**Informe Técnico de Prueba de Penetración – Infraestructura / Aplicación Web / Red Interna (ajustar según el tipo de pentest)**

**Organización Evaluada:**
Nombre de la empresa o institución objetivo (cliente)

**Empresa Ejecutora del Pentest:**
CertiSysNet Solutions



**Responsable del Informe:**
Nombre del consultor líder
Correo institucional
Teléfono de contacto profesional

**Fecha de Ejecución del Pentest:**
Del 23 al 30 de junio de 2025

**Fecha de Emisión del Informe:**
04 de julio de 2025

Contenido

[**Objetivo general de la prueba.** 2](#_Toc202559028)

[**Infraestructura Evaluada.** 2](#_Toc202559029)

[**Resultados destacados.** 3](#_Toc202559030)

[**Nivel de riesgo general detectado.** 4](#_Toc202559031)

[**Impacto General.** 4](#_Toc202559032)

[**Recomendaciones generales para la alta dirección.** 5](#_Toc202559033)

[**Alcance y Metodología.** 6](#_Toc202559034)

[**Cronograma del Pentest.** 6](#_Toc202559035)

[**Resumen Técnico de Hallazgos.** 6](#_Toc202559036)

[**Detalles Técnicos por Vulnerabilidad.** 7](#_Toc202559037)

[**Conclusión General.** 8](#_Toc202559038)

[**Anexos.** 9](#_Toc202559039)

# **Objetivo general de la prueba.**

El objetivo principal de la presente prueba de penetración es evaluar el nivel de seguridad técnica y operativa de los sistemas identificados dentro del alcance definido, mediante la simulación controlada de ataques reales. Esta evaluación busca:

* Identificar vulnerabilidades explotables en infraestructura, aplicaciones y servicios expuestos.
* Determinar el nivel de riesgo asociado a dichas vulnerabilidades, en términos de confidencialidad, integridad y disponibilidad.
* Validar la efectividad de los controles de seguridad implementados.
* Medir el grado de exposición ante un actor malicioso con conocimientos técnicos avanzados.
* Proveer recomendaciones específicas para reducir la superficie de ataque y fortalecer la postura de seguridad general de la organización.

La prueba se llevó a cabo siguiendo metodologías reconocidas internacionalmente, como OWASP, PTES y MITRE ATT&CK, garantizando una evaluación estructurada, ética y orientada a resultados prácticos.

* Alcance del pentest (activos, IPs, aplicaciones, etc.).

La prueba de penetración fue realizada sobre los activos previamente definidos por el cliente, considerando los siguientes elementos como parte del alcance autorizado:

# **Infraestructura Evaluada.**

* **Rango de direcciones IP internas:** 192.168.1.0/24

# **Resultados destacados.**

**1. Acceso no autorizado a sistemas internos**

Se logró acceso no autenticado al servidor FTP interno mediante credenciales por defecto, lo que permitió la descarga de archivos sensibles y la escalada lateral hacia otros activos de la red.

**2. Ejecución remota de comandos (RCE)**

Se identificó una vulnerabilidad de ejecución remota de código en la aplicación web interna (/admin/upload.php), permitiendo a un atacante ejecutar comandos arbitrarios en el servidor bajo el contexto del usuario del servicio web.

**3. Credenciales expuestas**

A través del análisis de tráfico SMB y servicios mal configurados, se recuperaron múltiples hashes NTLM válidos de usuarios del dominio. Uno de ellos fue crackeado exitosamente, revelando la contraseña de un usuario con privilegios elevados.

**4. Escalada de privilegios en infraestructura Windows**

Mediante el abuso de permisos delegados en GPOs y configuraciones de SeImpersonatePrivilege, se logró escalar privilegios hasta obtener acceso total (NT AUTHORITY\SYSTEM) en el servidor de Active Directory.

**5. Exposición de información confidencial**

Se descubrieron archivos accesibles públicamente (por ejemplo: /includes/config.php) que contenían credenciales de base de datos y claves de API no cifradas.

