INFORME EJECUTIVO

PENTEST DEL SISTEMA 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

Índice

Objetivo

La compañía XY, especializada en consultoría legal para litigios comerciales, implementó el Sistema Z para que sus clientes puedan realizar el seguimiento de sus expedientes legales de forma online. Debido a que estos contienen información confidencial, el acceso debe estar restringido únicamente a las partes autorizadas.
Tras la filtración de un expediente sensible difundido en medios, la empresa decidió encargar una auditoría urgente. En este contexto, se nos contrató para realizar un análisis de vulnerabilidades y una prueba de penetración (pentest) con el objetivo de identificar fallos de seguridad en el sistema y proponer soluciones que garanticen la protección de la información.

Alcance

El análisis incluyó:

- La revisión del mecanismo de autenticación del sistema.
- La evaluación de los controles de acceso a los expedientes legales.
- La validación del manejo de sesiones de usuarios.
- La verificación de la seguridad en las comunicaciones.
- El análisis de configuración del servidor donde se aloja el sistema.
- La detección de vulnerabilidades conocidas y riesgos críticos que pudieran permitir accesos no autorizados, robo de información o interrupción del servicio.

Se realizó tanto un análisis de vulnerabilidades como una prueba de penetración controlada, abarcando desde el comportamiento de la aplicación hasta la exposición del entorno operativo. El objetivo final fue identificar puntos débiles que puedan ser aprovechados por un atacante y proponer medidas correctivas que fortalezcan la seguridad del sistema.

Línea de Tiempo

Fase de Análisis (Reconocimiento y Diagnóstico)

Objetivo: Comprender el funcionamiento del sistema, identificar debilidades estructurales y posibles vectores de ataque, sin realizar aún acciones intrusivas.

Paso 1 – Análisis del mecanismo de inicio de sesión y control de acceso.
Se comprobó que no se requiere autenticación para acceder y modificar expedientes.

Paso 2 – Evaluación del acceso administrativo y exploración del entorno.
Se detectó que era posible cambiar la contraseña del administrador local y se realizó un escaneo de servicios expuestos.

Paso 3 – Revisión del manejo de datos transmitidos por el sistema.
Se identificó que las contraseñas se envían sin cifrado y que es posible cargar información inválida en los expedientes.

Paso 4 – Escaneo de seguridad automatizado y diagnóstico del servidor.
Se encontraron múltiples vulnerabilidades críticas: software desactualizado, posibilidad de ejecución remota de código y exposición de información técnica.

Fase de Pentesting (Pruebas de Explotación y Resistencia)

Objetivo: Confirmar el alcance real de las vulnerabilidades detectadas mediante pruebas controladas, evaluando su impacto potencial en la seguridad del sistema.

Paso 1 – Análisis de la gestión de sesiones y estabilidad del sistema.
Se detectaron fallos en la protección de las sesiones y se comprobó que el sistema puede colapsar ante múltiples solicitudes simultáneas.

Paso 2 – Ejecución controlada de un exploit conocido para prueba de impacto.
Se confirmó la posibilidad de tomar control del servidor a través de una vulnerabilidad crítica (Ghostcat).

Resumen Ejecutivo

Durante el análisis de seguridad se identificaron vulnerabilidades de distinto nivel de criticidad que afectan gravemente la confidencialidad, integridad y disponibilidad del sistema. A continuación, se resumen los hallazgos principales:

Vulnerabilidades Críticas

1. El sistema se ejecuta sobre CentOS 5, un sistema operativo obsoleto y sin soporte, dejándolo expuesto a ataques conocidos, sin posibilidad de corregirlos.
2. Se detectó una vulnerabilidad grave, conocida como “Ghostcat”, que permite a un atacante ejecutar código malicioso de forma remota, comprometiendo todo el entorno.
3. No hay control de acceso: cualquier usuario puede ver y crear expedientes sin autenticación.

4. Las credenciales de acceso se transmiten sin estar cifradas, lo que permite que puedan ser interceptadas y leídas fácilmente.
5. Gestión de sesión débil: las sesiones no se invalidan correctamente y podrían ser reutilizadas por un atacante.

