Propuesta de Trabajo
Sistema XY-Z
Grupo 8

Integrantes:

Nombre	Padrón	Mail
Clara Ruano Frugoli	106835	cruano@fi.uba.ar
Gabriel Katta	105935	gkatta@fi.uba.ar
Maria Paula Brück	107533	pbruck.ext@fi.uba.ar
Paolo Belforte	109432	pbelforte@fi.uba.ar
Rubén Bohórquez	109442	rbohorquez@fi.uba.ar
Ramiro Gestoso	105950	rgestoso@fi.uba.ar
Juan Ignacio Medone Sabatini	103878	jmedone@fi.uba.ar

1. Resumen Ejecutivo

La presente propuesta tiene como objetivo asistir a la compañía XY en la identificación y mitigación de las vulnerabilidades presentes en su nuevo sistema en línea denominado “Sistema Z”.

A raíz de la filtración de información sensible en la deep web, se identificó la necesidad de realizar una revisión integral de la seguridad del sistema, contemplando tanto la infraestructura como la aplicación web, y proponer medidas correctivas y preventivas.

Nuestro enfoque se basa en realizar un análisis de seguridad desde una perspectiva Greybox, combinando técnicas de auditoría y pruebas de penetración.

Asimismo, se contempla el análisis de factibilidad de incorporación de tecnologías como Web Application Firewall (WAF) u otras soluciones de seguridad perimetral, y el planteo de mejoras al diseño actual del sistema, acompañadas de un prototipo funcional de referencia.

La propuesta se estructura en tres fases:

- Diagnóstico: Relevamiento, análisis y prueba de seguridad sobre el sistema actual.
- Reingeniería: Evaluación de mejoras y rediseño con foco en seguridad.
- Prototipo y Presentación: Entrega de informes y presentación ejecutiva.

2. Entendimiento de los Requerimientos

Con base en la documentación provista y el pedido formal de propuesta, entendemos que la Compañía XY busca una evaluación técnica y una propuesta de mejora sobre el Sistema Z, en el contexto de un incidente de seguridad recientemente detectado.

En particular, se requiere:

- Realizar un *Penetration Test* de tipo *Greybox*, que permita identificar debilidades tanto a nivel de la aplicación como de su infraestructura. Este enfoque implica contar con información parcial del sistema y tiene como objetivo simular un escenario realista con conocimiento limitado, para detectar fallas que podrían ser explotadas por actores maliciosos con acceso parcial o conocimiento interno.

- Analizar la factibilidad de implementar soluciones de protección, como un *Web Application Firewall (WAF)* u otro mecanismo de mitigación a definir, teniendo en cuenta las características del entorno, los recursos disponibles y la política de uso preferente de tecnologías open-source.

- Elaborar una propuesta de mejora integral del sistema, que incluya recomendaciones sobre su arquitectura, criterios de seguridad y buenas prácticas, acompañada de un prototipo funcional que refleje los lineamientos principales de dicha propuesta.

Se espera como entregables:

- Un informe técnico que detalle las principales vulnerabilidades detectadas.
- Un informe ejecutivo orientado a la dirección.

Entendemos también que se valorará especialmente la viabilidad técnica y operativa de las propuestas dentro del contexto organizacional actual, priorizando el uso eficiente de recursos y herramientas de código abierto.

3. Descripción del Proyecto

3.1. Metodología de Trabajo

Para dar cumplimiento a los requerimientos establecidos, implementaremos una metodología estructurada en cinco fases secuenciales de las cuales se obtendrán diversas tareas que nos permitirán cumplir con los objetivos propuestos:

- **Fase 1: Planificación y Reconocimiento**

Estableceremos los parámetros fundamentales del proyecto definiendo el alcance de sistemas a evaluar, recopilando la información parcial disponible según el modelo greybox, estableciendo objetivos específicos con métricas de éxito, y elaborando un cronograma detallado que servirá como base estructural para las siguientes fases del proyecto.

- **Fase 2: Análisis y Penetration Testing**

Durante esta fase ejecutaremos un proceso riguroso de identificación y explotación controlada de vulnerabilidades, combinando herramientas automatizadas (como OWASP , OpenVAS) con técnicas manuales para detectar fallos en la aplicación e infraestructura, realizando pruebas estructuradas que incluyen vectores de ataque como inyecciones SQL, XSS y escalada de privilegios, posteriormente documentando cada hallazgo para ser utilizado en futuros análisis.

