Plan de Análisis de Seguridad y Fortalecimiento de la Infraestructura

Informe ejecutivo sobre incidentes de seguridad recientes y recomendaciones estratégicas

Descripción general y contexto

Problema: Se detectó un incidente de seguridad reciente en nuestra infraestructura crítica (servidor web/WordPress).

Impacto potencial: Riesgo de fuga de datos, interrupción del servicio, daño a la reputación y pérdidas financieras.

Objetivo de esta presentación:

- Informar a la gerencia sobre el incidente
- Las medidas de respuesta adoptadas
- Presentar un plan estratégico para fortalecer nuestra estrategia de seguridad.
- Proporcionar a la gerencia contexto sobre la importancia del tema y el objetivo de la reunión.

¿Qué pasó? (El incidente – Resumen ejecutivo)

Vector inicial (Fase 1):

- Vulnerabilidades como el acceso FTP anónimo
- La configuración del directorio de WordPress con un listado de archivos público (wp-content/uploads/).
- Riesgo: Podría permitir la carga de archivos maliciosos y facilitar el reconocimiento de la estructura.

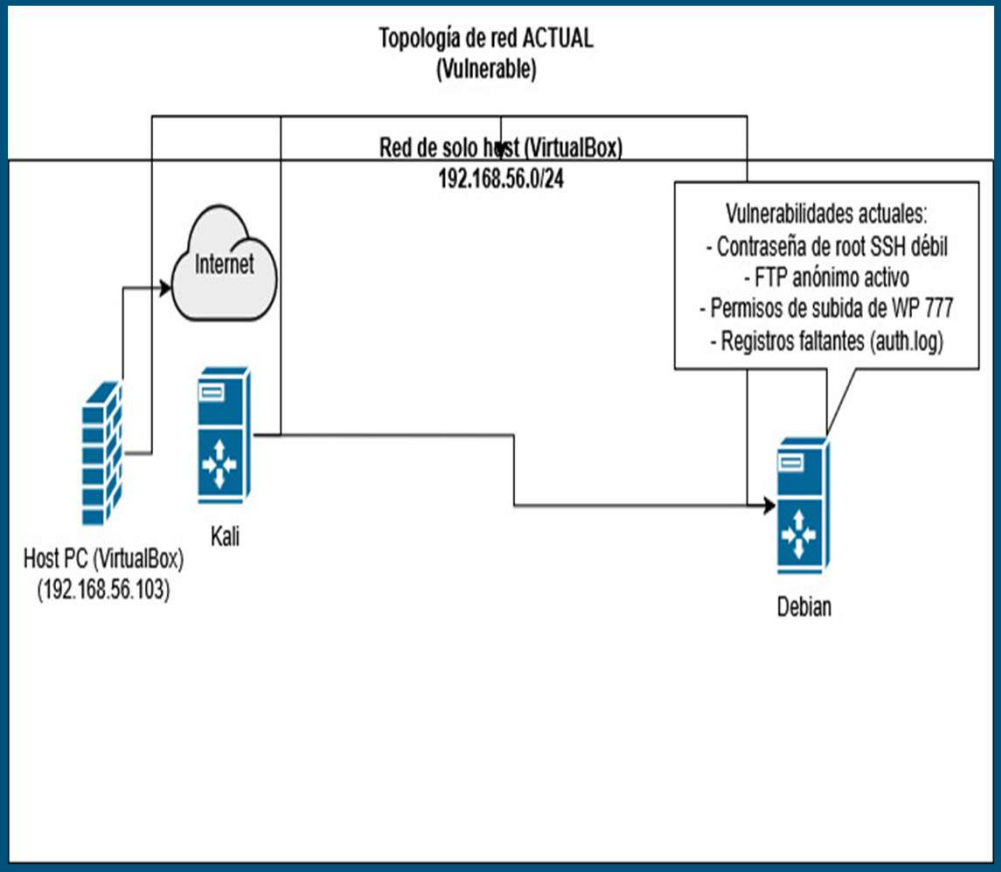
Vulnerabilidad crítica adicional (Fase 2):

