|  |  |  |  |
| --- | --- | --- | --- |
| **Responsable del proyecto por parte de CLIENTE** | **Elaboró - DSA** | **Revisó - DSA** | **Aprobó – DSA**  **TAM - DSA** |
| Nombre responsable Cliente | Armin García | Frank Ortiz | Jésus Santiago Ávila |
|  |  |  |  |
| Fecha de firma: | | | |
| Nota: La fecha de revisión del presente reporte por parte del CLIENTE**,** vence a los 5 días después de la fecha de entrega del mismo. | | | |

[1. Objetivo del documento 3](#_Toc346884175)

[2. Introducción 3](#_Toc346884176)

[3. Alcance 3](#_Toc346884177)

[4. Definiciones 4](#_Toc346884178)

[5. Alcance del análisis 5](#_Toc346884179)

[6. Visión General 6](#_Toc346884180)

[Sección A. Hallazgos 7](#_Toc346884181)

[Sección B. Lista de equipos escaneados 16](#_Toc346884182)

[Sección C. Recomendaciones 19](#_Toc346884183)

[ Tecnología 19](#_Toc346884184)

[ Procesos 19](#_Toc346884185)

|  |  |
| --- | --- |
| Objetivo del documento | El objetivo de este documento es proporcionar al CLIENTE los resultados generales e importantes de los escaneos de vulnerabilidades llevado a cabo por el Tiger Team de DSA de Scitum, resumen de actividades realizadas, hallazgos y recomendaciones para mitigar las vulnerabilidades encontradas en los equipos y servicios. |

|  |  |
| --- | --- |
| Introducción | El CLIENTE, tiene como una de sus funciones definir, difundir y supervisar el cumplimiento de las normas, políticas, estándares y procedimientos de calidad y seguridad de la información, con la finalidad de promover y mantener la integridad, precisión, confiabilidad, protección y congruencia de la información del CLIENTE.  Este documento contiene los resultados del escaneo de vulnerabilidades a diversos dispositivos del CLIENTE, basado en la premisa de mantener en niveles aceptables la percepción de riesgo de sufrir una amenaza o ataque por el aprovechamiento de vulnerabilidades. La selección de equipos fue realizada por parte del CLIENTE y se estableció un calendario para la realización de las pruebas.    Cabe mencionar que existieron diversas restricciones en la ejecución de las pruebas, debido a la criticidad de algunos equipos y los horarios planeados para el ejercicio. |

|  |  |
| --- | --- |
| Alcance | Este documento debe ser conocido por:   * + La dirección y las gerencias de Seguridad Informática del CLIENTE.   + Todos los miembros que participan directamente en la planeación, implantación y monitoreo de la infraestructura tecnológica. |

|  |  |
| --- | --- |
| Definiciones | Para facilitar la lectura y comprensión de este procedimiento, se consideran las siguientes definiciones:   1. EV (Escaneo de Vulnerabilidades): Es un proyecto orientado para la obtención de información sobre las debilidades en la infraestructura del CLIENTE. 2. Nessus: Es una herramienta de código libre que se utiliza para la valoración de seguridad que verifica la vulnerabilidad a los ataques de todas las entidades accesibles de la red. También examina todos los servicios TCP/IP de la red e incluye revisiones de vulnerabilidad específica para sistemas operativos, servidores Web y Firewalls. 3. Riesgo: Probabilidad que una amenaza particular explote una vulnerabilidad particular de un sistema. 4. Ataque: Acción de tratar de traspasar controles de seguridad en un sistema. Un ataque puede ser activo, resultando en la modificación de datos, o pasivo, resultando en la divulgación de información. El hecho de que un ataque sea realizado no significa que será exitoso, el grado de éxito depende de la vulnerabilidad del sistema o actividad y de la eficiencia de las medidas existentes. 5. Vulnerabilidad: Debilidad en los procedimientos de seguridad de un sistema, en el diseño del sistema, en la implementación, en los controles internos, y que puede ser explotada para violar la política de seguridad del sistema. 6. Falso positivo: Es la probabilidad de que estando presente cierta actividad identificada en un sistema de detección de intrusos o analizador de redes en un ambiente de red y analizada como tráfico normal, el sistema de detección asuma que la actividad es sospechosa y está presente. |

