

Empresa de demostración

Informe de resultados de la evaluación de seguridad

Confidencial comercial

Fecha: 28 de mayo de 2019

Proyecto: 897-19

Versión 1.0

# Tabla de contenido

[Tabla de contenidos](#_Toc9866461)  [2](#_Toc9866461)

[Declaración de confidencialidad](#_Toc9866462)  [3](#_Toc9866462)

[Descargo de responsabilidad](#_Toc9866463)  [3](#_Toc9866463)

[Información de contacto](#_Toc9866464)  [3](#_Toc9866464)

[Descripción general de la evaluación](#_Toc9866465)  [4](#_Toc9866465)

[Componentes de evaluación](#_Toc9866466)  [4](#_Toc9866466)

[Prueba de penetración externa](#_Toc9866467)  [4](#_Toc9866467)

[Encontrar clasificaciones de gravedad](#_Toc9866468)  [5](#_Toc9866468)

[Alcance](#_Toc9866469)  [6](#_Toc9866469)

[Exclusiones de alcance](#_Toc9866470)  [6](#_Toc9866470)

[Asignaciones para clientes](#_Toc9866471)  [6](#_Toc9866471)

[Resumen ejecutivo](#_Toc9866472)  [7](#_Toc9866472)

[Resumen del ataque](#_Toc9866473)  [7](#_Toc9866473)

[Fortalezas de seguridad](#_Toc9866474)  [8](#_Toc9866474)

[Alertas SIEM de escaneos de vulnerabilidad](#_Toc9866475)  [8](#_Toc9866475)

[Debilidades de seguridad](#_Toc9866476)  [8](#_Toc9866476)

[Autenticación multifactor faltante](#_Toc9866477)  [8](#_Toc9866477)

[Política de contraseñas débiles](#_Toc9866478)  [8](#_Toc9866478)

[Intentos de inicio de sesión sin restricciones](#_Toc9866479)  [8](#_Toc9866479)

[Vulnerabilidades por Impacto](#_Toc9866480)  [9](#_Toc9866480)

[Hallazgos de la prueba de penetración externa](#_Toc9866481)  [10](#_Toc9866481)

[Política de bloqueo insuficiente: Outlook Web App (crítico)](#_Toc9866482)  [10](#_Toc9866482)

[Informes y escaneos adicionales (informativos)](#_Toc9866483)  [13](#_Toc9866483)

# Declaración de confidencialidad

Este documento es propiedad exclusiva de Demo Company (DC) 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 DC como de TCMS.

TCMS puede compartir este documento con auditores en virtud de acuerdos de confidencialidad para demostrar el cumplimiento de los requisitos de las pruebas de penetración.

# Descargo de responsabilidad

Una prueba de penetración se considera una instantánea en el tiempo. Los hallazgos y recomendaciones reflejan la información recopilada durante la evaluación y no ningún cambio o modificación realizada fuera de ese período.

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 realizar evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito continuo de los controles.

# Información del contacto

|  |  |
| --- | --- |
|  |  |

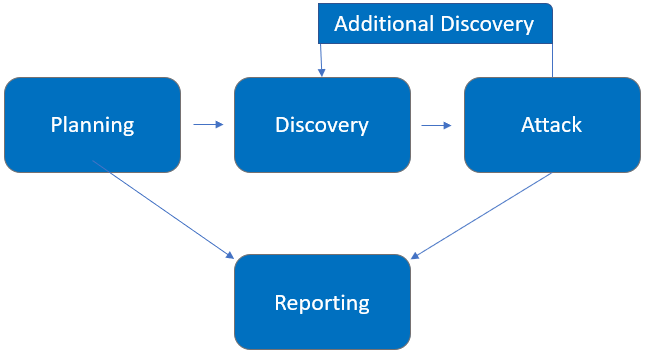
|  |  |  |
| --- | --- | --- |
| Nombre | Título | Información del contacto |
| **Empresa de demostración** | | |
| John Smith | Vicepresidente de Seguridad de la Información (CISO) | Oficina: (555) 555-5555  Correo electrónico: [john.smith@demo.com](mailto:john.smith@demo.com) |
| Jim Smith | Gerente de TI | Oficina: (555) 555-5555  Correo electrónico: [jim.smith@demo.com](mailto:jim.smith@demo.com) |
| Joe Smith | Ingeniero de redes | Oficina: (555) 555-5555  Correo electrónico: [joe.smith@demo.com](mailto:joe.smith@demo.com) |
| **Seguridad de la medicina tradicional china** | | |
| Heath Adams | Probador de penetración de plomo | Oficina: (555) 555-5555  Correo electrónico: [hadams@tcm-sec.com](mailto:hadams@tcm-sec.com) |
| Bob Adams | Probador de penetración | Oficina: (555) 555-5555  Correo electrónico: [badams@tcm-sec.com](mailto:badams@tcm-sec.com) |
| Rob Adams | Gerente de cuentas | Oficina: (555) 555-5555  Correo electrónico: [radams@tcm-sec.com](mailto:radams@tcm-sec.com) |

