A picture containing text, sign

Description automatically generated

MANIFESTACIÓN CORP

Seguridad Evaluación Recomendaciones Informe

## Negocio Confidencial

*Fecha: Marzo 9º , \_ Proyecto 2021 : DC-001 Versión 1.0*



## Mesa de Contenido

[Mesa de Contenido](#_bookmark0)  [2](#_bookmark0)

[Confidencialidad Declaración](#_bookmark1)  [4](#_bookmark1)

[Descargo de responsabilidad](#_bookmark2)  [4](#_bookmark2)

[Contacto Información](#_bookmark3)  [4](#_bookmark3)

[Evaluación Descripción general](#_bookmark4)  [5](#_bookmark4)

[Evaluación Componentes](#_bookmark5)  [5](#_bookmark5)

[Interno Penetración Prueba](#_bookmark6)  [5](#_bookmark6)

[Hallazgo Gravedad Calificaciones](#_bookmark7)  [6](#_bookmark7)

[Riesgo Factores 6 \_](#_bookmark8)

[Probabilidad](#_bookmark9)  [6](#_bookmark9)

[Impacto](#_bookmark10)  [6](#_bookmark10)

[Alcance](#_bookmark11)  [7](#_bookmark11)

[Alcance Exclusiones](#_bookmark12)  [7](#_bookmark12)

[Cliente Asignaciones](#_bookmark13)  [7](#_bookmark13)

[Ejecutivo Resumen](#_bookmark14)  [8](#_bookmark14)

[Alcance y Tiempo Limitaciones](#_bookmark15)  [8](#_bookmark15)

[Pruebas Resumen](#_bookmark16)  [8](#_bookmark16)

[Ensayador Notas y Recomendaciones](#_bookmark17)  [9](#_bookmark17)

[Llave Fortalezas y Debilidades](#_bookmark18)  [10](#_bookmark18)

[Vulnerabilidad Resumen & Informe Tarjeta](#_bookmark19)  [11](#_bookmark19)

[Interno Penetración Prueba Hallazgos](#_bookmark20)  [11](#_bookmark20)

[Técnico Hallazgos](#_bookmark21)  [13](#_bookmark21)

[Interno Penetración Prueba Hallazgos](#_bookmark22)  [13](#_bookmark22)

[Hallazgo IPT-001: Insuficiente LLMNR Configuración (Crítico)](#_bookmark23)  [13](#_bookmark23)

[Hallazgo IP T-002: Seguridad Mala configuración – Local Administración Contraseña Reutilizar (Crítico)](#_bookmark24)  [14](#_bookmark24)

[Hallazgo IPT-003: Seguridad Mala configuración – WDigest (Crítico)](#_bookmark25)  [15](#_bookmark25)

[Hallazgo IPT-004: Insuficiente Endurecimiento – Simbólico Interpretación (Crítico)](#_bookmark26)  [16](#_bookmark26)

[Hallazgo IPT-005: Insuficiente Contraseña Complejidad (Crítico)](#_bookmark27)  [17](#_bookmark27)

[Hallazgo IPT-006: Seguridad Mala configuración – IPv6 (Crítico)](#_bookmark28)  [18](#_bookmark28)

[Hallazgo \_ IPT-007: Insuficiente Endurecimiento – PYME Firma Desactivado (Crítico)](#_bookmark29)  [19](#_bookmark29)

[Hallazgo IPT-008: Insuficiente Parche Gestión – Software (Crítico)](#_bookmark30)  [20](#_bookmark30)

[Hallazgo IPT-009: Insuficiente Parche Gestión – Operando Sistemas (Crítico)](#_bookmark31)  [21](#_bookmark31)

[Hallazgo IPT-010: Insuficiente Parcheo – MS08-067 - ECLIPSEDWING/NETAPI (Crítico)](#_bookmark32)  [22](#_bookmark32)

[Hallazgo IPT-011: Insuficiente Parcheo – MS12-020 – Remoto Escritorio ICE (Crítico)](#_bookmark33)  [23](#_bookmark33)

[Hallazgo IPT-012: Insuficiente Parcheo – MS17-010 - EternoAzul (Crítico)](#_bookmark34)  [24](#_bookmark34)

[Hallazgo IPT-013: Insuficiente Parcheo – CVE-2019-0708 - azulmantener (Crítico)](#_bookmark35)  [25](#_bookmark35)

[Hallazgo IPT-014: Insuficiente Privilegiado Cuenta Gestión – Kerberoasting (Alto)](#_bookmark36)  [26](#_bookmark36)

[Hallazgo IPT-015: Seguridad Mala configuración – PPG Cartas credenciales (Alto)](#_bookmark37)  [27](#_bookmark37)



[Hallazgo IPT-016: Insuficiente Autenticación - VNC (Alto)](#_bookmark38)  [28](#_bookmark38)

[Hallazgo IPT-017: Por defecto Cartas credenciales en Web Servicios (Alto)](#_bookmark39)  [29](#_bookmark39)

[Hallazgo IPT-018: Insuficiente Endurecimiento – Listable Directorios (Alto)](#_bookmark40)  [30](#_bookmark40)

[Hallazgo IPT-019: No autenticado PYME Compartir Acceso (Moderado)](#_bookmark41)  [31](#_bookmark41)

[Hallazgo IPT-020: Insuficiente Parche Gestión – SMBv1 (Moderado)](#_bookmark42)  [32](#_bookmark42)

[Hallazgo IPT-021: IPMI Picadillo Divulgación (Moderado)](#_bookmark43)  [33](#_bookmark43)

[Hallazgo IPT-022: Insuficiente SNMP Comunidad Cadena Complejidad (Moderado)](#_bookmark44)  [34](#_bookmark44)

[Hallazgo IPT-023: Insuficiente Datos en Tránsito Cifrado - Telnet (Moderado)](#_bookmark45)  [35](#_bookmark45)

[Hallazgo IPT-024: Insuficiente Terminal Servicios Configuración (Moderado)](#_bookmark46)  [36](#_bookmark46)

[Hallazgo IPT-025: Pasos a Dominio Administración (Informativo)](#_bookmark47)  [37](#_bookmark47)

[Adicional Escaneos e Informes](#_bookmark48)  [37](#_bookmark48)

# Declaración de confidencialidad

Este documento es propiedad exclusiva de Demo Corp y TCM Security (TCMS). Este documento contiene información patentada y confidencial. La duplicación, redistribución o uso, total o parcial, en cualquier forma, requiere el consentimiento tanto de Demo Corp como de TCMS.

Manifestación corporación puede compartir este documento con auditores bajo no divulgación acuerdos a demostrar el cumplimiento de los requisitos de la prueba de penetración.

# Descargo de responsabilidad

Una prueba de penetración se considera una instantánea en el tiempo. Los hallazgos y recomendaciones reflejan la información. reunido durante el evaluación y no cualquier cambios o modificaciones hecho afuera de ese periodo.

Los compromisos de tiempo limitado no permiten una evaluación completa de todos los controles de seguridad. TCMS dio prioridad a la evaluación para identificar los controles de seguridad más débiles que un atacante podría explotar. TCMS recomienda conductible similar evaluaciones en un anual base por interno o tercero evaluadores para garantizar el éxito continuo de los controles.

# Información del contacto

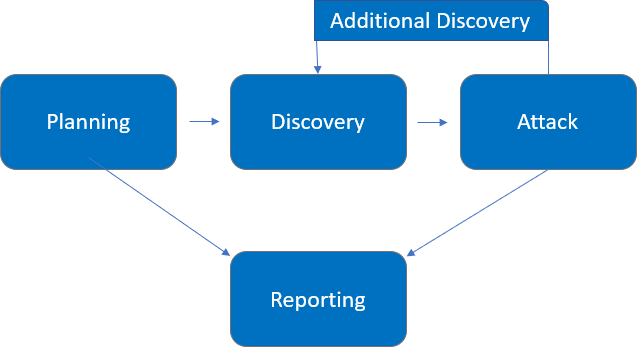
|  |  |  |
| --- | --- | --- |
| **Nombre** | **Título** | **Contacto Información** |
| Manifestación corporación | | |
| John Smith | Global Información Gerente de seguridad | Correo electrónico: [jsmith@democorp.com](mailto:jsmith@democorp.com) |
| medicina tradicional china Seguridad | | |
| Brezo adams | Dirigir Penetración Ensayador | Correo electrónico: [heath@tcm-sec.com \_](mailto:heath@tcm-sec.com) |

# Descripción general de la evaluación

Del 22 de febrero de 2021 al 5 de marzo de 2021, Demo Corp contrató a TCMS para evaluar la postura de seguridad de su infraestructura en comparación con las mejores prácticas actuales de la industria que incluían una red interna. penetración prueba. Todo pruebas realizado es basado en el NIST *SP 800-115 Técnico Guía a Pruebas y evaluaciones de seguridad de la información, Guía de pruebas OWASP (v4) y marcos de pruebas personalizados* .

Etapas de penetración pruebas actividades incluir el siguiente:

* Planificación – Cliente objetivos son reunido y normas de compromiso obtenido.
* Descubrimiento – Llevar a cabo exploración y enumeración a identificar potencial vulnerabilidades, áreas débiles y hazañas.
* Ataque – Confirmar potencial vulnerabilidades a través de explotación y llevar a cabo descubrimiento adicional tras un nuevo acceso.
* Informes – Documento todo encontró vulnerabilidades y hazañas, fallido intentos, y fortalezas y debilidades de la empresa.



