formatos detallados. Estos informes contienen escaneos de vulnerabilidades sin procesar y vulnerabilidades adicionales no explotadas por Hacker Mentor.

Los informes identifican problemas de higiene que requieren atención pero que tienen menos probabilidades de conducir a una brecha, es decir, oportunidades de defensa en profundidad. Para obtener más información, consulte los documentos de la carpeta de la unidad compartida titulada "Análisis e informes adicionales".



Última Página