# Descripción general de la evaluación

Del 20 de mayo de 2019 al 29 de mayo de 2019, DC 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 prueba de penetración externa. Todas las pruebas realizadas se basan en la *Guía técnica NIST SP 800-115 para pruebas y evaluaciones de seguridad de la información, la Guía de pruebas OWASP (v4) y marcos de pruebas personalizados* .

Las fases de las actividades de pruebas de penetración incluyen las siguientes:

* Planificación: se recopilan los objetivos del cliente y se obtienen las reglas de compromiso.
* Descubrimiento: realice escaneos y enumeraciones para identificar posibles vulnerabilidades, áreas débiles y exploits.
* Ataque: confirme vulnerabilidades potenciales mediante la explotación y realice descubrimientos adicionales tras un nuevo acceso.
* Informes: documente todas las vulnerabilidades y exploits encontrados, los intentos fallidos y las fortalezas y debilidades de la empresa.



# Componentes de la evaluación

## Prueba de penetración externa

Una prueba de penetración externa emula el papel de un atacante que intenta obtener acceso a una red interna sin recursos internos ni conocimiento interno. Un ingeniero de TCMS intenta recopilar información confidencial a través de inteligencia de código abierto (OSINT), incluida información de los empleados, contraseñas históricas violadas y más que se puede aprovechar contra sistemas externos para obtener acceso a la red interna. El ingeniero también realiza escaneos y enumeraciones para identificar vulnerabilidades potenciales con la esperanza de explotarlas.

# Encontrar clasificaciones de gravedad

La siguiente tabla 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.

| Gravedad | Rango de puntuación CVSS V3 | Definición |
| --- | --- | --- |
| Crítico | 9.0-10.0 | La explotación es sencilla y normalmente resulta en un 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 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. |
| Moderado | 4.0-6.9 | Las vulnerabilidades existen pero no son explotables o requieren pasos adicionales 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 | Las vulnerabilidades no se pueden explotar, pero reducirían la superficie de ataque de una organización. Se recomienda elaborar un plan de acción y parchear durante la próxima ventana de mantenimiento. |
| Informativo | N / A | No existe ninguna vulnerabilidad. Se proporciona información adicional sobre los elementos observados durante las pruebas, controles estrictos y documentación adicional. |

# Alcance

|  |  |
| --- | --- |
| Evaluación | Detalles |
| Prueba de penetración externa | 192.168.0.0/24,  192.168.1.0/24 |

* Información de alcance completo proporcionada en " **Demo Company-867-19 Full Findings.xslx"**

## Exclusiones de alcance

Por solicitud del cliente, TCMS no realizó ningún ataque de denegación de servicio durante las pruebas.

## Asignaciones para clientes

DC no proporcionó ningún subsidio para ayudar con las pruebas.

# Resumen ejecutivo

TCMS evaluó la postura de seguridad externa de DC a través de una prueba de penetración de red externa del 20 de mayo de 2019 al 29 de mayo de 2019. Al aprovechar una serie de ataques, TCMS encontró vulnerabilidades de nivel crítico que permitieron acceso completo a la red interna a la oficina central de DC. Se recomienda encarecidamente que DC aborde estas vulnerabilidades lo antes posible, ya que se encuentran fácilmente mediante un reconocimiento básico y se pueden explotar sin mucho esfuerzo.