# Componentes de la evaluación

### Interno Penetración Prueba

Una prueba de penetración interna emula el papel de un atacante desde dentro de la red. Un ingeniero escaneará la red para identificar posibles vulnerabilidades del host y realizará ataques de red internos comunes y avanzados, como: envenenamiento LLMNR/NBT-NS y otros ataques de intermediario, suplantación de tokens, kerberoasting , pass-the-hash. , billete dorado y más. El ingeniero buscará obtener acceso a los hosts mediante movimientos laterales, comprometer las cuentas de usuario y administrador del dominio y filtrar datos confidenciales.

# Hallazgo Gravedad Calificaciones

El siguiente mesa define niveles de gravedad y correspondiente cvss puntaje rango eso son utilizado a lo largo del documento para evaluar la vulnerabilidad y el impacto del riesgo.

|  |  |  |
| --- | --- | --- |
| **Gravedad** | **cvss V3**  **Puntaje Rango** | **Definición** |
| Crítico | 9,0-10,0 \_ | Explotación es directo y generalmente resultados en compromiso a nivel del sistema. Se recomienda elaborar un plan de acción y parchear inmediatamente. |
| Alto | 7,0-8,9 \_ | La explotación es más difícil pero podría causa elevado privilegios y potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda elaborar un plan de acción y parchear lo antes posible. |
| Moderado | 4,0-6,9 \_ | Vulnerabilidades existir pero son no explotable o requerir extra pasos como la ingeniería social. Se recomienda elaborar un plan de acción y parchear una vez que se hayan resuelto los problemas de alta prioridad. |
| Bajo | 0,1-3,9 \_ | Vulnerabilidades son no explotable pero haría reducir un superficie de ataque de la organización. Se recomienda elaborar un plan de acción y parchear durante la próxima ventana de mantenimiento. |
| Informativo | N / A | No vulnerabilidad existe. Adicional información es proporcionó con respecto a elementos observados durante las pruebas, controles estrictos y documentación adicional. |

# Riesgo Factores

Riesgo es Medido por dos factores: Probabilidad y Impacto:

### Probabilidad

Probabilidad medidas el potencial de a vulnerabilidad ser explotado. Calificaciones son dado basado en la dificultad del ataque, las herramientas disponibles, el nivel de habilidad del atacante y el entorno del cliente.

### Impacto

Impacto medidas el potencial vulnerabilidad efecto en operaciones, incluido confidencialidad, integridad y disponibilidad de los sistemas y/o datos del cliente, daño a la reputación y pérdida financiera.

# Alcance

|  |  |
| --- | --- |
| **Evaluación** | **Detalles** |
| Interno Penetración Prueba | 10.xxx/8 |

### Alcance Exclusiones

Por cliente pedido, TCMS hizo no llevar a cabo cualquier de el siguiente ataques durante pruebas:

* Negación de Servicio (DoS)
* Phishing/redes sociales Ingeniería

Todo otro ataques no especificado arriba eran permitido por Manifestación Corp.

### Cliente Asignaciones

Manifestación corporación proporcionó TCMS el siguiente asignaciones:

* Interno acceso a red a través de buzón y derechos portuarios

# Ejecutivo Resumen

TCMS evaluó la postura de seguridad interna de Demo Corp mediante pruebas de penetración del 22 de febrero . 2021 a Marzo 5to , \_ 2021. El siguiente secciones proporcionar a nivel alto descripción general de vulnerabilidades descubiertas, intentos exitosos y fallidos, y fortalezas y debilidades.

### Alcance y Tiempo Limitaciones

El alcance durante el compromiso no permitió la denegación de servicio ni la ingeniería social en todos los componentes de la prueba.

Tiempo limitaciones eran en lugar para pruebas. Interno red penetración pruebas era permitido para diez

1. negocio días.

### Pruebas Resumen

El red evaluación evaluado Manifestación Cuerpo interno red seguridad postura. De un perspectiva interna, el TCMS equipo realizado vulnerabilidad exploración contra todo IP proporcionó por Manifestación Corp para evaluar el estado general de los parches de la red. El equipo también realizó ataques comunes basados en Active Directory, como el envenenamiento por resolución de nombres de multidifusión local de enlace (LLMNR), retransmisión SMB, retransmisión de intermediario IPv6 y Kerberoasting . Más allá del escaneo de vulnerabilidades y los ataques a Active Directory, el TCMS evaluó otros riesgos potenciales, como archivos compartidos abiertos, credenciales predeterminadas en servidores/dispositivos y divulgación de información confidencial para obtener una imagen completa de la situación de seguridad de la red.

El equipo de TCMS descubrió que LLMNR estaba habilitado en la red (Encontrando IPT-001), lo que permitía la interceptación de hashes de usuario mediante envenenamiento de LLMNR. Estos hash fueron desconectados y agrietado a través de diccionario ataques, cual señales a débil contraseña política (Hallazgo IPT-005). Utilizando el agrietado contraseñas, el TCMS equipo ganado acceso a varios máquinas dentro el red, lo que indica cuentas de usuario demasiado permisivas.

Con acceso a la máquina y el uso de sistemas operativos más antiguos en la red (Finding IPT-009), el equipo pudo aprovechar WDigest (Finding IPT-003) para recuperar credenciales de texto sin cifrar en las cuentas. El equipo también pudo volcar hashes de cuentas locales en cada máquina a la que se accedió. El equipo de TCMS descubrió eso el local cuenta hashes eran ser reutilizado al otro lado de dispositivos (Hallazgo IPT-002), lo que conduce a un acceso adicional a la máquina a través de ataques pass-the-hash.

Por último, el TCMS equipo era capaz a aprovechar cuentas capturado a través de WDigest y picadillo volcados a mover lateralmente a lo largo de el red hasta aterrizaje en a máquina eso tenía a Dominio Credencial de administrador en texto sin formato vía WDigest . El equipo de pruebas pudo utilizar esta credencial para iniciar sesión en el controlador de dominio y comprometer todo el dominio. Para obtener un tutorial completo de la ruta hacia el administrador de dominio, consulte Búsqueda de IPT-025.

En suma a el compromiso listado arriba, el TCMS equipo encontró eso usuarios podría ser suplantados a través de ataques de delegación (Encontrando IPT-004), los ataques de retransmisión SMB fueron posibles debido a que la firma SMB estaba deshabilitada (Encontrando IPT-007) y el tráfico IPv6 no estaba restringido, lo que podría llevar a la retransmisión LDAPS y al compromiso del dominio (Encontrando IPT-006 ).

El resto de los hallazgos críticos se relacionan con la administración de parches, ya que los dispositivos con software crítico desactualizado (Finding IPT-008), sistemas operativos (Finding IPT-009) y vulnerabilidades de Microsoft RCE (Finding IPT-010, IPT-011, IPT -012, IPT-013), se encontraron presentes dentro de la red.

El resto de el recomendaciones eran alto, moderado, bajo, o informativo. Para más información sobre los hallazgos, revise los [Hallazgos técnicos](#_bookmark21) sección.

### Ensayador Notas y Recomendaciones

Los resultados de las pruebas de la red Demo Corp son indicativos de que una organización se está sometiendo a su primera prueba de penetración, como es el caso aquí. Muchos de los hallazgos descubiertos son vulnerabilidades dentro de Active Directory que vienen habilitadas de forma predeterminada, como LLMNR, IPv6 y Kerberoasting .

Durante las pruebas, se destacaron dos constantes: una política de contraseñas débil y parches débiles. La contraseña débil política condujo a el inicial compromiso de cuentas y es generalmente uno de el primero puntos de apoyo un atacante intenta utilizar en una red. La presencia de una política de contraseñas débiles está respaldada por la evidencia de que nuestro equipo de pruebas descifró más de 2200 contraseñas de cuentas de usuario, incluida la mayoría de las cuentas de administrador de dominio, mediante ataques de diccionario básicos.

Nosotros recomendado eso Manifestación corporación reevalúa su actual contraseña política y considera a política de 15 caracteres o más para su regular usuario cuentas y 30 caracteres o más para su Administrador de dominio cuentas. Nosotros también recomendar eso Manifestación corporación explorar contraseña lista negra y proporcionará una lista de contraseñas de usuario descifradas para que el equipo las evalúe. Por último, se debe considerar una solución de gestión de acceso a privilegios.

Los parches débiles y los sistemas operativos obsoletos llevaron al compromiso de docenas de máquinas dentro del red. Nosotros creer el número de comprometida máquinas haría tener estado significativamente más grande, sin embargo, los equipos de TCMS y Demo Corp acordaron que no era necesario intentar explotar ninguna vulnerabilidad basada en la ejecución remota de código (RCE), como MS17-010 (Finding IPT-012), ya que el controlador de dominio ya había sido comprometido y el Los equipos no querían correr el riesgo de que se les negara el servicio debido a ataques fallidos.

Recomendamos que el equipo de Demo Corp revise las recomendaciones de parches hechas en la sección Hallazgos técnicos del informe junto con los escaneos de Nessus proporcionados para obtener una descripción completa de los elementos que se deben parchear. También recomendamos que Demo Corp mejore sus políticas y procedimientos de administración de parches para ayudar a prevenir posibles ataques dentro de su red.

En a positivo nota, nuestro pruebas equipo motivado varios alertas durante el compromiso. El Manifestación Seguridad Corporativa Operaciones equipo descubierto nuestro vulnerabilidad exploración y era alertado cuando nosotros intentó utilizar ataques ruidosos en una máquina comprometida. Si bien no todos los ataques se descubrieron durante las pruebas, estas alertas son un comienzo positivo. Se ha proporcionado orientación adicional sobre alertas y detección de hallazgos, cuando sea necesario, en la sección Hallazgos técnicos.