# **Nivel de riesgo general detectado.**

Con base en los hallazgos identificados, el entorno evaluado presenta un **nivel de riesgo general ALTO**, debido a la combinación de vulnerabilidades críticas, accesos no autorizados, mala gestión de credenciales y configuraciones inseguras.

**Resumen por Nivel de Severidad**

* 🔴 **Críticas:** 3 hallazgos (RCE, acceso no autenticado, escalada a SYSTEM)
* 🟠 **Altas:** 4 hallazgos (exposición de hashes, archivos sensibles, SMB abierto)
* 🟡 **Medias:** 5 hallazgos (versiones desactualizadas, directorios sin restricción)
* 🔵 **Bajas / Informativas:** 6 hallazgos (cabeceras de seguridad ausentes, fingerprinting)

# **Impacto General.**

* **Confidencialidad:** Comprometida — se accedió a información sensible y credenciales.
* **Integridad:** En riesgo — se logró modificar parámetros internos mediante ejecución remota.
* **Disponibilidad:** No afectada directamente, aunque algunos vectores podrían derivar en DoS si se explotan en cadena.

Este nivel de riesgo implica que un atacante con acceso externo o interno limitado podría, con un esfuerzo razonable, comprometer activos críticos de la organización y escalar privilegios de manera progresiva.

Se recomienda aplicar **acciones correctivas prioritarias** sobre los vectores de mayor impacto y realizar una reevaluación de seguridad una vez mitigadas las vulnerabilidades críticas.

# **Recomendaciones generales para la alta dirección.**

A partir de los hallazgos detectados durante la prueba de penetración, se proponen las siguientes recomendaciones estratégicas dirigidas a la alta dirección, con el objetivo de fortalecer la postura de ciberseguridad organizacional:

**1. Establecer un plan de remediación priorizado**

Implementar un plan de acción inmediato para mitigar las vulnerabilidades críticas y altas, especialmente aquellas que permiten acceso no autorizado, escalada de privilegios o exposición de información sensible.

**2. Fortalecer la gestión de credenciales**

Revisar políticas de contraseñas, deshabilitar credenciales por defecto, habilitar autenticación multifactor (MFA) donde sea posible y controlar el ciclo de vida de las cuentas privilegiadas.

**3. Establecer procesos regulares de pruebas de seguridad**

Formalizar la ejecución periódica de pruebas de penetración y escaneos de vulnerabilidades como parte del ciclo continuo de gestión del riesgo tecnológico.

**4. Integrar la ciberseguridad en decisiones de negocio**

Incluir la ciberseguridad como un eje transversal en procesos estratégicos, adquisiciones tecnológicas y proyectos de transformación digital, asegurando que las soluciones cumplan con requisitos mínimos de seguridad desde su diseño.

**5. Capacitación del personal técnico y operativo**

Fomentar la formación continua del equipo de TI en gestión de vulnerabilidades, hardening de sistemas y buenas prácticas de configuración, además de concientizar al personal general sobre riesgos comunes (phishing, ingeniería social).

**6. Adoptar marcos de seguridad reconocidos**

Evaluar la adopción de estándares y marcos como ISO/IEC 27001, NIST Cybersecurity Framework o CIS Controls, para fortalecer la gobernanza y alinearse con las mejores prácticas del sector.

Estas recomendaciones buscan reducir significativamente el riesgo organizacional y facilitar una toma de decisiones informada, alineada con los objetivos de continuidad operativa, cumplimiento normativo y protección de activos críticos.

# **Alcance y Metodología.**

* Tipo de prueba: Caja Negra, Caja Gris, Caja Blanca.
* Enfoque: Interno / Externo / Aplicaciones Web / Infraestructura / Ingeniería Social.
* Herramientas utilizadas (ej. Nmap, Burp Suite, Metasploit, etc.).
* Referencias metodológicas: OWASP, PTES, NIST, OSSTMM.

# **Cronograma del Pentest.**

* Fechas de ejecución.
* Fases del test.



