<LOGOTIPO/NOMBRE DEL EQUIPO>

<AÑO> Informe de evaluación de la seguridad preparado para

<REEMPLAZAR CON EL LOGOTIPO DEL CLIENTE: CAMBIAR LOS COLORES TAMBIÉN>

Informe emitido: <FECHA DEL EXAMEN>

## Aviso de confidencialidad

*Este informe contiene información sensible, privilegiada y confidencial. Se deben tomar precauciones para proteger la confidencialidad de la información contenida en este documento. La publicación de este informe puede causar daños a la reputación de <NOMBRE CLIENTE> o facilitar ataques contra <NOMBRE CLIENTE>. <TEAM NAME> no será responsable de los daños especiales, incidentales, colaterales o consecuentes que surjan del uso de esta información.*

## Renuncia

*Tenga en cuenta que es posible que esta evaluación no revele todas las vulnerabilidades que están presentes en los sistemas dentro del alcance del compromiso. Este informe es un resumen de los hallazgos de una evaluación "puntual" realizada en el entorno de <CLIENT NAME>. Cualquier cambio realizado en el entorno durante el período de prueba puede afectar los resultados de la evaluación.*

**TABLA DE CONTENIDOS**

**RESUMEN 3**

[<Opcional - Problema mayor> Recomendación](#_xi9pwbdo96zs) 3

[**DESCRIPCIÓN GENERAL DE LA EVALUACIÓN DE ALTO**](#_vrxmgfhvd2vy) **NIVEL 4**

[Fortalezas de seguridad observadas](#_hbll3idtj3mt) 4

[Áreas de mejora](#_8scnpo1z4bcx) 4

[Recomendaciones a corto plazo](#_3wlz3a5xsr9u) 4

[Recomendaciones a largo plazo](#_kjl6c96bkl8) 4

[**ALCANCE**](#_si0wj5j15p77) **6**

[Redes](#_ivezkd6kiocx) 6

[Otros](#_nzuakwsdt6rt) 6

[Credenciales proporcionadas](#_1guor7qepakl) 6

[**METODOLOGÍA DE**](#_dam9lby6qdj3) **ENSAYO 7**

[**DEFINICIONES DE**](#_4cbm8he7gc1m) **CLASIFICACIÓN 8**

[Clasificaciones de riesgo](#_s6qypp4zj5nq) 8

[Clasificaciones de probabilidad de explotación](#_lruj9twjesc2) 8

[Clasificaciones de impacto en el negocio](#_uqxr1e88ekga) 9

[Clasificaciones de dificultad de corrección](#_sm4k0lgedf14) 9

[**RESULTADOS DE LA**](#_5s0202lc8e79) **EVALUACIÓN 10**

[**APÉNDICE A - HERRAMIENTAS UTILIZADAS**](#_g7cophwnkg9g) **13**

[**APÉNDICE B - INFORMACIÓN SOBRE EL**](#_kzx5oj6hc3zc) **COMPROMISO 14**

[Información del cliente](#_veb77t36itfa) 14

[Información de la versión](#_zew1fi62hkvd) 14

[Información de contacto](#_mmygx7611ii0) 14

# 

# RESUMEN EJECUTIVO

<NOMBRE DEL EQUIPO> realizó una evaluación de seguridad de la red corporativa interna de <NOMBRE DE CLIENTE> EN <FECHA DE PRUEBA>. La prueba de penetración de <TEAM NAME> simuló un ataque de un actor de amenazas externo que intentaba obtener acceso a los sistemas dentro de la red corporativa <CLIENT NAME>. El propósito de esta evaluación fue descubrir e identificar vulnerabilidades en la infraestructura de <CLIENT NAME> y sugerir métodos para remediar las vulnerabilidades. <NOMBRE DEL EQUIPO> identificó un total de vulnerabilidades <VULN TOTAL NUM> dentro del alcance del compromiso que se desglosan por gravedad en la tabla a continuación.

|  |  |  |  |
| --- | --- | --- | --- |
| **CRÍTICO** | **ALTO** | **MEDIO** | **BAJO** |
| **1** | **2** | **2** | **1** |

Las vulnerabilidades de mayor gravedad dan a los atacantes potenciales la oportunidad de <MALAS ACCIONES QUE PODRÍAN OCURRIR AQUÍ - PÁRRAFO COMPLETO CON DETALLES DE ALTO NIVEL>. Para garantizar la confidencialidad, integridad y disponibilidad de los datos, las correcciones de seguridad deben implementarse como se describe en los resultados de la evaluación de seguridad.