En general, la red Demo Corp funcionó como se esperaba para una prueba de penetración por primera vez. Recomendamos que el equipo de Demo Corp revise minuciosamente las recomendaciones hechas en este informe, corrija los hallazgos y vuelva a realizar pruebas anualmente para mejorar su postura general de seguridad interna.

### Llave Fortalezas y Debilidades

El siguiente identifica el llave fortalezas identificado durante el evaluación:

* 1. Observado alguno exploración de común enumeración herramientas (Neso)
  2. Mimikatz detectado en alguno máquinas
  3. Servicio cuentas eran no correr como dominio administradores
  4. Manifestación corporación local administrador cuenta contraseña era único a cada dispositivo A continuación se identifican las debilidades clave identificadas durante la evaluación:

1. Contraseña política encontró a ser insuficiente
2. críticamente fuera de plazo operando sistemas y débil parchear existir dentro el red
3. Contraseñas eran observado en Borrar texto pendiente a WDigest
4. LLMNR es activado dentro el red
5. PYME firma es desactivado en todo no servidor dispositivos en la obra
6. IPv6 es incorrectamente administrado dentro el red
7. Usuario cuentas poder ser suplantado a través de simbólico delegación
8. Local administración cuentas tenía contraseña reutilizar y eran demasiado permisivo
9. Por defecto cartas credenciales eran descubierto en crítico infraestructura, semejante como iDRAC
10. No autenticado compartir acceso era permitido
11. Usuario cuentas eran encontró a ser correr como servicio cuentas
12. Servicio cuentas utilizado débil contraseñas
13. Dominio administrador utilizado débil contraseñas

# Vulnerabilidad Resumen & Informe Tarjeta

El siguiente mesas ilustrar el vulnerabilidades encontró por impacto y recomendado remediaciones:

### Interno Penetración Prueba Recomendaciones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 13 | 5 | 6 | 0 | 1 |
| Crítico | Alto | Moderado | Bajo | Informativo |

|  |  |  |
| --- | --- | --- |
| **Hallazgo** | **Gravedad** | **Recomendación** |
| Interno Penetración Prueba | | |
| IPT-001: Insuficiente Configuración LLMNR | Crítico | Desactivar multidifusión nombre resolución a través de GPO. |
| IPT-002: Seguridad Mala configuración – Reutilización de contraseña de administrador local | Crítico | Utilizar único local contraseñas de administrador  y límite local administración usuarios a través de privilegios mínimos . |
| IPT-003: Seguridad Mala configuración – Wdigest | Crítico | Desactivar WDigest a través de GPO. |
| IPT-004: Insuficiente Endurecimiento – Suplantación de tokens | Crítico | Restringir simbólico delegación. |
| IPT-005: Insuficiente Complejidad de la contraseña | Crítico | Implementar CEI Punto de referencia Requisitos de contraseña/solución PAM. |
| IPT-006: Seguridad Mala configuración – IPv6 | Crítico | Restringir DHCPv6 tráfico y anuncios de enrutadores entrantes en el Firewall de Windows a través de GPO. |
| IPT-007: Insuficiente Endurecimiento – Firma SMB deshabilitada | Crítico | Permitir PYME firma en todo Manifestación Computadoras de dominio Corp. |
| IPT-008: Insuficiente Gestión de parches – Software | Crítico | Actualizar a el el último software versión. |
| IPT-009: Gestión de parches insuficiente – Operando Sistemas | Crítico | Actualizar Operando Sistemas a la última versión. |
| IPT-010: Parches insuficientes – MS08-067 - ECLIPSEDWING/NETAPI | Crítico | Aplicar el adecuado parches de microsoft a remediar el asunto. |
| IPT-011: Insuficiente Parcheo –  MS12-020 – Remoto RCE de escritorio | Crítico | Aplicar el adecuado microsoft  parches a remediar el asunto. |
| IPT-012: Insuficiente Parcheo – MS17-010 - Azul Eterno | Crítico | Aplicar el adecuado parches de microsoft a remediar el asunto. |
| IPT-013: Insuficiente Parcheo – CVE-2019-0708- BlueKeep | Crítico | Aplicar el adecuado parches de microsoft a remediar el asunto. |

|  |  |  |
| --- | --- | --- |
| **Hallazgo** | **Gravedad** | **Recomendación** |
| IPT-014: Insuficiente Gestión de cuentas privilegiadas –  Kerberoasting | Alto | Utilice cuentas de servicio administradas por grupo (GMSA) para privilegiado  servicios. |
| IPT-015: Seguridad Mala configuración – Credenciales GPP | Alto | Aplicar proveedor parcheo. Hacer no Utilice contraseñas GPP . |
| IPT-016: Insuficiente Autenticación -VNC \_ | Alto | Permitir autenticación en el Servidor VNC . |
| IPT-017: Por defecto Cartas credenciales en Servicios web | Alto | Cambiar por defecto cartas credenciales o deshabilitar cuentas no utilizadas. |
| IPT-018: Insuficiente Endurecimiento – Directorios enumerables | Alto | Restringir acceso y conducta web evaluación de la aplicación . |
| IPT-019: No autenticado PYME Compartir acceso | Moderado | Desactivar PYME compartir o requieren autenticación. |
| IPT-020: Insuficiente Gestión de parches – SMBv1 | Moderado | Mejora a SMBv3 y aplicar últimos parches. |
| IPT-021: IPMI Picadillo Divulgación | Moderado | Desactivar IPMI encima LAN si él es innecesario . |
| IPT-022: Comunidad SNMP insuficiente Cadena Complejidad | Moderado | Desactivado SNMP si no requerido. |
| IPT-023: Insuficiente Datos en Cifrado de tránsito: Telnet | Moderado | Emigrar a TLS protegido protocolos. |
| IPT-024: Insuficiente Configuración de servicios de terminal | Moderado | Permitir Red Nivel Autenticación (NLA) en el servidor RDP remoto. |
| IPT-025: Pasos a Dominio Administración | Informativo | Revisar acción y remediación pasos. |

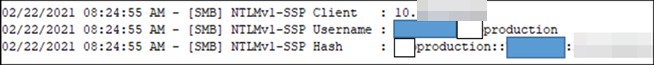
# Hallazgos técnicos

### Interno Penetración Prueba Recomendaciones

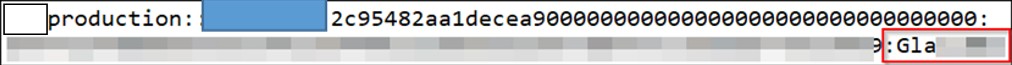
Hallazgo IPT-001: Insuficiente LLMNR Configuración (Crítico)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación permite multidifusión nombre resolución en su usuario final redes. TCMS capturó 20 hashes de cuentas de usuario envenenando el tráfico de LLMNR y descifró 2 con software de descifrado básico.  El agrietado cuentas eran usado a aprovechar más acceso eso condujo a el compromiso del Controlador de Dominio. |
| Riesgo: | Probabilidad: Alto – Este ataque es eficaz en entornos permitiendo resolución de nombres de multidifusión.  Impacto: Muy Alto – LLMNR envenenamiento permisos atacantes a captura hashes de contraseñas para descifrar fuera de línea o transmitir en tiempo real y pivotar lateralmente en el entorno. |
| Sistema: | Todo |
| Herramientas Usado: | Respondedor, Hashcat |
| Referencias: | [Popa Seguridad](https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning) - Local Red Ataques: LLMNR y NBT-NS Envenenamiento NIST SP800-53 r4 IA-3 - Identificación y autenticación del dispositivo [NIST SP800-53 r4 CM-6(1)](https://nvd.nist.gov/800-53/Rev4/control/CM-6#enhancement-1) - Ajustes de configuración |

Evidencia



*Cifra 1: capturado picadillo de "producción"*



Remediación

*Cifra 2: Agrietado picadillo de "producción"*

Desactivar multidifusión nombre resolución a través de GPO. Para lleno mitigación y detección guía, consulte la guía MITRE [aquí .](https://attack.mitre.org/techniques/T1557/001/)

Los hashes descifrados demuestran una política de complejidad de contraseñas deficiente. Si la resolución de nombre de multidifusión es requerido, Red Acceso Control (NAC) conjunto con solicitud lista blanca puede limitar estos ataques.