Vulnerabilidades Altas

6. El sistema no cuenta con mecanismos que limiten intentos de acceso forzados (como intentos repetidos de adivinar contraseñas), ni en la aplicación ni en el servidor.
7. Varios servicios sensibles, como por ejemplo la base de datos, están expuestos a internet sin protección adecuada.
8. Es posible cambiar la contraseña del administrador del servidor de forma local sin restricciones.
9. El sistema es vulnerable a posibles interrupciones por sobrecarga (ataque conocido como denegación de servicio, donde el servidor deja de funcionar debido a múltiples peticiones que lo sobrecargan).

Vulnerabilidades Medias

10. El sistema permite el uso de funciones que no deberían estar activas y que podrían ser usadas por un atacante para espiar cómo funciona el sistema desde adentro, facilitando ataques más graves.
11. Se están usando tecnologías de conexión antiguas que ya no se consideran seguras, lo que podría facilitar que se intercepten o manipulen las comunicaciones.
12. El sistema muestra información sensible de manera innecesaria cuando ocurre un error, lo que podría ser útil para un atacante.

Vulnerabilidades Bajas

13. El sistema revela pequeños detalles técnicos, como marcas de tiempo y respuestas del servidor, que aunque no son peligrosos por sí solos, pueden ayudar a un atacante a planear un ataque más avanzado.

Vulnerabilidades ocasionadas por fallas organizacionales

14. Se detectó que en las minutas y documentos técnicos del equipo de desarrollo y arquitectura se incluyen datos reales de cuentas y credenciales de acceso al sistema. Esto representa un riesgo grave, ya que esos documentos circulan por múltiples áreas y personas, aumentando la probabilidad de filtración accidental o malintencionada. La exposición de credenciales en documentos no protegidos

compromete toda la seguridad del sistema, independientemente de las medidas técnicas implementadas.

Explicación del Ataque

Se explica a continuación cómo se descubrió y probó cada vulnerabilidad descrita anteriormente.

1. Sistema Operativo sin soporte

Descripción: El servidor que aloja el *Sistema Z* utiliza el sistema operativo CentOS 5, una versión que alcanzó su fin de soporte el 31 de marzo de 2017. Desde esa fecha no recibe parches, lo que lo deja expuesto a ataques conocidos que ya tienen herramientas públicas disponibles para explotarlos.
Además, esta situación incumple buenas prácticas internacionales de seguridad informática y podría tener consecuencias legales o regulatorias.
Evaluación de riesgo: 10/10
Detectado por: escáner de seguridad Greenbone/OpenVAS, que lo clasificó como crítico.
Impacto potencial: un atacante podría tomar control total del sistema explotando fallas conocidas sin necesidad de descubrir nuevas vulnerabilidades.
Pruebas realizadas: se ejecutó un análisis con una herramienta conocida como Greenbone/OpenVAS, que detectó el sistema operativo como obsoleto y sin soporte, lo cual representa una falla crítica.

2. Ghostcat

Descripción: Se detectó que el servidor tiene habilitado un componente llamado AJP, que normalmente se usa para la comunicación interna entre servidores. Sin embargo, en este caso está mal configurado y expuesto a internet. Esta falla permite un ataque conocido como “Ghostcat”, mediante el cual una persona no autorizada puede acceder a archivos internos del sistema e, incluso, subir archivos maliciosos para tomar el control total del servidor.

Evaluación de riesgo: 9.8/10
Detectado por: Escáner de seguridad Greenbone/OpenVAS, que lo reportó como **crítico**.
Impacto potencial: Un atacante podría ejecutar comandos en el servidor como si fuera un administrador, accediendo a toda la información y modificando el sistema a voluntad.

Pruebas realizadas: Se realizó un escaneo con Greenbone/OpenVAS, que identificó la presencia de esta vulnerabilidad específica (“Ghostcat”) y la clasificó con nivel de severidad crítico.

3. Control de acceso

Descripción: Cualquier usuario, incluso sin haberse autenticado, puede acceder al sistema de expedientes y ver o crear registros. No se verifica que el usuario tenga permisos para realizar estas acciones, lo que expone información sensible y permite alterarla sin restricciones.

Evaluación de riesgo: Crítico. Permite a cualquier persona acceder a datos sensibles sin necesidad de autenticación, lo que representa un serio riesgo de filtración o manipulación de información.