# Alcance del análisis

El presente reporte incluye un análisis de XXX equipos de los diversos segmentos del Inmueble del CLIENTE Centro que se enlistan a continuación:

|  |  |
| --- | --- |
| **Descripción** | **IP** |
| **Direccionamientos** | **EJEMPLO**  **99.40.24.0/24** |
| **EJEMPLO**  **99.40.20.0/24** |
| **EJEMPLO**  **99.40.16.0/24** |
| **EJEMPLO**  **99.40.12.0/24** |
| **EJEMPLO**  **99.40.36.0/24** |
| **EJEMPLO**  **99.40.40.0/24** |

Estos hallazgos se listan en la **Sección A** de este documento.

|  |  |
| --- | --- |
| Visión General |  |

La auditoría se realizó desde las instalaciones del inmueble de CLIENTE . El escaneo fue realizado en un ambiente con privilegios y direccionamiento interno, con el fin de analizar los componentes y procesos, para mostrar las debilidades de configuración y vulnerabilidades que un usuario malicioso podría aprovechar.

El estudio se considera:

* Cuantificable.
* Consistente.
* Repetible.
* Detallado.

La ejecución de escaneo de vulnerabilidades consistió en las siguientes actividades realizadas:

Las pruebas de descubrimiento de vulnerabilidades que se llevaron a cabo durante el AV a la infraestructura, fueron realizadas acorde a lo especificado por la herramienta de escaneo utilizada, en un horario de 09:00 a 18:00hrs. Durante el mes de enero del 2013.

* No se realizaron pruebas con denegación de servicios activadas, así como técnicas de hackeo activadas.
* No se realizó implementación alguna, derivada de recomendaciones al servicio afectado.

Los resultados muestran la criticidad de las vulnerabilidades descubiertas, de acuerdo al siguiente orden:

* **ALTA:** Equipos que de acuerdo al resultado del escaneo de vulnerabilidades, requieren de un análisis o acción inmediata. Estas vulnerabilidades deben ser corregidas de forma inmediata o en un corto plazo, ya que su presencia pone en riesgo la confidencialidad, integridad y/o disponibilidad de la información contenida en los dispositivos.
* **MEDIA:** Estas vulnerabilidades son consecuencia de una configuración predeterminada o falta de aseguramiento en los dispositivos. Su presencia no pone en riesgo inminente la integridad o confidencialidad de la información, sin embargo es necesario mitigarlas inmediatamente después de corregir las vulnerabilidades críticas.
* **BAJA:** Equipos que tienen habilitados algunos puertos de servicios comunes de acuerdo al sistema operativo y que son necesarios, pero susceptibles de sufrir alguna vulnerabilidad.

## Sección A. Hallazgos

Durante el escaneo de vulnerabilidades los hallazgos fueron los siguientes:

**Cantidad de vulnerabilidades de criticidad Alta – Media - Baja:**

**Segmento 99.40.16.0**

|  |  |
| --- | --- |
| **Riesgo** | **Ocurrencias** |
| Alto | 157 |
| Medio | 15 |
| Bajo | 3 |

**Segmento 99.40.20.0**

|  |  |
| --- | --- |
| **Riesgo** | **Ocurrencias** |
| Alto | 385 |
| Medio | 61 |
| Bajo | 5 |

**Segmento 99.40.24.0**

|  |  |
| --- | --- |
| **Riesgo** | **Ocurrencias** |
| Alto | 524 |
| Medio | 87 |
| Bajo | 10 |

**Segmento 99.40.40.0**

|  |  |
| --- | --- |
| **Riesgo** | **Ocurrencias** |
| Alto | 300 |
| Medio | 40 |
| Bajo | 3 |

**Vulnerabilidades de Riesgo** **Alto**

Las vulnerabilidades de criticidad **Alta** son causadas por las siguientes razones:

**Segmento 99.40.16.0**

**Segmento 99.40.20.0**

**Segmento 99.40.24.0**

**Segmento 99.40.40.0**

Las vulnerabilidades de criticidad Alta detectadas en esta prueba están relacionadas principalmente con la falta de actualizaciones del sistema operativo y aplicaciones instaladas en los mismos. Dichas vulnerabilidades pueden ser remediadas por medio de la instalación de parches de seguridad.