Hallazgo IPT-002: Seguridad Mala configuración – Local Administración Contraseña Reutilización (crítica)

|  |  |
| --- | --- |
| Descripción: | TCMS utilizó administrador local hashes para obtener acceso a otras máquinas en el red a través de a 'pasar el hash' ataque. El local administrador hashes se obtuvieron a través del acceso a la máquina proporcionado por la cuenta pirateada en IPT-001.  Los ataques Pass-the-hash no requieren conocer la contraseña de la cuenta para iniciar sesión correctamente en una máquina. Por lo tanto, reutilizar la misma contraseña de administrador local (y por lo tanto el mismo picadillo) en múltiple máquinas voluntad permiso sistema acceso a esos ordenadores.  TCMS apalancado este ataque a ganar acceso a ~50 máquinas dentro el principal  oficina. Este condujo a más cuenta acceso y el eventual compromiso de el controlador de dominio. |
| Riesgo: | Probabilidad: Alto – Este ataque es eficaz en grande redes con local Reutilización de contraseña de administrador.  Impacto: Muy Alto – pasar el hash permisos un agresor a mover lateralmente y verticalmente en toda la red. |
| Sistema: | Todo |
| Herramientas Usado: | paquete , Crackmapexec |
| Referencias: | <https://capec.mitre.org/data/definitions/644.html>  [https://tcm-sec.com/pentest-tales-001-you-spent-ho wmuch-on-security/](https://tcm-sec.com/pentest-tales-001-you-spent-how-much-on-security/) |

Evidencia



*Cifra 3: Local administración picadillo usado a ganar acceso a máquina*

Remediación

Utilice contraseñas de administrador locales únicas. Limite los usuarios administradores locales mediante privilegios mínimos. Considere implementar a PAM solución. Para lleno mitigación y detección guía, por favor referencia la guía MITRE [aquí .](https://attack.mitre.org/techniques/T1550/002/)

Hallazgo IPT-003: Seguridad Mala configuración – WDigest (Crítico)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación permitido fuera de plazo operando sistemas dentro su red, incluidos Windows 7, 8, Server 2008 y Server 2012.  Estos operando sistemas, por por defecto, permiso WDigest , cual historias todo Las contraseñas del usuario que ha iniciado sesión actualmente en texto sin cifrar.  TCMS aprovechó el acceso a la máquina obtenido en IPT-001 e IPT-002 para moverse lateralmente a lo largo de el red hasta descubriendo a máquina con Dominio Administración  cartas credenciales almacenado en WDigest . |
| Riesgo: | Probabilidad: Moderado – Este ataque es eficaz en redes con más viejo sistemas operativos .  Impacto: Muy Alto – WDigests cartas credenciales son almacenado en claro texto, cual puede permitir el robo de cuentas confidenciales, como las de administradores de dominio. |
| Sistema: | Todo sistemas más viejo que ventanas 10 y Servidor 2016 |
| Herramientas Usado: | metasploit, kiwi |
| Referencias: | [https://stealthbits.com/blog/wdigest-clear-text-passwords-stealing-more-than-](https://stealthbits.com/blog/wdigest-clear-text-passwords-stealing-more-than-a-hash/) [a-hash/](https://stealthbits.com/blog/wdigest-clear-text-passwords-stealing-more-than-a-hash/) |

Evidencia



*Cifra 4: Borrar texto contraseñas de Dominio Administradores*

Remediación

Desactivar WDigest a través de GPO. Para lleno mitigación y detección guía, por favor referencia la orientación [aquí .](https://www.csoonline.com/article/3438824/how-to-detect-and-halt-credential-theft-via-windows-wdigest.html)

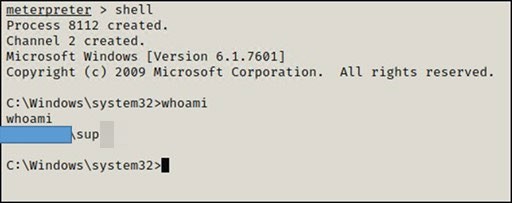
Hallazgo IPT-004: Insuficiente Endurecimiento – Simbólico Interpretación (Crítico)

|  |  |
| --- | --- |
| Descripción: | TCMS suplantado el simbólico de “ supcb ” a obtener Dominio Privilegios de administrador . |
| Riesgo: | Probabilidad: Alto – El penetración ensayador visto y suplantado fichas con el uso de herramientas de código abierto.  Impacto: Muy Alto - Si explotado, un agresor ganancias dominio administrador acceso. |
| Sistema: | Todo |
| Herramientas Usado: | metasploit, Incógnito |
| Referencias: | [NIST SP800-53 r4 CM-7 -](https://nvd.nist.gov/800-53/Rev4/control/CM-7) El menos Funcionalidad [NIST SP800-53 r4 AC-6 -](https://nvd.nist.gov/800-53/Rev4/search/results?controlDesc=Least%2BPrivilege) Privilegios mínimos  [https://docs.microsoft.com/en-us/windows-server/identity/ad-](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts) [ds/manage/cómo-configurar- cuentas-protegidas](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts) |

Evidencia



*Cifra 5: Interpretación de "sorber"*



Remediación

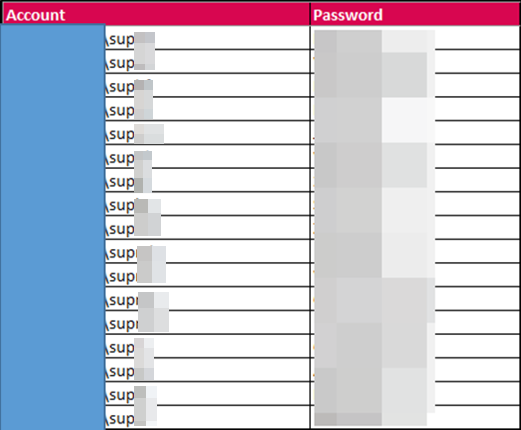
*Cifra 6: Caparazón acceso como Dominio Administración "sorber"*

Restringir simbólico delegación. Para lleno mitigación y detección guía, por favor referencia el Guía MITRE [aquí .](https://attack.mitre.org/techniques/T1134/003/)

Hallazgo IPT-005: Insuficiente Contraseña Complejidad (Crítico)

|  |  |
| --- | --- |
| Descripción: | TCMS objeto de dumping hashes de el dominio controlador y procedió a intentar ataques comunes de adivinación de contraseñas contra todos los usuarios.  TCMS agrietado 2,226 contraseñas usando básico contraseña lista adivinación ataques y bajo esfuerzo bruto forzando ataques. 17 agrietado cuentas tenía dominio derechos de administrador . |
| Riesgo: | Probabilidad: alta: las contraseñas simples son susceptibles a ataques de descifrado de contraseñas. Cifrado proporciona alguno proteccion, pero diccionario ataques base en listas de palabras comunes a menudo descifran contraseñas débiles.  Impacto: Muy Alto - Dominio administración cuentas con débil contraseñas podría dirigir a un adversario que impacta críticamente la capacidad de operación de Demo Corp. |
| Sistema: | Todo |
| Herramientas Usado: | Manual Revisar |
| Referencias: | [NIST SP800-53 IA-5(1) -](https://nvd.nist.gov/800-53/Rev4/control/IA-5#enhancement-1) Gestión de autenticadores [https://www.cisecurity.org/white-papers /cis-password-policy-guide/](https://www.cisecurity.org/white-papers/cis-password-policy-guide/) |

Evidencia



Remediación

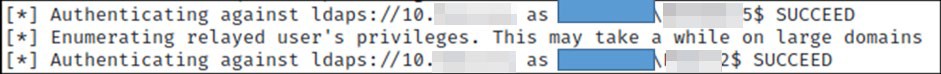
*Cifra 7: Extracto de agrietado dominio hashes*

Implementar CEI Punto de referencia contraseña requisitos / PAM solución. TCMS recomienda eso Demo Corp aplica las mejores prácticas de la industria en torno a la complejidad y la gestión de contraseñas. También se recomienda un filtro de contraseña para evitar que los usuarios utilicen contraseñas comunes y fáciles de adivinar. Además, TCMS recomienda que Demo Corp aplique requisitos de contraseña más estrictos para el administrador de dominio y otras cuentas confidenciales.

Hallazgo IPT-006: Seguridad Mala configuración – IPv6 (Crítico)

|  |  |
| --- | --- |
| Descripción: | A través de IPv6 DNS envenenamiento, el TCMS equipo era capaz a exitosamente transmitir credenciales al controlador de dominio de Demo Corp. |
| Riesgo: | Probabilidad: Alto – IPv6 es activado por por defecto en ventanas redes. El Las herramientas y técnicas necesarias para realizar esta tarea son triviales.  Impacto: Muy Alto - Si explotado, un agresor poder ganar dominio acceso de administrador . |
| Sistema: | Todo |
| Herramientas Usado: | Mitm6, Paquete |
| Referencias: | [https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-](https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/) [ipv6/](https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/) |

Evidencia



Remediación

*Cifra 8: Exitosamente retransmitido LDAP cartas credenciales a través de mitm6*

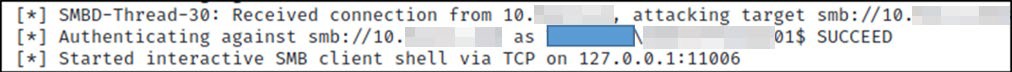
1. El envenenamiento de IPv6 abusa del hecho de que Windows solicita una dirección IPv6 incluso en entornos que solo utilizan IPv4. Si no utiliza IPv6 internamente, la forma más segura de evitar mitm6 es bloquear el tráfico DHCPv6 y los anuncios entrantes del enrutador en el Firewall de Windows a través de la Política de grupo. Deshabilitar IPv6 enteramente puede tener no deseado lado efectos. Configuración el siguiente predefinido Las reglas para bloquear en lugar de permitir evitan que el ataque funcione:
   1. (Entrante) Centro Redes - Dinámica Anfitrión Configuración Protocolo para IPv6 (DHCPV6- entrada)
   2. (Entrante) Centro Redes - Enrutador Anuncio (ICMPv6- En)
   3. (Saliente) Centro Redes - Dinámica Anfitrión Configuración Protocolo para IPv6 (DHCPV6- salida)
2. Si WPAD es no en usar internamente, desactivar él a través de Grupo Política y por deshabilitar el servicio WinHttpAutoProxySvc .
3. retransmisión a LDAP y LDAPS poder solo ser mitigado por habilitando ambos LDAP firma y Enlace de canal LDAP.

Considerar Administrativo usuarios a el Protegido Usuarios grupo o calificación a ellos como Cuenta es sensible y no se puede delegar, lo que evitará cualquier suplantación de ese usuario mediante delegación.