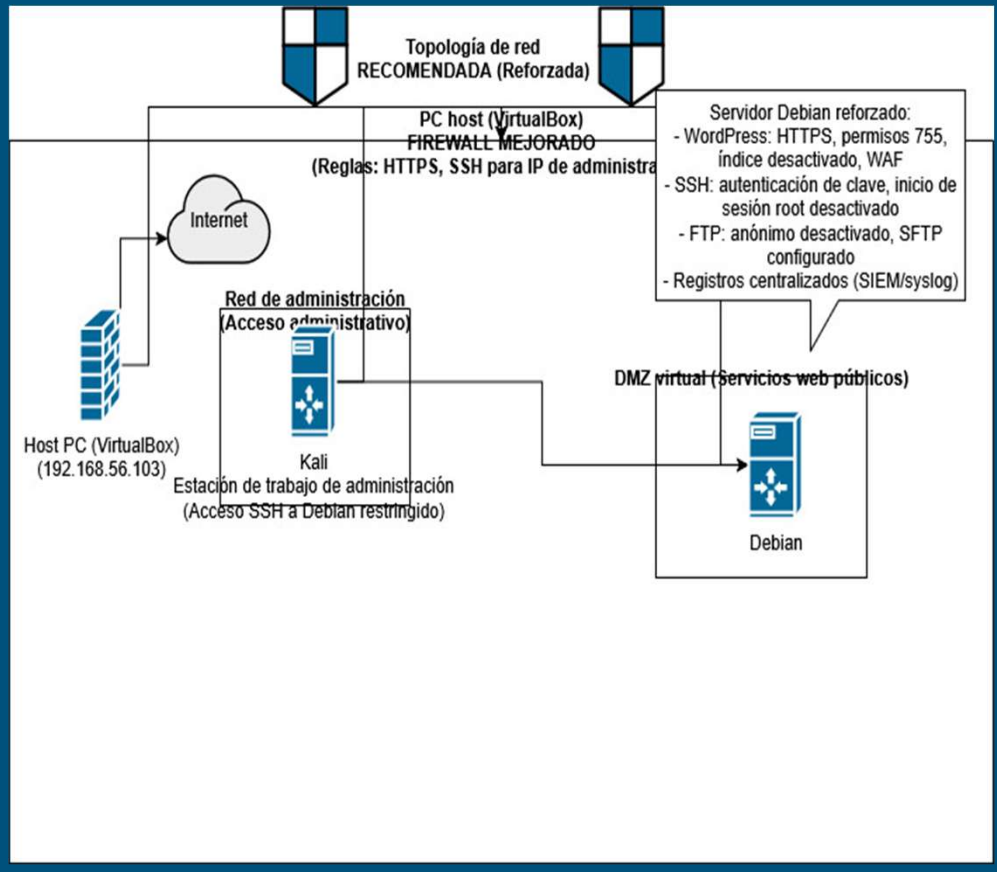
- Credenciales SSH del usuario root extremadamente débiles
- **Impacto**: Otorgó acceso total de administrador al servidor, lo que permitió el control completo y la eliminación de rastros (por ejemplo, eliminando los registros de autenticación).
- **Evidencia de encubrimiento**: Ausencia de registros de autenticación en el servidor.
- **En resumen**: Una combinación de configuraciones predeterminadas inseguras y credenciales débiles creó un punto de entrada crítico para el acceso no autorizado con privilegios elevados.
- **Objetivo**: Explicar el incidente de forma concisa, centrándose en lo sucedido y el posible impacto para la empresa, sin ahondar en jerga técnica compleja.

Medidas inmediatas tomadas (respuesta rápida)

- **Detección**: Monitoreo y análisis manual de vulnerabilidades.
- **Contención y erradicación**: Eliminación de credenciales
- **FTP anónimas**: Cierre del puerto de acceso no autenticado.
- **Corrección de permisos críticos**: Cambio de los permisos del directorio de subidas de WordPress de 777 (acceso completo) a 755 (seguro), desactivando el listado público.
- **Restablecimiento de SSH**: Cambio de la contraseña root a una contraseña segura y compleja. (Esto es crítico).
- **Recuperación**: Se confirmó el funcionamiento y la seguridad de los servicios críticos (web, base de datos) tras las correcciones.
- **Objetivo**: Demostrar que el equipo actuó con rapidez y eficacia para contener y remediar el incidente.

Diagrama de red: antes y después





Recomendaciones estratégicas para el futuro (prevención y resiliencia)

Plan de Respuesta a Incidentes (PRI - Basado en NIST SP 800-61):

Objetivo: Minimizar el impacto y el tiempo de recuperación de futuros incidentes.

Acciones Clave: Formar un equipo de respuesta, desarrollar guías de estrategias, implementar SIEM para el registro y la monitorización centralizados, y realizar simulacros de incidentes con regularidad.

Fortalecer la Protección de Datos:

Copias de Seguridad Robustas: Implementar y probar rigurosamente políticas de copias de seguridad periódicas (externas, aisladas).

Cifrado Integral: Cifrar datos en tránsito (se requiere HTTPS) y en reposo.

Controles de Acceso Estrictos: Implementar la Autenticación Multifactor (MFA) para el acceso crítico, una política de contraseñas robusta y adherirse al Principio de Mínimo Privilegio.

Implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) - ISO 27001:

Objetivo: Adoptar un marco reconocido internacionalmente para la gestión continua de la seguridad de la información.

Beneficios: Reducción de riesgos, cumplimiento normativo, mejora de la reputación.

Acciones Clave: Análisis de riesgos, políticas de seguridad, controles tecnológicos (WAF, reforzamiento, parches) y mejora continua.

Objetivo: Presentar soluciones a largo plazo para fortalecer la seguridad, vinculándolas con beneficios estratégicos para la empresa.

Próximos pasos y solicitud

- **Aprobación**: Solicitar la aprobación de la gerencia para iniciar la fase de implementación de estas recomendaciones estratégicas.
- **Recursos**: Es necesario asignar presupuesto y personal cualificado para los proyectos de SGSI.
- **Plazo estimado**: de 3 a 6 meses para la implementación inicial de SGSI y los controles más urgentes; de 12 a 18 meses para obtener la certificación ISO 27001.
- **Objetivo**: Instar a la gerencia a actuar describiendo los recursos necesarios y un cronograma para los próximos pasos.

FIN DE LA PRESENTACIÓN

Dudas o preguntas

Gracias