Detectado por: Pruebas manuales, ingresando directamente a distintas direcciones del sistema y pruebas con herramientas simples para simular cómo se conecta un usuario

Pruebas realizadas:

- Se pudo buscar y crear expedientes sin necesidad de iniciar sesión ni identificarse en el sistema.
- Fue posible crear expedientes vacíos (sin título ni contenido), y que el sistema les asignara un código inválido.
- Un usuario podía ver todos los expedientes, incluso los creados por otras personas, sin ninguna restricción.

4. Transmisión de credenciales sin cifrado

Descripción: Los usuarios ingresan su usuario y contraseña, pero estos datos viajan por la red sin ningún tipo de protección. Esto quiere decir que, si alguien está espiando la conexión (por ejemplo, en una red Wi-Fi pública), puede ver el usuario y la contraseña tal cual, sin tener que hacer ningún esfuerzo extra para descifrarlos.

Evaluación de riesgo: Alto. Permite el robo de credenciales con ataques muy simples y facilita el acceso no autorizado al sistema.

Detectado por: Revisión manual del funcionamiento del sistema y cómo se envían los datos.

Pruebas realizadas: Pruebas manuales y pruebas con una herramienta conocida como Thunder Client, que te permite emular las peticiones que haría una persona al sistema y analizar las respuestas. Se comprobó que las contraseñas se envían sin cifrado y que el sistema usa HTTP, que es una conexión no segura a Internet, lo que hace más fácil interceptar esos datos.

5. Gestión de sesión deficiente

Descripción: El sistema no cierra bien las sesiones cuando alguien se desconecta. Esto hace que se puedan seguir usando accesos antiguos, lo que facilita que otra persona pueda entrar sin permiso, incluso después de que el usuario cerró su sesión.

Evaluación de riesgo: Alto. Esto puede permitir que un atacante acceda al sistema sin tener que iniciar sesión, especialmente si logra obtener alguna información de acceso guardada.

Cómo se detectó: Se revisó manualmente cómo se comportan las sesiones y se hicieron pruebas con las "llaves" de acceso.

Pruebas realizadas:

- El sistema permite usar accesos antiguos por un tiempo, incluso después de cerrar sesión.

- Las "cookies" (pequeños archivos que el navegador guarda para recordar que estás identificado en un sitio) que guarda el navegador para mantener la sesión tienen configuraciones inseguras, por lo que podrían ser robadas o usadas por alguien más.

6. Falta de límite para intentos fallidos de acceso

Descripción: El sistema permite que cualquiera intente muchas veces seguidas poner usuario y contraseña sin que pase nada más que un mensaje de error. No hay bloqueos, esperas ni pruebas tipo captcha para evitar que alguien pruebe combinaciones una tras otra.

Evaluación de riesgo: Alto. Esto facilita que un atacante pruebe miles de contraseñas hasta encontrar la correcta y acceder al sistema.

Detectado por: Revisión manual y pruebas de acceso repetidas.

Pruebas realizadas: Se hicieron muchos intentos fallidos de login y el sistema nunca bloqueó el acceso ni pidió verificaciones adicionales.

7. Servicios sensibles expuestos sin protección en internet

Descripción: El servidor tiene abiertos varios servicios importantes (como la base de datos y acceso remoto) directamente a internet, sin las protecciones necesarias.

Evaluación de riesgo: Alto. Esto abre la puerta a ataques que podrían tomar control total del servidor o robar información.

Detectado por: Escaneo automático con herramientas especializadas.

Pruebas realizadas: Se descubrió que hay puntos de acceso abiertos en el sistema que pueden ser usados para entrar sin permiso, incluyendo herramientas para conectarse de forma remota y bases de datos expuestas con problemas de seguridad.

8. Cambio de contraseña del administrador sin restricciones

Descripción: Cualquier persona con acceso físico al servidor puede cambiar la contraseña del usuario administrador sin ningún control, lo que le da control total sobre el sistema.

Evaluación de riesgo: Alto. Un acceso físico permite tomar el control completo del servidor sin impedimentos.

Detectado por: Pruebas manuales con acceso local.

Pruebas realizadas: Se comprobó que es posible cambiar la contraseña del administrador sin pedir autenticación ni autorizaciones.

9. Vulnerabilidad a ataques de denegación de servicio (DoS)

Descripción: El sistema se puede bloquear o volver muy lento cuando recibe muchas peticiones al mismo tiempo, como intentos repetidos de acceso o búsquedas.