Tenga en cuenta que es posible que esta evaluación no revele todas las vulnerabilidades que están presentes en los sistemas dentro del alcance. Cualquier cambio realizado en el entorno durante el período de prueba puede afectar los resultados de la evaluación.

## <Opcional - Gran problema> Recomendación

Este es un párrafo opcional que analiza una serie muy crítica de fallas comerciales (por ejemplo, incumplimiento de las regulaciones legales aplicables) que no es una vulnerabilidad técnica, pero aún así debe llamarse la atención del equipo ejecutivo.

# DESCRIPCIÓN GENERAL DE LA EVALUACIÓN DE ALTO NIVEL

## Fortalezas de seguridad observadas

<NOMBRE DEL EQUIPO> identificó las siguientes fortalezas en la red de <NOMBRE CLIENTE> lo que aumenta considerablemente la seguridad de la red. <NOMBRE DEL CLIENTE> debe continuar monitoreando estos controles para garantizar que sigan siendo efectivos.

<Categoría de fuerza>

* Gran cosa que vimos aquí que nos causa problemas (lo cual es algo bueno)
* Lorem ipsum dolor sit amet, consectetur adipiscing elit, eiusmod sed tempor incididunt ut labore et dolore magna aliqua.

## Áreas de mejora

<NOMBRE DEL EQUIPO> recomienda <NOMBRE DE CLIENTE> realiza las siguientes acciones para mejorar la seguridad de la red. La implementación de estas recomendaciones reducirá la probabilidad de que un atacante pueda atacar con éxito los sistemas de información de <CLIENT NAME> y/o reducir el impacto de un ataque exitoso.

### Recomendaciones a corto plazo

<NOMBRE DEL EQUIPO> recomienda <NOMBRE DEL CLIENTE> realizar las siguientes acciones lo antes posible para minimizar el riesgo empresarial.

<Categoría de recomendación>

* <Recomendación individual>
* Lorem ipsum dolor sit amet, consectetur adipiscing elit, eiusmod sed tempor incididunt ut labore et dolore magna aliqua.

### Recomendaciones a largo plazo

<NOMBRE DEL EQUIPO> recomienda que se tomen las siguientes medidas durante los próximos <NUM> meses para solucionar problemas difíciles de solucionar que no representan un riesgo urgente para el negocio.

<Categoría de recomendación>

* <Recomendación individual>
* Lorem ipsum dolor sit amet, consectetur adipiscing elit, eiusmod sed tempor incididunt ut labore et dolore magna aliqua.

# 

# ALCANCE

Todas las pruebas se basaron en el alcance definido en la Solicitud de Propuesta (RFP) y las comunicaciones oficiales escritas. Los elementos en el ámbito se enumeran a continuación.

## Redes

|  |  |
| --- | --- |
| **Red** | **Nota** |
| 10.0.1.0/24 | Red para la sede corporativa |
| 10.0.2.0/24 | Gotham, NY, sucursal |

## Otro

|  |  |  |
| --- | --- | --- |
| **Nombre** | **Tipo de sistema** | **Nota** |
| Sistema IVR | Teléfono | 555-555-1234 |

## Credenciales proporcionadas

<NOMBRE DEL CLIENTE> proporcionado <NOMBRE DEL EQUIPO> con las siguientes credenciales y acceso para facilitar la evaluación de seguridad que se enumeran a continuación.

|  |  |
| --- | --- |
| **Artículo** | **Nota** |
| Cuenta de cliente | (testuser@example.com) Una cuenta de cliente falsa en la aplicación XXXX para probar la funcionalidad que requiere autenticación. |
| Teléfono de prueba IVR | (555-555-5678) Teléfono específico para usar en las pruebas del sistema IVR. |

# 

# METODOLOGÍA DE PRUEBA

<EL NOMBRE DEL EQUIPO VA AQUÍ> La metodología de prueba de se dividió en tres fases: *Reconocimiento*, *Evaluación de objetivos* y *Ejecución de vulnerabilidades*. Durante el reconocimiento, recopilamos información sobre los sistemas de red de <CLIENT NAME>. <EL NOMBRE DEL EQUIPO VA AQUÍ> utilizó el escaneo de puertos y otros métodos de enumeración para refinar la información de destino y evaluar los valores objetivo. A continuación, realizamos nuestra evaluación específica. <EL NOMBRE DEL EQUIPO VA AQUÍ> simuló un atacante que explota vulnerabilidades en la red <NOMBRE DE CLIENTE>. <EL NOMBRE DEL EQUIPO VA AQUÍ> reunió evidencia de vulnerabilidades durante esta fase del compromiso mientras realizaba la simulación de una manera que no interrumpiera las operaciones comerciales normales.