# **Resumen Técnico de Hallazgos.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nombre de la Vulnerabilidad | Severidad | Impacto Potencial | Recurso Afectado | CVSS v3 |
| Ejecución remota de código (RCE) | **Crítica** | Toma de control total del servidor afectado. | srv-web01 | 9.8 |
| Acceso no autenticado a FTP | **Alta** | Acceso a archivos sensibles sin autenticación. | srv-ftp01 | 8.6 |
| Exposición de archivo config.php | **Alta** | Filtración de credenciales de base de datos. | /includes/config.php | 7.5 |
| Hash NTLM expuesto por SMB | **Media** | Posibilidad de crackeo de contraseñas offline. | srv-files01 | 6.5 |
| Enumeración de usuarios por error de login | **Baja** | Enumeración de usuarios válidos del dominio. | srv-ad01 | 3.7 |

Cálculo de CVSS v3.1 (Common Vulnerability Scoring System)

Los rangos de calificaciones de CVSS v3.1 definen la severidad de una vulnerabilidad con base en el puntaje numérico que va de 0.0 a 10.0, dividido en cinco categorías estándar. Aquí se muestra la escala oficial:



# **Detalles Técnicos por Vulnerabilidad.**

|  |  |
| --- | --- |
| Vulnerabilidad | Acceso no autenticado a FTP |
| CVSS v3.1 | **8.6 – Alta** (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N)Acceso sin autenticación, alto impacto en confidencialidad |
| Descripción | El servicio FTP permite conexión sin autenticación. |
| Recomendación | Deshabilitar acceso anónimo o restringirlo por IP. |
| Referencias Técnicas | OWASP A5:2017, CWE-306 |
| Incumplimiento ISO 27001 | A.9.1.2 – Acceso de usuarios a sistemas autorizadosA.13.1.1 – Protección de redes |

Evidencia

Conexión FTP anónima exitosa desde Kali Linux (ftp 192.168.1.11).

# **Conclusión General.**

**Grado de Exposición**

El entorno evaluado presenta un **alto grado de exposición**, tanto a nivel de servicios accesibles sin autenticación (como FTP) como en aplicaciones web con validaciones débiles y almacenamiento inseguro de credenciales. Se identificaron vulnerabilidades críticas que permiten comprometer la confidencialidad y facilitar movimientos laterales dentro de la red interna.

**Nivel de Madurez en Seguridad**

Se observa un **nivel de madurez bajo a intermedio**, con ausencia de controles fundamentales como:

* Autenticación robusta en servicios críticos.
* Gestión adecuada de credenciales y archivos sensibles.
* Procesos de revisión de configuración y hardening.
* Implementación sistemática de parches y actualizaciones.

La arquitectura actual carece de una estrategia unificada de defensa en profundidad.

**Capacidades de Respuesta**

Durante el ejercicio no se detectaron mecanismos automáticos de defensa (como EDR, WAF, alertas SIEM o firewalls de aplicación). No hubo evidencia de bloqueo, detección o respuesta ante intentos de intrusión, lo que indica **capacidad de respuesta reactiva o inexistente** en ciertos segmentos de red.

**Riesgos Críticos a Mitigar a Corto Plazo**

1. **Deshabilitar accesos no autenticados** (FTP, SMB, recursos compartidos).
2. **Remediar RCEs y validar cargas de archivos** en aplicaciones web.
3. **Rotar credenciales expuestas** y almacenar configuraciones sensibles fuera del alcance web.
4. **Implementar segmentación de red y restricción de privilegios** en cuentas de servicio.
5. **Establecer monitoreo activo** de eventos sospechosos y alertas de intrusión.

Se recomienda realizar una nueva evaluación técnica tras aplicar las correcciones, con el fin de validar el cierre de brechas y medir la mejora en la postura de seguridad.

# **Anexos.**

* Evidencias completas.
* Scripts utilizados.
* Logs relevantes.
* Archivos de configuración, capturas de tráfico (pcap), etc.