

Informe de incidente de seguridad



4 Geeks academy

Contenido

[1. Información General 2](#_Toc191382367)

[2. Descripción del Incidente 2](#_Toc191382368)

[3. Impacto del Incidente 3](#_Toc191382369)

[4. Respuesta al Incidente 3](#_Toc191382370)

[5. Análisis del Incidente 4](#_Toc191382371)

[6. Recomendaciones 4](#_Toc191382372)

[7. Conclusiones 4](#_Toc191382373)

# Información General

- Fecha del Informe : 25 de Febrero de 2025

- Hora del Informe : 13:24 AM

- Nombre del Reportante : Jesús Castaño Martínez

- Cargo del Reportante : Administrador de Sistemas

- Departamento : TI

- Contacto : jesus.castano@4geeks.com

# Descripción del Incidente

-Fecha del Incidente : 26 de Febrero de 2025

-Hora del Incidente : 3:00 PM

-Tipo de Incidente : Acceso no autorizado

-Descripción :

- Se detectó un acceso no autorizado al servidor FTP anónimo de la organización. El acceso fue registrado en los logs del servidor, donde se observó que un usuario no autorizado logró conectarse y descargar archivos sensibles. La actividad sospechosa fue notificada por el sistema de monitoreo de seguridad.

# Impacto del Incidente

- Sistemas Afectados :

- Servidor FTP (IP: 192.168.1.38)

- Datos Afectados :

- Archivos de configuración y documentos internos que no deberían estar disponibles para acceso anónimo.

- Impacto en la Operación :

- El incidente comprometió la confidencialidad de información sensible y generó preocupación sobre la seguridad de otros sistemas. Se detuvo temporalmente el acceso al servidor FTP mientras se investigaba el incidente.

# Respuesta al Incidente

-Acciones Inmediatas:

- Se deshabilitó el acceso anónimo al servidor FTP y se revisaron los logs para identificar la dirección IP del atacante. Se implementaron medidas de seguridad adicionales, como la restricción de acceso por IP.

- Equipos Involucrados:

- Equipo de TI, incluyendo el Administrador de Sistemas y el Especialista en Seguridad.

- Herramientas Utilizadas:

- Herramientas de monitoreo de logs (ej. Splunk), herramientas de análisis de tráfico (ej. Wireshark).

# Análisis del Incidente

- Causa Raíz:

- El acceso no autorizado se debió a la configuración incorrecta del servidor FTP, que permitía el acceso anónimo sin restricciones adecuadas.

- Vulnerabilidades Identificadas:

- Configuración de seguridad inadecuada en el servidor FTP.

- Falta de monitoreo proactivo de accesos y actividades sospechosas.

- Lecciones Aprendidas:

- Es crucial revisar y actualizar regularmente las configuraciones de seguridad de los servidores, especialmente aquellos que permiten acceso anónimo. Se debe implementar un monitoreo más riguroso de los accesos al servidor.

# Recomendaciones

- Medidas Inmediatas:

- Deshabilitar el acceso anónimo al servidor FTP.

- Implementar autenticación de usuario para el acceso al servidor FTP.

- Medidas a Largo Plazo:

- Realizar auditorías de seguridad periódicas en todos los servidores.

- Capacitar al personal sobre las mejores prácticas de seguridad y la importancia de la configuración adecuada de los sistemas.

# Conclusiones

El incidente de acceso no autorizado al servidor FTP anónimo ha resaltado la necesidad de mejorar las medidas de seguridad en la organización. Se han tomado acciones inmediatas para mitigar el riesgo y se han propuesto recomendaciones para prevenir futuros incidentes similares.