La siguiente imagen es una representación gráfica de esta metodología.

# 

# DEFINICIONES DE CLASIFICACIÓN

## Clasificaciones de riesgo

|  |  |  |
| --- | --- | --- |
| **Nivel** | **Puntuación** | **Descripción** |
| **Crítico** | **10** | La vulnerabilidad representa una amenaza inmediata para la organización. La explotación exitosa puede afectar permanentemente a la organización. La corrección debe realizarse inmediatamente. |
| **Alto** | **7-9** | La vulnerabilidad representa una amenaza urgente para la organización, y se debe priorizar la corrección. |
| **Medio** | **4-6** | La explotación exitosa es posible y puede resultar en una interrupción notable de la funcionalidad del negocio. Esta vulnerabilidad debe remediarse cuando sea posible. |
| **Bajo** | **1-3** | La vulnerabilidad representa una amenaza insignificante/mínima para la organización. La presencia de esta vulnerabilidad debe tenerse en cuenta y remediarse si es posible. |
| **Informativo** | **0** | Estos hallazgos no tienen una amenaza clara para la organización, pero pueden hacer que los procesos de negocio funcionen de manera diferente a la deseada o revelar información confidencial sobre la empresa. |

## Clasificaciones de probabilidad de explotación

|  |  |
| --- | --- |
| **Probabilidad** | **Descripción** |
| **Probable** | Los métodos de explotación son bien conocidos y se pueden realizar utilizando herramientas disponibles públicamente. Los atacantes poco calificados y las herramientas automatizadas podrían explotar con éxito la vulnerabilidad con una dificultad mínima. |
| **Posible** | Los métodos de explotación son bien conocidos, pueden realizarse utilizando herramientas públicas, pero requieren configuración. La comprensión del sistema subyacente es necesaria para una explotación exitosa. |
| **Improbable** | La explotación requiere una comprensión profunda de los sistemas subyacentes o habilidades técnicas avanzadas. Pueden requerirse condiciones precisas para una explotación exitosa. |

## Clasificaciones de impacto en el negocio

|  |  |
| --- | --- |
| **Impacto** | **Descripción** |
| **Destacado** | La explotación exitosa puede resultar en grandes interrupciones de las funciones críticas del negocio en toda la organización y daños financieros significativos. |
| **Moderado** | La explotación exitosa puede causar interrupciones significativas en las funciones comerciales no críticas. |
| **Menor** | La explotación exitosa puede afectar a pocos usuarios, sin causar mucha interrupción en las funciones comerciales rutinarias. |

## Clasificaciones de dificultad de corrección

|  |  |
| --- | --- |
| **Dificultad** | **Descripción** |
| **Duro** | La corrección puede requerir una reconfiguración extensa de los sistemas subyacentes que lleva mucho tiempo. La corrección puede requerir la interrupción de las funciones comerciales normales. |
| **Moderado** | La corrección puede requerir reconfiguraciones o adiciones menores que pueden requerir mucho tiempo o ser costosas. |
| **Fácil** | La remediación se puede lograr en un corto período de tiempo, con poca dificultad. |

## 

# RESULTADOS DE LA EVALUACIÓN

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Número** | **Hallazgo** | **Puntuación de riesgo** | **Riesgo** | **Página** |
| 1 | Ejemplo de búsqueda de vulnerabilidades | **9** | **Alto** | 11 |
| 2 | El conjunto de reglas de firewall no es una práctica recomendada | **8** | **Alto** | 12 |
| 3 | Software obsoleto | **6** | **Medio** | 69 |
| 4 | Múltiples vulnerabilidades XYZ | **5** | **Medio** | 420 |
| 5 | Hallazgo falso | **2** | **Bajo** | 6969 |

NOTA DE LA PLANTILLA: (Ordenar por puntuación de riesgo descendente)