Hallazgo IPT-007: Insuficiente Endurecimiento – PYME Firma Desactivado (Crítico)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación fallido a implementar PYME firma en múltiple dispositivos. El La ausencia de firma de SMB podría provocar ataques de retransmisión de SMB, generando shells a nivel de sistema sin requerir una contraseña de usuario. |
| Riesgo: | Probabilidad: Alto – retransmisión contraseña hashes es a básico técnica no que requiere craqueo fuera de línea.  Impacto: Alto – Si explotado, un adversario ganancias código ejecución, principal a movimiento lateral a través de la red. |
| Sistema: | Identificado 709 máquinas, por favor ver el abajo archivo para listado.  [archivo remoto] |
| Herramientas Usado: | Neso, mapa n, multirelé , Respondedor |
| Referencias: | [CIS Microsoft Windows Server 2012 R2 v2.2.0](https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0.pdf) (Página 180) <https://github.com/lgandx/Responder/blob/master/tools/MultiRelay.py> |

Evidencia



Remediación

*Cifra 9: Exitoso PYME relé*

Habilite la firma SMB en todas las computadoras del dominio Demo Corp. Alternativamente, como la firma SMB puede causar problemas de rendimiento, deshabilitar la autenticación NTLM, aplicar la clasificación de cuentas y limitar el administrador local. usuarios poder efectivamente ayuda mitigar ataques. Para lleno mitigación y detección guía, consulte la guía MITRE [aquí .](https://attack.mitre.org/techniques/T1557/001/)

Hallazgo IPT-008: Insuficiente Parche Gestión – Software (Crítico)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación permitido varios obsoleto software en su red. Esto incluye:   * apache versión < 2.4.46 * apache Gato versión < 7.0.100, 8.5.51, 9.0.31 * Cisoco AireOS versión 8.5.151.10 * Medidor de código versión 3.05 (5.21.1478.500) * Dropbear SSH Servidor versión 2015.68 * Dell iDRAC7 versión 2.63.60.62.01 * Dell iDRAC8 versión 2.63.60.61.06 * Dell iDRAC9 versión 3.36.36.36.21 * ESXi versión 5.5 * ESXi versión 6.5 construir 15256549 * Flexera Flexnet Editor versión 11.16.0 * IIS versión 7.5 * ISC UNIR versión 9.6.2- P2 * microsoft DNS Servidor versión 6.1.7601.24261 * microsoft SQL Servidor versión 11.0.6594.0 * netatalk Sesión abierta versión < 3.1.12 * PHP versión < 7.3.11 * rockwell Automatización RSLinx Clásico   Arriba liza todo crítico y altamente calificado obsoleto software, el mayoría de que permiten vulnerabilidades graves, como la ejecución remota de código. por un completo  parchear lista, por favor revisar el proporcionó Neso escanear documentación. |
| Riesgo: | Probabilidad: Alto – Un agresor poder descubrir estos vulnerabilidades con herramientas básicas .  Impacto: Muy Alto – Si explotado, un agresor podría posiblemente ganar lleno Ejecución remota de código o denegación de servicio a un sistema. |
| Herramientas Usado: | Neso |
| Referencias: | [NIST SP800-53 r4 MA-6](https://nvd.nist.gov/800-53/Rev4/control/MA-6) – Oportuno Mantenimiento [NIST SP800-53 r4 SI-2](https://nvd.nist.gov/800-53/Rev4/control/SI-2) – Reparación de fallas |

Remediación

Actualizar a el el último software versión. Para a lleno lista de vulnerable sistemas, versiones, y requisitos de parcheo, consulte el siguiente documento.

[archivo remoto]

Hallazgo IPT-009: Insuficiente Parche Gestión – Operando Sistemas (Crítico)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación permitido varios obsoleto software en su red. Esto incluye:   * ventanas Servidor 2003 (fin de vida en Julio 14, 2015) * ventanas Servidor 2008 R2 (fin de vida en Enero 14, 2020) * ventanas experiencia (fin de vida en Abril 8, 2014) * ventanas 7 (fin de vida en Enero 14, 2020) * ubuntu 11 (fin de vida en Puede 9, 2013) * FreeBSD 11.0 (fin de vida en octubre de 2016)   Fin de vida sistemas son susceptible a a multitud de vulnerabilidades. TCMS no intentó ningún ataque contra estos servidores debido al riesgo de denegación de servicio, que está fuera de alcance. |
| Riesgo: | Probabilidad: Alto – Un agresor poder descubrir estos vulnerabilidades con herramientas básicas .  Impacto: Alto – Si explotado, un agresor podría posiblemente ganar lleno remoto Ejecución de código o denegación de servicio a un sistema. |
| Sistema: | Identificado 139 máquinas, por favor ver el abajo archivo para listado.  [archivo remoto] |
| Herramientas Usado: | Neso |
| Referencias: | [NIST SP800-53 r4 MA-6](https://nvd.nist.gov/800-53/Rev4/control/MA-6) – Oportuno Mantenimiento [NIST SP800-53 r4 SI-2](https://nvd.nist.gov/800-53/Rev4/control/SI-2) – Reparación de fallas |

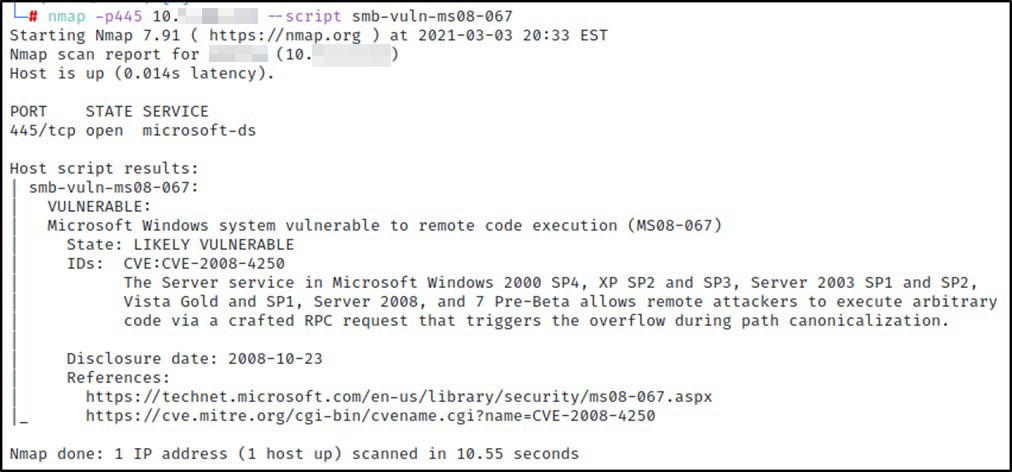
Remediación

Actualizar Operando Sistemas a el ultima versión.

Hallazgo IPT-010: Insuficiente Parcheo – MS08-067 - ECLIPSEDWING/NETAPI (Crítico)

|  |  |
| --- | --- |
| Descripción: | Demo Corp permitió un sistema sin parches en la red interna que es vulnerable a MS08-067. medicina tradicional china Seguridad confirmado eso el vulnerabilidad probablemente exista, pero no intentó explotarlo para evitar cualquier denegación de servicio. |
| Riesgo: | Probabilidad: Alto – Consideró uno de el mayoría explotado vulnerabilidades en Microsoft Windows, ya que se envía de forma nativa con Windows XP.  Impacto: Muy Alto – Si explotado, un agresor ganancias código ejecución como el sistema  usuario. Un adversario voluntad requerir adicional técnicas a obtener acceso de administrador de dominio. |
| Sistema: | 10.xxx |
| Herramientas Usado: | Neso, Nmapa |
| Referencias: | [NIST SP800-53 r4 MA-6](https://nvd.nist.gov/800-53/Rev4/control/MA-6) – Oportuno Mantenimiento [NIST SP800-53 r4 SI-2](https://nvd.nist.gov/800-53/Rev4/control/SI-2) – Reparación de fallas |

Evidencia



Remediación

*Cifra 10: Sin parchear MS08-067 \_*

Aplicar el adecuado microsoft parches a remediar el asunto. Más información en El parche MS08-067 se puede encontrar aquí: [https://docs.microsoft.com/en-us/security-](https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067) [actualizaciones/ Boletines de seguridad /2008/ms08-067](https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067)

Hallazgo IPT-011: Insuficiente Parcheo – MS12-020 – Remoto Escritorio ICE (Crítico)

|  |  |
| --- | --- |
| Descripción: | Demo Corp permitió un sistema sin parches en la red interna que es vulnerable a MS12-020. medicina tradicional china Seguridad confirmado eso el vulnerabilidad probablemente exista, pero no intentó explotarlo para evitar cualquier denegación de servicio. |
| Riesgo: | Probabilidad: Alto – El vulnerabilidad es fácilmente descubrible y explotable con herramientas de código abierto.  Impacto: Muy Alto – Si explotado, un agresor ganancias código ejecución como el sistema  usuario. Un adversario voluntad requerir adicional técnicas a obtener acceso de administrador de dominio. |
| Sistema: | 10.xxx |
| Herramientas Usado: | Neso, Nmapa |
| Referencias: | [NIST SP800-53 r4 MA-6](https://nvd.nist.gov/800-53/Rev4/control/MA-6) – Oportuno Mantenimiento [NIST SP800-53 r4 SI-2](https://nvd.nist.gov/800-53/Rev4/control/SI-2) – Reparación de fallas |