## Resumen del ataque

La siguiente tabla describe cómo TCMS obtuvo acceso a la red interna, paso a paso:

|  |  |  |
| --- | --- | --- |
| Paso | Acción | Recomendación |
| 1 | Se obtuvieron credenciales históricas de cuenta violadas para aprovechar todas las páginas de inicio de sesión de la empresa. | Disuadir a los empleados de utilizar correos electrónicos y nombres de usuario del trabajo como credenciales de inicio de sesión para otros servicios a menos que sea necesario. |
| 2 | Intentó un ataque de “relleno de credenciales” contra Outlook Web Access (OWA), que no tuvo éxito. Sin embargo, OWA proporcionó una enumeración de nombres de usuarios, lo que permitió a TCMS recopilar una lista de nombres de usuarios válidos para aprovecharlos en futuros ataques. | Sincronice mensajes de cuentas válidos e inválidos. |
| 3 | Realicé un ataque de “rociación de contraseñas” contra OWA utilizando los nombres de usuario descubiertos en el paso 2. ¡TCMS usó la contraseña de Summer2018! (temporada + año + carácter especial) contra todas las cuentas válidas y obtuvo acceso a la aplicación OWA. | OWA permite autenticar con credenciales válidas. TCMS recomienda que DC implemente la autenticación multifactor (MFA) en todos los servicios externos.  OWA permitió intentos de inicio de sesión ilimitados. TCMS recomienda que DC restrinja los intentos de inicio de sesión en su servicio.  TCMS recomienda una política de contraseñas mejorada de: 1) 14 caracteres o más 2) Utilice contraseñas diferentes para cada cuenta a la que acceda . 3) No utilice palabras ni nombres propios en las contraseñas, independientemente del idioma.  Además, TCMS recomienda que DC:   * Capacite a los empleados sobre cómo crear una contraseña adecuada |
| 4 | Credenciales válidas aprovechadas para iniciar sesión en VPN | OWA permite autenticar con credenciales válidas. TCMS recomienda que DC implemente la autenticación multifactor (MFA) en todos los servicios externos. |

# Fortalezas de seguridad

## Alertas SIEM de escaneos de vulnerabilidades

Durante la evaluación, el equipo de seguridad de DC alertó a los ingenieros de TCMS sobre el escaneo de vulnerabilidades detectadas en sus sistemas. El equipo pudo identificar con éxito la dirección IP del atacante del ingeniero de TCMS a los pocos minutos de escanear y fue capaz de incluir a TCMS en la lista negra para futuras acciones de escaneo.

# Debilidades de seguridad

## Autenticación multifactor faltante

TCMS aprovechó múltiples ataques contra formularios de inicio de sesión de DC utilizando credenciales válidas recopiladas a través de inteligencia de código abierto. Los inicios de sesión exitosos incluyeron cuentas de correo electrónico de los empleados a través de Outlook Web Access y acceso interno a través del inicio de sesión de Active Directory en la VPN. El uso de autenticación multifactor habría impedido el acceso completo y habría requerido que TCMS utilizara métodos de ataque adicionales para obtener acceso a la red interna.

## Política de contraseñas débiles

TCMS realizó con éxito ataques de adivinación de contraseñas contra formularios de inicio de sesión de DC, proporcionando acceso a la red interna. ¡Un formato de contraseña predecible de Summer2018! (temporada + año + personaje especial) se intentó y tuvo éxito.

## Intentos de inicio de sesión sin restricciones

Durante la evaluación, TCMS realizó múltiples ataques de fuerza bruta contra formularios de inicio de sesión encontrados en la red externa. Para todos los inicios de sesión, se permitieron intentos ilimitados, lo que permitió un inicio de sesión exitoso en la aplicación Outlook Web Access.

# Vulnerabilidades por impacto

El siguiente cuadro ilustra las vulnerabilidades encontradas por impacto:

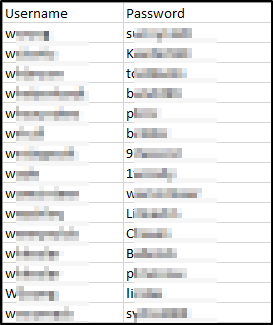
## Hallazgos de la prueba de penetración externa

Política de bloqueo insuficiente: aplicación web de Outlook (crítica)

|  |  |
| --- | --- |
| Descripción: | DC permitió intentos de inicio de sesión ilimitados en sus servicios Outlook Web App (OWA). Esta configuración permitió ataques de fuerza bruta y de adivinación de contraseñas en los que TCMS solía obtener acceso a la red interna de DC. |
| Impacto: | Crítico |
| Sistema: | 192.168.0.5 |
| Referencias: | [NIST SP800-53r4 AC-17](https://nvd.nist.gov/800-53/Rev4/control/AC-17) - Acceso remoto  [NIST SP800-53r4 AC-7(1)](https://nvd.nist.gov/800-53/Rev4/control/AC-7#enhancement-1) - Intentos de inicio de sesión fallidos | Bloqueo automático de cuenta |