**1 - Ejemplo de búsqueda de vulnerabilidades**

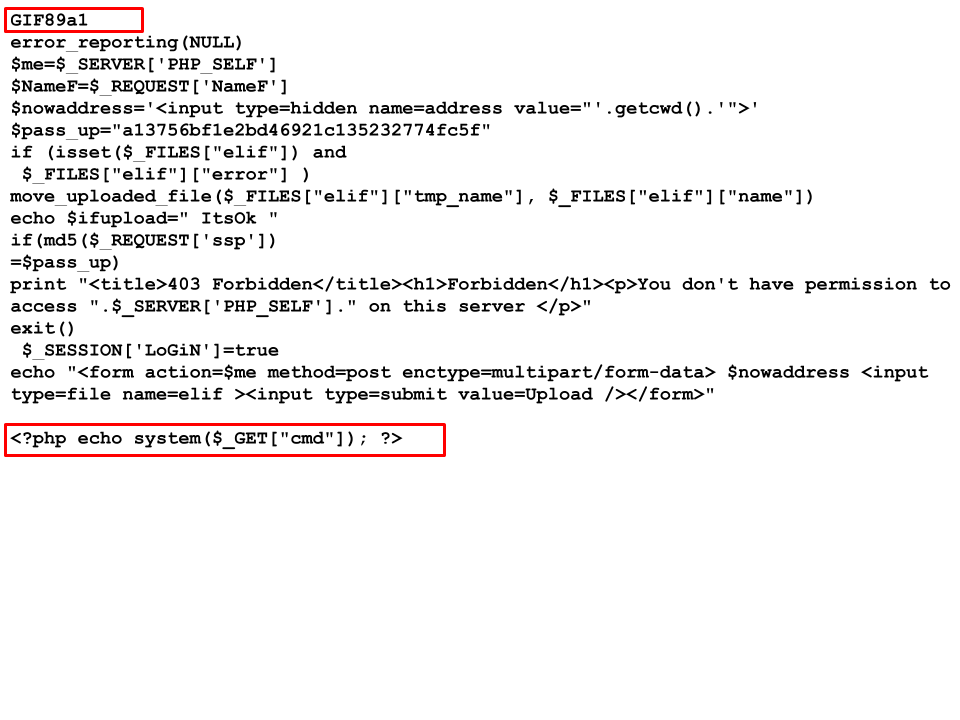
|  |  |
| --- | --- |
| **ALTO RIESGO (8/10)** | |
| **Probabilidad de explotación** | **Posible** |
| **Impacto en el negocio** | **Muy fuerte** |
| **Dificultad de remediación** | **Fácil** |

**Implicaciones de seguridad**

Aquí es donde usted da una descripción de 1-2 oraciones sobre el mayor impacto del hallazgo. Este hallazgo es muy importante porque puede destruir todo el negocio si no se controla.

**Análisis**

Discusión más larga del hallazgo. Incluye capturas de pantalla. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum (véase el apéndice 1).



***Figura 2.3.1****: Un webshell* *php cargado en la aplicación XYZ*

**Recomendaciones**

* Elimine XYZ para hacer las cosas más seguras
* Si no puede eliminar XYZ, haga esto...

**Referencias (opt)**

* <https://github.com/Sevaarcen/RADAR/tree/master/radar/playbooks>
* <https://owasp.org/www-project-top-ten/>

# APÉNDICE A - HERRAMIENTAS UTILIZADAS

|  |  |
| --- | --- |
| **HERRAMIENTA** | **DESCRIPCIÓN** |
| **Edición comunitaria** de BurpSuite | Se utiliza para probar aplicaciones web. |
| **Metasploit** | Se utiliza para la explotación de servicios vulnerables y el escaneo de vulnerabilidades. |
| **Nmap** | Se utiliza para escanear puertos en hosts. |
| **OpenVAS** | Se utiliza para escanear las redes en busca de vulnerabilidades. |
| **Herramientas de cliente de PostgreSQL** | Se utiliza para conectarse al servidor PostgreSQL. |

***Cuadro A.1:*** *Herramientas utilizadas durante la evaluación*

# APÉNDICE B - INFORMACIÓN SOBRE EL COMPROMISO

## Información del cliente

|  |  |
| --- | --- |
| **Cliente** | <NOMBRE DEL CLIENTE> |
| **Contacto principal** | <Nombre de la persona>, <Título de la persona> |
| **Aprobadores** | Las siguientes personas están autorizadas a cambiar el alcance del compromiso y modificar los términos del compromiso.   * <NOMBRE DE LA PERSONA 1> * <NOMBRE DE LA PERSONA 2> |

## Información de la versión

|  |  |  |
| --- | --- | --- |
| **Versión** | **Fecha** | **Descripción** |
| 1.0 | <FECHA AQUÍ> | Informe inicial al cliente |

## Información de contacto

|  |  |
| --- | --- |
| **Nombre** | <NOMBRE DEL EQUIPO> Consultoría |
| **Dirección** | 1001 Fake Street, Gotham, NY 11201 |
| **Teléfono** | 555-185-1782 |
| **Correo electrónico** | <REEMPLAZAR CON EL CORREO ELECTRÓNICO PROPORCIONADO> |