Informe Final

Evaluación de Seguridad y Reingeniería del Sistema Z

Cliente XY

Grupo: **G06**

Integrantes:

Nombre	Padrón
Pedro Flynn	*105742*
Agustina Schmidt	*103409*
Agustina Fraccaro	*103199*
Kevin Gadacz	*104531*
Abraham Osco	*102256*
Ricardo Luizaga	*87528*

Introducción

El presente documento detalla el análisis, las recomendaciones y las acciones necesarias para mejorar la seguridad y la funcionalidad del Sistema Z, tras identificar vulnerabilidades críticas en su arquitectura actual. Enfocado en garantizar la confidencialidad, integridad y disponibilidad de la información, el informe cubre tanto la evaluación inicial del sistema como las propuestas para su reingeniería y las soluciones a corto y largo plazo para mitigar los riesgos detectados.

El análisis de seguridad incluyó un exhaustivo pentest que evaluó la infraestructura, la aplicación web y las configuraciones de red, revelando problemas como servicios obsoletos, credenciales expuestas y configuraciones deficientes. A partir de estos hallazgos, se establecieron acciones inmediatas y planes de mejora para proteger el sistema contra posibles amenazas.

Asimismo, se propone una transformación integral del sistema para implementar una arquitectura moderna y escalable, con controles de acceso robustos, mecanismos avanzados de cifrado y un diseño enfocado en la experiencia del usuario y la sostenibilidad a largo plazo. Las recomendaciones incluyen herramientas y procesos específicos para fortalecer la seguridad y mantener una postura proactiva ante riesgos emergentes.

Este documento busca servir como una hoja de ruta clara y accionable para alcanzar un nivel óptimo de seguridad y desempeño en el Sistema Z.

RESUMEN EJECUTIVO

El análisis de seguridad del sistema Z reveló vulnerabilidades críticas que comprometen la confidencialidad, integridad y disponibilidad de la información. Se realizó una reingeniería completa del sistema, priorizando un nuevo diseño que implemente controles de seguridad modernos, un almacenamiento seguro de datos y mejores políticas de gestión de acceso. Este enfoque garantizará que el sistema cumpla con los estándares de seguridad actuales y responda a las necesidades del negocio a largo plazo.

1. Evaluación de Seguridad (Pentest)

Objetivo y Alcance

El objetivo principal del pentest fue evaluar la seguridad del servidor y la aplicación web del Sistema Z, identificando vulnerabilidades que pudieran comprometer la confidencialidad, integridad y disponibilidad de los datos de los usuarios y del sistema.

Alcance del pentest:

- Servicios del sistema operativo (SSH, MySQL).
- Aplicación web alojada en un servidor Tomcat.
- Configuraciones de red y firewall.

Hallazgos Clave

1. **Vulnerabilidades en servicios:**
    - **SSH:** Versión obsoleta, susceptible a ataques de fuerza bruta y exploits conocidos.
    - **MySQL:** Configuración predeterminada con cuentas sin contraseñas seguras.
2. **Problemas en la aplicación web:**
    - Exposición de credenciales en el código fuente.
    - Falta de validación de entradas del usuario, abriendo la posibilidad a ataques como SQL Injection.
3. **Configuraciones de red:**
    - Puertos expuestos innecesariamente.
    - Ausencia de reglas estrictas en el firewall.

Recomendaciones Inmediatas

- Actualizar a versiones seguras de todos los servicios y aplicaciones.
- Cambiar contraseñas y eliminar cuentas no autorizadas.
- Implementar un firewall que filtre tráfico sospechoso y limite el acceso externo.

Documentación

- **Informe técnico:** Detalla las vulnerabilidades encontradas, sus implicaciones técnicas y soluciones específicas. Incluye ejemplos prácticos como configuraciones y logs.
- **Informe ejecutivo:** Dirigido a la alta dirección, presenta un resumen claro de los riesgos principales y cómo afectan a los objetivos del negocio.

---

2. Propuesta de Reingeniería

Motivación

El análisis inicial mostró que el Sistema Z opera sobre una arquitectura desactualizada y vulnerable, con controles de seguridad insuficientes. Se recomendó una reingeniería completa para abordar estas deficiencias.

- **Seguridad Integral:** Implementar una arquitectura de seguridad que incluya autenticación y control de acceso adecuado.
- **Mejorar la Experiencia de Usuario:** Rediseñar la interfaz y el flujo de autenticación para optimizar la usabilidad sin comprometer la seguridad.
- **Escalabilidad y Sostenibilidad:** Construir un sistema modular y adaptable para soportar futuras expansiones y cambios de requisitos.
- **Mejora del código:** El diseño del código actual viola los principios SOLID y las buenas prácticas de programación y tiene muy baja cohesión y alto acoplamiento.

- **Implementar la trazabilidad**: Se implementará un registro de las acciones que hace cada usuario, garantizando el no repudio. Y se podrá visualizar gráficos de las solicitudes de recursos a nuestro sistema.

Propuestas Detalladas

1. **Rediseño de la arquitectura:**
    - Migrar hacia microservicios desplegados en contenedores (Docker, Kubernetes).
    - Usar un proxy inverso seguro como Nginx para gestionar el tráfico y añadir un WAF.
2. **Cifrado:**
    - Cifrar todas las comunicaciones con TLS (HTTPS, conexiones a bases de datos).
    - Almacenar datos sensibles en bases de datos cifradas con claves rotativas.
3. **Gestión de accesos:**
    - Implementar políticas de acceso basadas en roles (RBAC).
    - Uso de autenticación multifactor para accesos administrativos.

---

3. Soluciones Temporales

1. **Implementación de un Web Application Firewall (WAF):**
   Se configurará un WAF para filtrar y bloquear ataques comunes como SQL Injection y Cross-Site Scripting (XSS).
2. **Endurecimiento de servidores:**
    - Actualización inmediata de todas las dependencias y servicios.
    - Revisión de configuraciones de permisos en directorios y archivos críticos.
3. **Parcheo de vulnerabilidades:**
   Uso de herramientas como OpenVAS para escanear y aplicar parches en servicios vulnerables.
4. **Control de acceso:**
    - Eliminar cuentas inactivas o innecesarias.
    - Establecer reglas estrictas para contraseñas seguras.
    - Resetear todas las contraseñas existentes con las nuevas reglas.

---

4. Soluciones a Largo Plazo

1. **Monitoreo y detección de amenazas:**
   Implementar un sistema SIEM (Security Information and Event Management) para centralizar y analizar logs, permitiendo detectar amenazas en tiempo real.

2. **Automatización de pruebas de seguridad:**
   Integrar herramientas como OWASP ZAP y Burp Suite en el pipeline de desarrollo para realizar pruebas de seguridad automatizadas.
3. **Capacitación:**
   Diseñar un programa continuo de formación en ciberseguridad para el personal técnico y administrativo.
4. **Revisión periódica:**
   Establecer auditorías regulares para evaluar el cumplimiento de las políticas de seguridad y detectar posibles desviaciones.

---

5. Conclusiones

El proyecto abordó con éxito la evaluación de seguridad y estableció un plan sólido para la reingeniería del sistema. Las acciones inmediatas reducirán significativamente el riesgo mientras se trabaja en soluciones a largo plazo. Este enfoque garantiza un balance entre mitigación de riesgos y mejora continua del sistema.

Recomendaciones finales:

- Priorizar la reingeniería para resolver las deficiencias estructurales del sistema.
- Adoptar una mentalidad de seguridad proactiva en el desarrollo y operación del sistema.
- Continuar evaluando y ajustando las estrategias para adaptarse a un entorno de amenazas en constante evolución.