- **Fase 3: Análisis de Factibilidad WAF/Protecciones**

En esta etapa evaluaremos la viabilidad de implementar soluciones de protección adaptadas al entorno específico, realizando un análisis comparativo de opciones de Web Application Firewall, estudiando su compatibilidad con la infraestructura existente y el potencial impacto en rendimiento.

- **Fase 4: Diseño de Soluciones**

Sobre la base de los hallazgos anteriores, desarrollaremos una propuesta integral de mejora que incluirá el diseño de una arquitectura optimizada utilizando metodologías de modelado de amenazas como STRIDE/DREAD y principios de defensa en profundidad, implementando un prototipo funcional que incorpore las mejoras críticas y la configuración del WAF seleccionado, validando posteriormente la efectividad de estas implementaciones

mediante re-testing de las vulnerabilidades identificadas para garantizar la eficacia de los controles propuestos.

- **Fase 5: Documentación y Reportes**

Como fase final, elaboraremos la documentación comprensiva del proyecto que incluirá un informe técnico detallado con las vulnerabilidades clasificadas por severidad CVSS, descripción técnica exhaustiva, pruebas de concepto y recomendaciones específicas de remediación, así como un informe ejecutivo orientado a la dirección que presentará los hallazgos en lenguaje de negocio, análisis de riesgo e impacto, propuesta de plan de acción con evaluación de costos/beneficios y un roadmap claro para la implementación progresiva de las mejoras recomendadas.

3.2. Información solicitada

Para llevar a cabo efectivamente las fases de nuestra metodología, requerimos la siguiente información preliminar:

- **Información de Sistemas y Aplicaciones**

1. Catálogo y descripción de aplicaciones a ser evaluadas.
2. Casos de uso de las aplicaciones.

- **Información de Infraestructura**

1. Minutas de la infraestructura utilizada por las aplicaciones a ser evaluadas.

- **Información de Acceso**

1. Credenciales de Usuarios de Prueba con privilegios mínimos.
2. Información sobre las prácticas de control de accesos actuales en el sistema (2FA y/o gestores de contraseñas).
3. Máquinas Virtuales que repliquen el ambiente a ser explotado para hacer uso en las pruebas.

- **Información de Seguridad Existente**

1. Información o Reportes de vulnerabilidades previamente detectadas (Si existen).
2. Especificaciones sobre implementaciones de firewalls existentes.

3.3. Tareas y Entregables

Las tareas se organizan de acuerdo con las fases previamente descritas, y se detallan junto con los entregables correspondientes. A continuación, se describe el plan de trabajo con las actividades y sus entregables asociados:

Fase 1: Planificación y Reconocimiento

- **Tarea 1.1:** Definir el alcance de los sistemas a evaluar.
    - **Entregable:** Documento de alcance del proyecto.
- **Tarea 1.2:** Establecer un cronograma detallado del proyecto.
    - **Entregable:** Cronograma de proyecto.

Fase 2: Análisis y Penetration Testing

- **Tarea 2.1:** Realizar pruebas de penetración utilizando herramientas automatizadas (OpenVAS, etc).
    - **Entregable:** Informe de pruebas automatizadas con detalle de vulnerabilidades detectadas (aplicación, infraestructura) y su clasificación CVSS.
- **Tarea 2.2:** Ejecutar pruebas manuales sobre vectores de ataque como inyecciones SQL, XSS, y escala de privilegios.
    - **Entregable:** Informe de pruebas manuales con hallazgos específicos.
- **Tarea 2.3:** Revisión de gestión de accesos.
    - **Entregable:** Informe de evaluación de permisos y accesos.

Fase 3: Análisis de Factibilidad WAF/Protecciones

- **Tarea 3.1:** Evaluar diferentes soluciones de Web Application Firewall (WAF) que se ajusten a las necesidades de la compañía.
    - **Entregable:** Matriz de comparación de soluciones.
- **Tarea 3.2:** Realizar pruebas de compatibilidad y evaluar el impacto en el rendimiento.
    - **Entregable:** Informe de Impacto de Implementación de WAF.

Fase 4: Diseño de Soluciones

- **Tarea 4.1:** Desarrollar la propuesta integral de mejora del sistema, incluyendo la arquitectura optimizada y el diseño de las soluciones de seguridad.
    - **Entregable:** Documento de propuesta de mejora del sistema.
- **Tarea 4.2:** Desarrollar un prototipo funcional que refleje las mejoras propuestas, con validación de efectividad.
    - **Entregable:** Prototipo funcional con implementación de soluciones de seguridad.