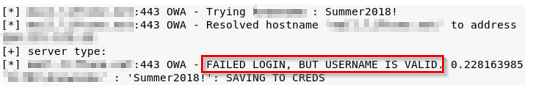
**Prueba de concepto de explotación**

TCMS recopiló datos históricos violados encontrados en volcados de credenciales. Los datos ascendieron a 868 credenciales de cuenta en total ( **Nota:** puede encontrar una lista completa de cuentas comprometidas en " **Demo Company-867-19 Full Findings.xslx"** .).



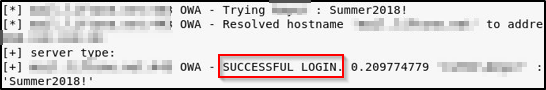
*Figura 1 : Lista de muestra de credenciales de usuario violadas*

TCMS utilizó las credenciales recopiladas para realizar un ataque de relleno de credenciales contra la página de inicio de sesión de OWA. Los ataques de relleno de credenciales toman credenciales previamente conocidas e intentan utilizarlas en formularios de inicio de sesión para obtener acceso a los recursos de la empresa. TCMS no tuvo éxito en el ataque, pero pudo recopilar información confidencial adicional del servidor OWA en forma de enumeración de nombres de usuarios.



*Figura 2 : Enumeración del nombre de usuario de OWA*

TCMS recopiló los nombres de usuario válidos y realizó un ataque de pulverización de contraseñas. Un ataque de pulverización de contraseñas intenta utilizar contraseñas comunes contra nombres de usuarios conocidos con la esperanza de obtener acceso a los recursos de la empresa. ¡TCMS intentó utilizar el Summer2018 común! (temporada + año + carácter especial) contra todos los nombres de usuario válidos conocidos. Un nombre de usuario devuelto como un inicio de sesión exitoso:



*Figura 3 : Inicio de sesión exitoso en OWA*

TCMS aprovechó las credenciales válidas para iniciar sesión en el portal VPN del cliente y obtener acceso a la red interna.

**Remediación**

|  |  |
| --- | --- |
| OMS: | Equipo de TI |
| Vector: | Remoto |
| Acción: | Elemento 1: El inicio de sesión de VPN y OWA con credenciales válidas no requería autenticación multifactor (MFA). TCMS recomienda que DC implemente y aplique MFA en todos los servicios de inicio de sesión externos.  Punto 2: OWA permitió intentos de inicio de sesión ilimitados. TCMS recomienda que DC restrinja los intentos de inicio de sesión en su servicio.  Punto 3: DC permitió un inicio de sesión exitoso mediante un ataque de pulverización de contraseñas, lo que significa una política de contraseñas débil. TCMS recomienda la siguiente política de contraseñas, según el Centro para la Seguridad de Internet (CIS):   * 14 caracteres o más * Utilice contraseñas diferentes para cada cuenta a la que acceda * No utilice palabras y nombres propios en las contraseñas, independientemente del idioma.   Ítem 4: OWA permitió la enumeración de usuarios. TCMS recomienda que DC sincronice los mensajes de cuenta válidos e inválidos.  Además, TCMS recomienda que DC:   * Capacite a los empleados sobre cómo crear una contraseña adecuada * Verifique las credenciales de los empleados con contraseñas violadas conocidas * Disuadir a los empleados de utilizar correos electrónicos y nombres de usuario del trabajo como credenciales de inicio de sesión para otros servicios a menos que sea absolutamente necesario. |

Informes y escaneos adicionales (informativos)

TCMS proporciona a todos los clientes toda la información del informe recopilada durante las pruebas. Esto incluye análisis de vulnerabilidades y una hoja de cálculo de resultados detallados. Para obtener más información, consulte los siguientes documentos:

* **Compañía de demostración-867-19 Hallazgos completos.xslx**
* **Demo Company-867-19 Resumen de análisis de vulnerabilidades.xslx**
* **Demo Company-867-19 Escaneo de vulnerabilidad por Host.pdf**



Última página