Evidencia



Remediación

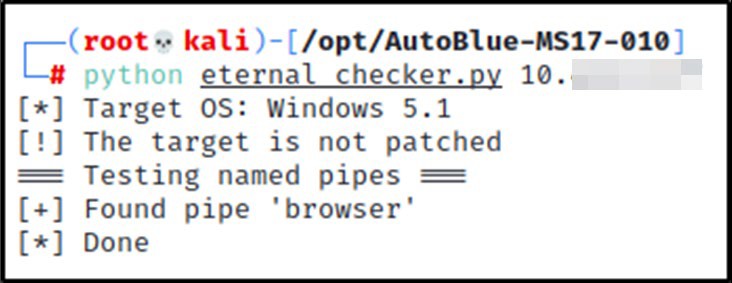
*Cifra 11: Sin parchear MS12-020 \_*

Aplicar el adecuado microsoft parches a remediar el asunto. Más información en El parche MS12-020 se puede encontrar aquí: [https://docs.microsoft.com/en-us/security-](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-020) [actualizaciones/ boletines de seguridad /2012/ms12-020](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-020)

Hallazgo IPT-012: Insuficiente Parcheo – MS17-010 - EternoAzul (Crítico)

|  |  |
| --- | --- |
| Descripción: | Demo Corp permitió varios sistemas sin parches en la red interna que son vulnerables a MS17-010 ( EternalBlue ). TCM Security confirmó que la vulnerabilidad probable existe pero hizo no intentar el explotar a prevenir cualquier negación de servicio. |
| Riesgo: | Probabilidad: Alto – Malicioso actores tener usado PYME explotaciones como EternalBlue en infracciones recientes.  Impacto: Muy Alto – Si explotado, un agresor ganancias código ejecución como el usuario del sistema. Un adversario requerirá técnicas adicionales para obtener el dominio.  administrador acceso. |
| Sistema: | 10.xxx |
| Herramientas Usado: | Neso, metasploit, Autoazul |
| Referencias: | [NIST SP800-53 r4 MA-6](https://nvd.nist.gov/800-53/Rev4/control/MA-6) – Oportuno Mantenimiento [NIST SP800-53 r4 SI-2](https://nvd.nist.gov/800-53/Rev4/control/SI-2) – Reparación de fallas |

Evidencia



Remediación

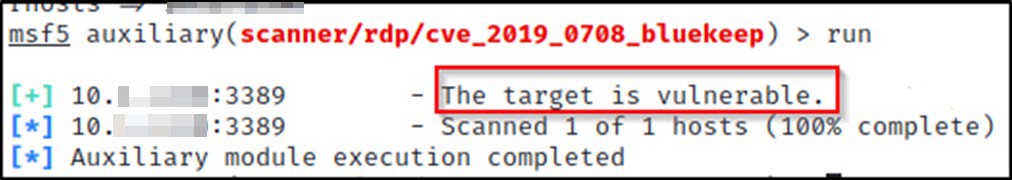
*Cifra 12: Sin parchear MS17-010 \_*

Aplicar el adecuado microsoft parches a remediar el asunto. Más información en El parche MS17-010 se puede encontrar aquí: [https://docs.microsoft.com/en-us/security-](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010) [actualizaciones/ boletines de seguridad /2017/ms17-010](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010)

Hallazgo IPT-013: Insuficiente Parcheo – CVE-2019-0708 - azulmantener (Crítico)

|  |  |
| --- | --- |
| Descripción: | Demo Corp permitió varios sistemas sin parches en la red interna que están vulnerable a CVE-2019-0708 ( Manténgase Azul ). medicina tradicional china Seguridad confirmado eso la vulnerabilidad probable existe pero hizo no intentar el explotar a prevenir cualquier negación de servicio. |
| Riesgo: | Probabilidad: Alto – El vulnerabilidad es fácilmente descubrible y explotable con herramientas de código abierto.  Impacto: Muy Alto – Si explotado, un agresor ganancias código ejecución como el usuario del sistema. Un adversario requerirá técnicas adicionales para obtener el dominio.  administrador acceso. |
| Sistema: | 10.xxx |
| Herramientas Usado: | Neso, Nmapa |
| Referencias: | [NIST SP800-53 r4 MA-6](https://nvd.nist.gov/800-53/Rev4/control/MA-6) – Oportuno Mantenimiento [NIST SP800-53 r4 SI-2](https://nvd.nist.gov/800-53/Rev4/control/SI-2) – Reparación de fallas |

Evidencia



Remediación

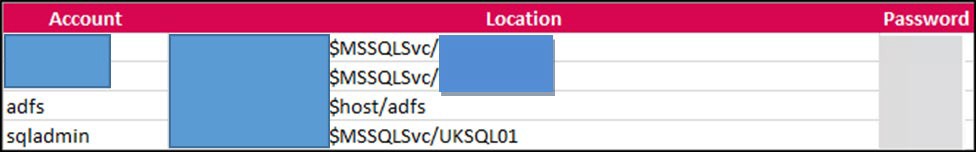
*Cifra 13: Sin parchear CVE- 2019-0708*

Aplicar el adecuado microsoft parches a remediar el asunto. Más información en parchear CVE [-](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) 2019-0708 se puede encontrar aquí: [https://support.microsoft.com/en-us/topic/customer-guidance-for-](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) [cve-2019-0708-servicios-de-escritorio- remoto-vulnerabilidad-de-ejecución-de-código-remoto-14-mayo-2019-](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) [0624e35b-5f5d-6da7-632c-27066a79262e](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 IPT-014: Insuficiente Privilegiado Cuenta Gestión – Kerberoasting (Alto)

|  |  |
| --- | --- |
| Descripción: | TCMS recuperó todos los nombres principales de servicio de usuario (SPN) del controlador de dominio de Demo Corp utilizando una cuenta de nivel de usuario de dominio (IPT-001) en un Kerberoasting ataque. Recuperando estos usuario SPN permitido TCMS a grieta 4 contraseñas de cuenta.  No servicio cuentas eran observado correr como dominio administradores. Se observó que las cuentas de usuario se ejecutaban como un servicio, lo cual no es una buena práctica. |
| Riesgo: | Probabilidad: Alto – Cualquier cuenta unido a el dominio poder pedido usuario SPN.  Impacto: Alto – Usando SPN, él es posible a recuperar sensible cuenta hashes de contraseñas y descifrarlos sin conexión. |
| Herramientas Usado: | paquete , Hashcat |
| Referencias: | Kerberoasting detalles: <https://adsecurity.org/?p=2293> [Descripción general de las cuentas de servicio administradas por grupos](https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview) |

Evidencia



Remediación

*Cifra 14: Agrietado servicio cuentas*

Usar Grupo Administrado Servicio Cuentas (GMSA) para privilegiado servicios. GMSA cuentas poder ser Se utiliza para garantizar que las contraseñas sean largas, complejas y cambien con frecuencia. Cuando GMSA no sea aplicable, proteja las cuentas utilizando una solución de almacenamiento de contraseñas.

TCMS recomienda configurar el registro de alertas en los controladores de dominio para el ID de evento de Windows 4769 siempre que solicite un ticket de servicio Kerberos. Estas alertas son propensas a altas tasas de falsos positivos, pero son a suplementario detective control. Sastre a seguridad información y evento gestión herramienta (SIEM) para alertar sobre solicitudes excesivas de SPN de los usuarios.

Hallazgo IPT-015: Seguridad Mala configuración – PPG Cartas credenciales (Alto)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación utilizado “ ccontraseñas ” en Grupo Política Preferencia (PPB) cual cualquier usuario de dominio puede realizar consultas desde la carpeta SYSVOL de un controlador de dominio. Microsoft publicó la clave para descifrar estas contraseñas. |
| Riesgo: | Probabilidad: Alto – Cualquier autenticado usuario poder obtener este información y descifre la contraseña con herramientas de código abierto .  Impacto: Alto – Un adversario poder usar estos cartas credenciales a mover lateralmente dentro de la red. |
| Herramientas Usado: | metasploit |
| Referencias: | [NIST SP800-53 IA-5(1) -](https://nvd.nist.gov/800-53/Rev4/control/IA-5#enhancement-1) Autenticador Gestión |

Evidencia



Remediación

*Cifra 15: objeto de dumping PPG cartas credenciales*

Aplicar parches de proveedores. No utilice contraseñas GPP . Además, habilitar la autenticación en NFS compartir voluntad proteger el confidencialidad de el almacenado información. Exportador autenticación registros a una solución SIEM brindará a los equipos de respuesta a incidentes información sobre los intentos de inicio de sesión por fuerza bruta.