Evaluación de riesgo: Alto. Un atacante podría hacer que el sistema deje de funcionar, interrumpiendo su uso legítimo.

Detectado por: Pruebas de carga manuales y observación del comportamiento bajo presión.

Pruebas realizadas: Se enviaron muchas solicitudes simultáneas y repetidas que causaron que el sistema se colgara o tardará mucho más en responder.

10. Uso de funciones innecesarias activas en el sistema

Descripción: El sistema tiene activas funciones o servicios que no deberían estar disponibles y que pueden ser aprovechadas por atacantes para obtener datos internos del servidor.

Evaluación de riesgo: Medio. Aunque no da acceso directo, facilita que un atacante consiga información para atacar mejor el sistema.

Detectado por: Escaneo automático y análisis manual.

Pruebas realizadas: Se detectaron funciones activas que revelan datos técnicos o internos que no deberían estar accesibles.

11. Uso de tecnologías de conexión obsoletas e inseguras

Descripción: El sistema utiliza métodos de conexión antiguos que ya no se consideran seguros, lo que facilita que alguien pueda interceptar o manipular la comunicación.

Evaluación de riesgo: Medio. Esto aumenta la posibilidad de que la información viaje sin la protección adecuada y pueda ser comprometida.

Detectado por: Análisis del protocolo y configuraciones del servidor.

Pruebas realizadas: Se identificaron conexiones usando estándares viejos y vulnerables.

12. Exposición innecesaria de información técnica en mensajes de error

Descripción: Cuando el sistema falla o hay un error, muestra detalles técnicos que no debería revelar y que pueden ayudar a un atacante a entender cómo funciona por dentro.

Evaluación de riesgo: Medio. Esta información puede ser usada para planear ataques más efectivos.

Detectado por: Revisión manual de respuestas ante errores.

Pruebas realizadas: Se verificó que los mensajes de error incluyen datos técnicos o mensajes detallados que no aportan al usuario común.

13. Revelación de pequeños detalles técnicos en respuestas del servidor

Descripción: El sistema deja “pistas” técnicas como marcas de tiempo o respuestas del servidor que, aunque no son un problema grave por sí solos, pueden ayudar a un atacante a preparar ataques más sofisticados.

Evaluación de riesgo: Bajo. No compromete directamente la seguridad, pero ofrece información útil para atacantes avanzados.

Detectado por: Análisis manual y escaneo automático.

Pruebas realizadas: Se detectaron respuestas del servidor y detalles de tiempo que se podrían usar para ataques más elaborados.

Conclusión

El Sistema Z y los servicios que lo respaldan presentan múltiples debilidades que comprometen los pilares esenciales de la seguridad de la información.
Nuestro equipo ofensivo ha identificado y documentado exhaustivamente estos fallos, destacando los vectores de ataque más críticos que, combinados, permiten escalar privilegios, filtrar expedientes y degradar el servicio.
En el informe se enumeran todas las vulnerabilidades detectadas y su posible relación con la reciente filtración de un documento clasificado. Sin embargo, no es factible determinar con certeza qué vector fue el utilizado por los atacantes; por ello, la sección de recomendaciones cubre la mitigación de cada escenario plausible.
Recomendamos implementar las siguientes acciones prioritarias

1. Correción inmediata
    - Corregir o mitigar las vulnerabilidades críticas.
2. Revisión de políticas y configuraciones
    - Actualizar gestión de sesiones, cifrados y exposición de servicios
3. Capacitación continua
    - Establecer un programa de formación en ciberseguridad para todo el personal.

La exposición de un sistema legal sin protección suficiente no solo implica un riesgo técnico, sino también un riesgo reputacional y legal. Este informe busca ser un punto de partida para elevar la seguridad del Sistema Z a estándares aceptables en la industria.
La ejecución disciplinada de estas acciones reducirá los riesgos actuales y fortalecerá la resiliencia de la organización frente a amenazas futuras. La seguridad es un proceso continuo; mantener un enfoque proactivo y adaptativo resulta esencial en un panorama de amenazas en permanente evolución.

Pasos a Seguir

Con la entrega de este documento concluye la fase de Pentest. El siguiente paso sería la re-ingeniería defensiva, y será abordado por el equipo de seguridad interno para implementar las correcciones y validar su efectividad, avanzando así hacia una infraestructura alineada con los más altos estándares de seguridad.