Fase 5: Documentación y Reportes

- **Tarea 5.1:** Elaborar un informe técnico que incluya todas las vulnerabilidades encontradas y que detalle en profundidad las 5 de mayor gravedad.
    - **Entregable:** Informe técnico detallado.
- **Tarea 5.2:** Elaborar un informe ejecutivo orientado al CEO de la empresa.
    - **Entregable:** Informe ejecutivo.
- **Tarea 5.3:** Preparar la presentación y el elevator pitch.
    - **Entregable:** Diapositivas para la presentación.

4. Antecedentes de Trabajo

Nuestro equipo de trabajo está conformado por estudiantes avanzados de ingeniería en informática de la Facultad de Ingeniería de la UBA, contamos con experiencia en varios ámbitos vinculados a la seguridad informática gracias a haber cursado materias tales como Sistemas Operativos, Redes, y en proceso de Criptografía y Seguridad Informática.

Realizamos distintos trabajos utilizando herramientas como Nmap y Wireshark para análisis de paquetes, junto con herramientas de Linux y conocimiento en servicios de DNS, HTTP y SSH.

Se adjuntan los CVs de cada uno de los participantes junto con este informe para información más detallada.

5. Oferta Económica

A continuación, se presenta la estimación financiera correspondiente al desarrollo del proyecto para la empresa XY, conforme a la metodología propuesta.

5.1. Perfiles y Costos Estimados

Para la correcta ejecución del proyecto, se contempla la participación de un equipo interdisciplinario conformado por 7 profesionales con experiencia en áreas clave de ciberseguridad, desarrollo de software y gestión de bases de datos. Se enfocarán en realizar el Penetration Test Greybox y en el análisis y evaluación de componentes de seguridad.
La siguiente tabla detalla los perfiles requeridos, la estimación de horas de trabajo por profesional, la tarifa horaria correspondiente y el costo total asociado a cada rol:
Nota: Todos los valores presentados están expresados en **dólares estadounidenses (USD)**.

Perfil profesional	Cantidad de puestos	Horas estimadas	Tarifa por hora	Costo total
Especialista en Ciberseguridad	3	480 (160 horas por persona)	USD 65/hora	USD 31.200
Analista de Base de Datos	1	160 horas	USD 60/hora	USD 9.600
Desarrollador de Software	3	480 (160 horas por persona)	USD 55/hora	USD 26.400
TOTAL	7	1120 horas		USD 67.200

Esta estructura de costos ha sido calculada en función de la duración estimada de cada fase del proyecto y la dedicación requerida por cada perfil. Los valores presentados permiten ofrecer una estimación clara y transparente de la inversión necesaria para cumplir con los objetivos establecidos.

5.2. Costo Total Estimado del Proyecto

El costo total del proyecto ha sido calculado a partir de la suma de las tareas contempladas en la metodología propuesta, incluyendo el Penetration Test Greybox, el análisis de

mejoras/reingeniería, y la posibilidad de implementar componentes adicionales de seguridad.

A continuación, se detalla la distribución estimada de los costos:

Penetration Test Greybox y análisis inicial de vulnerabilidades: USD 33.200
Análisis de mejora y reingeniería del sistema: USD 34.000
Implementación de componentes adicionales de seguridad: *No incluida en el costo base, en caso de querer solicitar este servicio se realizará el presupuesto del mismo en base a las opciones disponibles.*

***Total estimado del proyecto (sin adicionales)**: **USD* 67.200**
Total estimado del proyecto (con adicionales)**: **USD* 67.200 + el costo correspondiente a la opción seleccionada

5.3. Ampliación del Contrato

En caso de que la compañía XY decida ampliar el alcance del proyecto para incluir tareas adicionales o realizar análisis complementarios no contemplados en el alcance inicial, se aplicarán tarifas horarias específicas para cada recurso asignado.

Para la evaluación, diseño e implementación de componentes de seguridad adicionales como un Web Application Firewall (WAF) u otras tecnologías relevantes se establece una tarifa horaria de:

- **USD 60 por hora** (por especialista involucrado)

Esta tarifa contempla actividades tales como análisis de viabilidad, pruebas técnicas, ajustes sobre el entorno actual, y cualquier otra acción relacionada que se derive de los requerimientos adicionales definidos por la compañía XY.