Hallazgo IPT-016: Insuficiente Autenticación - VNC (alto)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación desplegada 3 servidores eso permitido no autenticado acceso a través de Servidor VNC . |
| Riesgo: | Probabilidad: Alto – Descubriendo no autenticado VNC servidores es trivial y se puede hacer con herramientas de código abierto.  Impacto: Alto – Atacantes poder control industrial dispositivos, destruir datos, o apagar los sistemas. |
| Sistema: | 10.xxx, 10.xxx, 10.xxx |
| Herramientas Usado: | Neso, VNC Espectador |
| Referencias: | [NIST SP800-53 IA-5(1) -](https://nvd.nist.gov/800-53/Rev4/control/IA-5#enhancement-1) Autenticador Gestión |

Evidencia

Remediación

[imagen redactada]

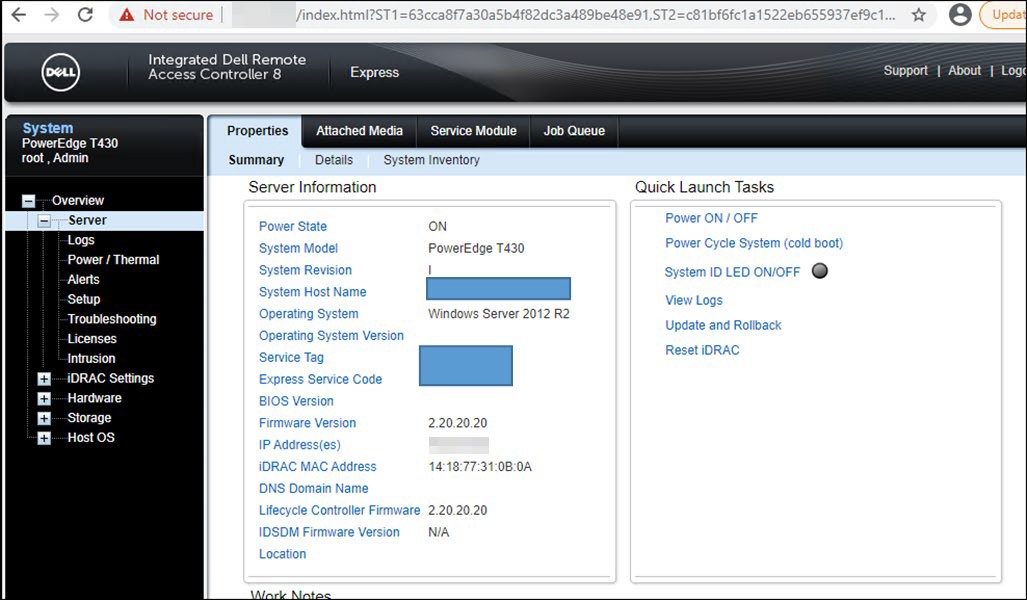
*Cifra dieciséis: Acceso a sistema a través de VNC*

Permitir autenticación en el VNC Servidor.

Hallazgo IPT-017: Por defecto Cartas credenciales en Web Servicios (Alto)

|  |  |
| --- | --- |
| Descripción: | TCMS validado por defecto cartas credenciales trabajó en múltiple web aplicaciones dentro del entorno de Demo Corp. |
| Riesgo: | Probabilidad: Alto – Cartas credenciales son publicado para estos dispositivos y un Primer intento de autenticación del atacante.  Impacto: Alto – Atacantes poder control dispositivos, destruir datos, o cerrar sistemas caídos . |
| Sistema: | Por defecto cartas credenciales eran probado en a muestra colocar de web aplicaciones, pero sugiere verificar las siguientes direcciones como mínimo:  [archivo remoto] |
| Herramientas Usado: | Manual Revisar |
| Referencias: | [NIST SP800-53 IA-5(1) -](https://nvd.nist.gov/800-53/Rev4/control/IA-5#enhancement-1) Autenticador Gestión |

Evidencia



Remediación

*Cifra 17: Dell iDRAC acceso a través de por defecto cartas credenciales*

Cambiar por defecto cartas credenciales o desactivar no usado cuentas.

Hallazgo IPT-018: Insuficiente Endurecimiento – Listable Directorios (Alto)

|  |  |
| --- | --- |
| Descripción: | Demo Corp reveló información al permitir directorios enumerables y almacenar potencialmente crítico elementos en web servidor. Él es fuertemente recomendado eso Demo Corp realiza una evaluación exhaustiva de la aplicación web en este recurso. |
| Riesgo: | Probabilidad: Moderado – Adversarios voluntad descubrimiento contenido con abierto fuente herramientas.  Impacto: Alto – Atacantes usar este información en conjunción con otro ataques para enumeración y catalogación para ataques rápidos cuando surgen vulnerabilidades. |
| Sistema: | Lleno lista de descubierto listable directorios:  [archivo remoto] |
| Herramientas Usado: | Manual Revisar |
| Referencias: | [NIST SP800-53r4 CM-7 -](https://nvd.nist.gov/800-53/Rev4/control/CM-7) El menos Funcionalidad  [NIST SP800-53r4 AC-6(3) -](https://nvd.nist.gov/800-53/Rev4/control/AC-6#enhancement-3) El menos Privilegio |

Evidencia



Remediación

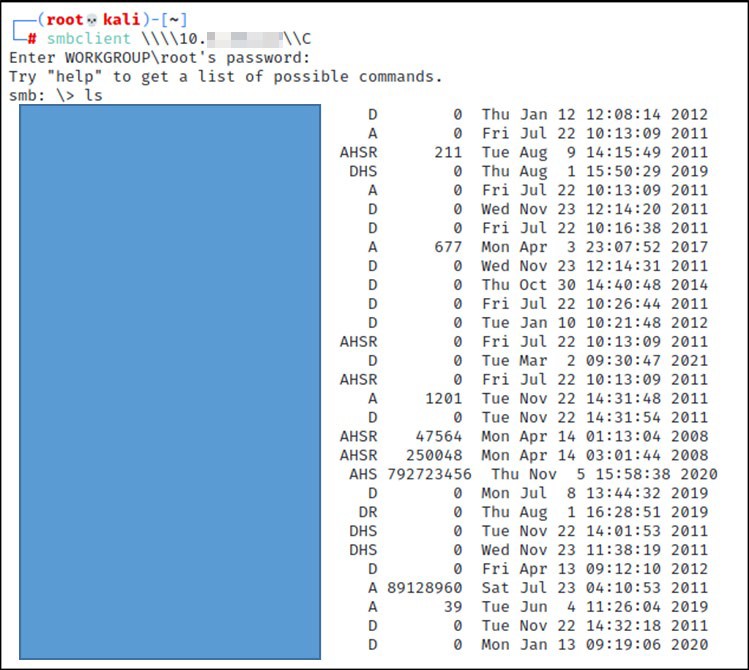
*Cifra 18: Listable directorio*

Restringir acceso y conducta web aplicación evaluación.

Hallazgo IPT-019: No autenticado PYME Compartir Acceso (Moderado)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación expuesto múltiple servidores con no autenticado archivo servidor acceso. |
| Riesgo: | Probabilidad: Moderado – Adversarios voluntad descubrir estos Comparte con Técnicas de reconocimiento básicas y silenciosas.  Impacto: Moderado – Atacantes aprender acerca de el ambiente a través de fugas de información . |
| Sistema: | 10.xxx |
| Herramientas Usado: | Neso, cliente smb |
| Referencias: | [NIST SP800-53r4 AC-6(3) -](https://nvd.nist.gov/800-53/Rev4/control/AC-6#enhancement-3) El menos Privilegio  [NIST SP800-53 r4 SC-4](https://nvd.nist.gov/800-53/Rev4/control/SC-4) - Información en Compartido Recursos |

Evidencia



*Cifra 19: No autenticado Compartir acceso*

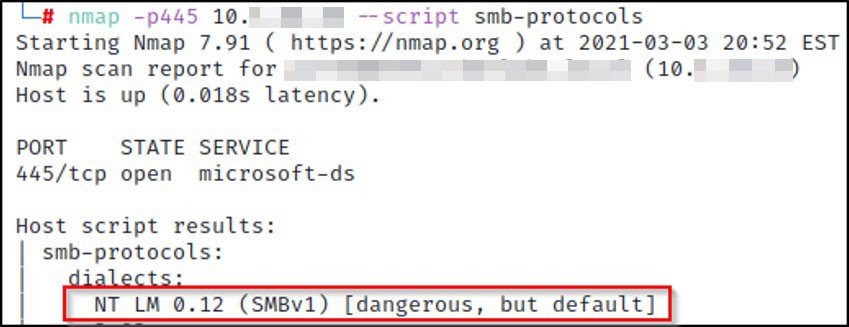
Remediación

Desactivar PYME compartir o requerir autenticación. Habilitando autenticación en el compartir voluntad proteger la confidencialidad de la información almacenada. Exportar registros de autenticación a una solución SIEM brindará a los equipos de respuesta a incidentes información sobre los intentos de inicio de sesión por fuerza bruta.

Hallazgo IPT-020: Insuficiente Parche Gestión – SMBv1 (Moderado)

|  |  |
| --- | --- |
| Descripción: | Demo Corp no pudo parchear SMBv1. Esta versión es vulnerable a múltiples ataques de denegación de servicio y ejecución remota de código. TCM Security confirmó que la vulnerabilidad probablemente existe pero lo hizo no intentar el explotar a prevenir cualquier negación de servicio. |
| Riesgo: | Probabilidad: Moderado – Básico exploraciones haría identificar el PYME versión pero requeriría que un adversario estuviera en la red interna e identificara un exploit.  Impacto: Moderado – Si explotado, un agresor ganancias negación de servicio y capacidad de ejecución de código. |
| Sistema: | 10.xxx |
| Herramientas Usado: | Neso, Nmapa |
| Referencias: | [https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ \_](https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/)  [NIST SP800-53 r4 SI-2 -](https://nvd.nist.gov/800-53/Rev4/control/SI-2) Defecto Remediación |

Evidencia



*Cifra 20: No autenticado Compartir acceso*

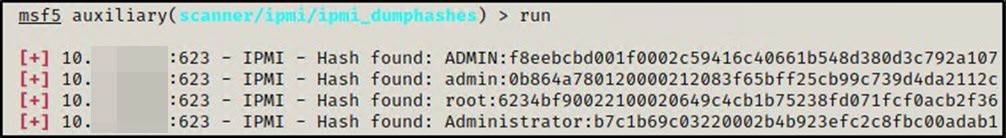
Remediación

Mejora a SMBv3 y aplicar el último parcheo.