**Vulnerabilidades de Riesgo** **Medio**

Las vulnerabilidades de criticidad **Media** son causadas por las siguientes razones:

**Segmento 99.40.16.0**

**Segmento 99.40.20.0**

**Segmento 99.40.24.0**

**Segmento 99.40.40.0**

Las vulnerabilidades de criticidad Media detectadas en esta prueba están relacionadas principalmente con falta de actualizaciones de aplicaciones y de sistema operativo, malas configuraciones, uso de protocolos no seguros y configuraciones por defecto, estas pueden ser remediadas a través de fortalecimiento, configuración de aplicaciones e instalación de parches a sistemas operativos y a las aplicaciones que estos albergan.

**Vulnerabilidades de Riesgo** **Bajo**

Las vulnerabilidades identificadas con criticidad **Baja**, son principalmente causadas por las siguientes razones:

**Segmento 99.40.16.0**

**Segmento 99.40.20.0**

**Segmento 99.40.24.0**

**Segmento 99.40.40.0**

La mayoría de las vulnerabilidades de criticidad Baja encontradas están relacionadas con problemas de protocolo, mala configuración y pueden ser remediadas a través de fortalecimiento al sistema operativo, además se recomienda revisar la configuración de aplicaciones y sistema operativo y evaluando que los factores configurados no obedezcan configuraciones por defecto y que reflejen un nivel de seguridad que permita resguardad la CIA de la información.

## Sección B. Lista de equipos escaneados

La siguiente tabla lista los equipos que fueron escaneados, a continuación se proporcionan una breve descripción de los campos que conforma la tabla que a continuación se presenta:

* **IP:** Dirección IP de equipo analizado.
* **Nombre:** Muestra el nombre del dispositivo evaluado.

|  |  |  |
| --- | --- | --- |
| **IP** | | **NOMBRE** |
| **99.40.16.0** | | |
| 99.40.16.61 |  | |
| 99.40.16.102 |  | |

## Sección C. Recomendaciones

## Tecnología

Durante la realización del análisis de vulnerabilidades del mes de enero de 2013, se pudieron identificar vulnerabilidades de nivel, Alto, Medio y Bajo. Las vulnerabilidades afectan tanto a sistemas operativos como a las aplicaciones que se encuentran en los mismos.

La mayoría de las vulnerabilidades descubiertas pueden remediarse con las siguientes acciones:

* Instalación de parches y actualizaciones más recientes en aplicaciones, equipos y sistemas operativos.
* Determinar los parámetros necesarios para evitar una mala configuración o configuración por defecto en equipos.
* Determinar si el servicio de Terminal Services es necesario de lo contrario deshabilitarlo.

Es importante mencionar que las mejores prácticas nos indican que antes de poder instalar un parche de seguridad o fortalecer cualquier servicio o sistema, los cambios deben ser verificados en ambientes de desarrollo para la validación del funcionamiento. Después de esto ya deben ser aplicados a los sistemas en producción. También antes de instalar cualquier actualización es importante la revisión de las políticas de seguridad de la organización, esto para la validación de los cambios correspondiente.

Dar prioridad a los equipos que muestran vulnerabilidades de tipo ALTA y MEDIA en el mediano plazo, llevando a cabo las siguientes recomendaciones:

* Actualizar los parches necesarios para el sistema operativo y aplicaciones albergadas en los mismos.
* Deshabilitar servicios no seguros en caso de no ser necesarios, o en su defecto manejar servicios alternativos que manejen cifrado de las comunicaciones.

## Procesos

* Crear un procedimiento que evalúe los sistemas operativos a utilizar y realice pruebas de compatibilidad
* con actualizaciones para mantener una configuración base (security baseline) que permita al servidor contar con una seguridad mínima aceptable.
* Ejecutar periódicamente pruebas de penetración para descubrir nuevos huecos de seguridad en las aplicaciones.
* Establecer una política de actualización de aplicaciones en equipos y servidores.
* Establecer y/o difundir y/o auditar una política de contraseñas para evitar contraseñas débiles, por defecto o en blanco.