Hallazgo IPT-021: IPMI Picadillo Divulgación (Moderado)

|  |  |
| --- | --- |
| Descripción: | Demo Corp implementó un host remoto compatible con IPMI v2.0. El protocolo (IPMI) se ve afectado por un información divulgación vulnerabilidad pendiente a el apoyo de Autenticación RMCP+ Protocolo de intercambio de claves autenticado (RAKP). Un atacante remoto  poder obtener contraseña picadillo información para válido usuario cuentas a través de el HMAC de una respuesta al mensaje 2 RAKP de un BMC. |
| Riesgo: | Probabilidad: Alto – Básico red exploraciones voluntad identificar este vulnerabilidad.  Impacto: Moderado – Si explotado, un agresor poder ganar acceso a dispositivos de gestión sensibles. TCMS no pudo descifrar ningún hash durante el  evaluación. |
| Sistema: | Identificado 34 máquinas, por favor ver el abajo archivo para listado.  [archivo remoto] |
| Herramientas Usado: | metasploit |
| Referencias: | <https://blog.rapid7.com/2013/07/02/a-penetration-testers-guide-to-ipmi/> |

Evidencia



*Cifra 21: IPMI Picadillo Divulgación*

Remediación

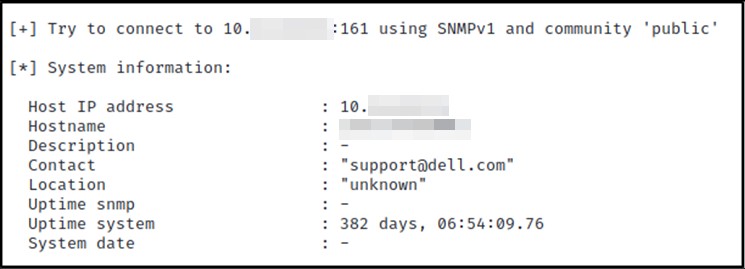
Allá es No parche para este vulnerabilidad; él es un inherente problema con el especificación para IPMI v2.0. Las mitigaciones sugeridas incluyen:

* Deshabilitar IPMI encima LAN si él es no necesario.
* Usando fuerte contraseñas a límite el éxito de desconectado diccionario ataques.
* Usando Acceso Control Liza (ACL) o aislado redes a límite acceso a su Interfaces de gestión IPMI.

Hallazgo IPT-022: Insuficiente SNMP Comunidad Cadena Complejidad (Moderado)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación desplegada SNMP con por defecto "público" comunidad instrumentos de cuerda. Esta configuración expuso acceso de solo lectura a la base de información de administración (MIB) del sistema, incluidas las configuraciones de red. |
| Riesgo: | Probabilidad: Alto – Básico red exploraciones voluntad identificar este vulnerabilidad.  Impacto: Moderado – Si explotado, un agresor poder perfil el dispositivo y ataques de enfoque . |
| Sistema: | Identificado 45 máquinas, por favor ver el abajo archivo para listado.  [archivo remoto] |
| Herramientas Usado: | Neso, verificación SNMP, Ettercap |
| Referencias: | [NIST SP800-53 r4 AC-17(2)](https://nvd.nist.gov/800-53/Rev4/control/AC-17?baseline=moderate&enhancement-2) - Remoto Acceso Proteccion de confidencialidad/integridad mediante cifrado |

Evidencia



*Cifra 22: Información divulgación a través de público SNMP comunidad instrumentos de cuerda*



*Cifra 23: No público SNMP cadena capturado a través de Ettercap*

Remediación

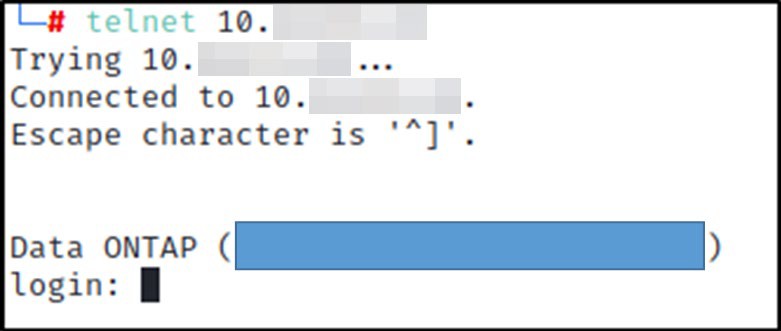
medicina tradicional china Seguridad recomienda Manifestación corporación considerar el siguiente correctivo comportamiento:

* Desactivado SNMP si no requerido
* Filtrar UDP paquetes yendo a puerto UDP – 161
* Evaluar migración a SNMPv3
* Usar contraseña complejidad pautas para comunidad instrumentos de cuerda

Hallazgo IPT-023: Insuficiente Datos en Tránsito Cifrado - Telnet (Moderado)

|  |  |
| --- | --- |
| Descripción: | Manifestación corporación permitido Telnet cual hace no cifrar datos en tránsito. Telnet usa simple texto autenticación y pasa todo datos (incluido contraseñas) en claro texto y puede ser interceptado por un atacante. |
| Riesgo: | Probabilidad: Bajo – Un adversario requiere a Hombre en el medio posición entre el cliente y el servidor.  Impacto: Alto – Si explotado un adversario puede interceptar Credenciales administrativas que pueden usarse en otros ataques. |
| Sistema: | Identificado 53 máquinas, por favor ver el abajo archivo para listado.  [archivo remoto] |
| Herramientas Usado: | Telnet |
| Referencias: | [NIST SP800-53 r4 AC-17(2) -](https://nvd.nist.gov/800-53/Rev4/control/AC-17#enhancement-2) Remoto Acceso |Protección de Confidencialidad / Integridad mediante cifrado |

Evidencia



*Cifra 24: Telnet acceso inmediato*

Remediación

Emigrar a TLS protegido protocolos.

Hallazgo IPT-024: Insuficiente Terminal Servicios Configuración (Moderado)

|  |  |
| --- | --- |
| Descripción: | Los Servicios de Terminal Server remotos no están configurados para utilizar la autenticación a nivel de red (ALN) solo. NLA usos el Credencial Seguridad Apoyo Protocolo de proveedor ( CredSSP ) para realizar una autenticación sólida del servidor a través de mecanismos TLS/SSL o Kerberos, que protegen contra ataques de intermediario. Además de mejorar la autenticación, NLA también ayuda a proteger la  remoto computadora de malicioso usuarios y software por completando autenticación de usuario antes de que se establezca una conexión RDP completa. |
| Riesgo: | Probabilidad: Bajo – Un agresor poder descubrir estos vulnerabilidades con básico herramientas.  Impacto: Alto – Si explotado, un adversario ganancias código ejecución, principal a movimiento lateral a través de la red. |
| Sistema: | Identificado 118 máquinas, por favor ver el abajo archivo para listado.  [archivo remoto] |
| Herramientas Usado: | Neso |
| Referencias: | [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v%3Dws.11)) [2008-R2-y-2008/cc732713(v=ws.11)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v%3Dws.11)) |

Remediación

Permitir Red Nivel Autenticación (ALN) en el remoto PDR servidor. Este es generalmente hecho en la pestaña 'Remoto' de la configuración 'Sistema' en Windows.

Hallazgo IPT-025: Pasos a Dominio Administración (Informativo)

El pasos abajo describir cómo el penetración ensayador obtenido dominio administrador acceso. Cada paso también proporciona recomendaciones de solución para ayudar a mitigar el riesgo.

|  |  |  |
| --- | --- | --- |
| Paso | Acción | Remediación |
| 1 | envenenado LLMNR respuestas a obtener Hash NetNTLMv2 de un usuario habitual de la red | Desactivar multidifusión nombre Resolución vía GPO. |
| 2 | Hash NTLM crackeado fuera de línea del administrador de dominio usuarios 'producción' y '[nombre eliminado]' | Aumentar contraseña complejidad. Utilice múltiples  factor. Implementar una cuenta privilegiada Gestión solución. Utilice un filtro de contraseña. |
| 3 | apalancado contraseña de 'producción' cuenta a obtener acceso a varias máquinas dentro de la red | Límite local administrador privilegios y hacer cumplir el privilegio mínimo. |
| 4 | objeto de dumping hashes en accedido máquinas a encuentre la contraseña en texto claro de la cuenta 'Bartender' a través de  resumen | Desactivar WDigest a través de GPO. |
| 5 | Demasiado permisivo 'Barman' cuenta acceso permitido a a grande cantidad de máquinas dentro el  red | Límite local administrador privilegios y hacer cumplir el privilegio mínimo. |
| 6 | Hashes volcados en las máquinas a las que se accede para encontrar texto sin cifrar contraseña de Dominio Administrador cuenta | Desactivar WDigest a través de GPO. |
| 7 | Utilizado descubierto cartas credenciales a registro en el controlador de dominio. |  |

Remediación

Revisar acción y remediación pasos.

### Adicional Escaneos y Informes

TCMS proporciona a todos los clientes toda la información del informe recopilada durante las pruebas. Esto incluye archivos Nessus y análisis completos de vulnerabilidades en formatos detallados. Estos informes contienen análisis de vulnerabilidades sin procesar y vulnerabilidades adicionales que TCM Security no explota.

Los informes identifican problemas de higiene que requieren atención, pero es menos probable que conduzcan a una infracción, es decir, defensa en profundidad. oportunidades. Para más información, por favor ver el documentos en su carpeta de la unidad compartida denominada "Análisis e informes adicionales".



Último Página