Alumno: Rodrigo Vila

Ejercicios Modulo 6 Unidad 1

Ejercicio Número 1 Unidad 1

De acuerdo a lo que se expuso en esta unidad, armar un entregable que describa las opciones que podemos aplicar de medidas de seguridad en un servidor SMTP o a un FTP (cualquier sistema operativo).

Y así como describimos lo bueno, también armar un entregable que describa una opción posible de incidente a un servidor SMTP o a un FTP.

Lo que se solicita, es explicar un ataque a un servidor SMTP o a un FTP (cualquier tipo de ataque, pero dejarlo en claro).

Ejemplo seleccionado: Servidor FTP

1. **Medidas de Seguridad para Servidores FTP**

Servidor FTP (File Transfer Protocol)

1. Introducción

Un servidor FTP (File Transfer Protocol) facilita la transferencia de archivos entre sistemas a través de una red. Sin embargo, el FTP, al ser un protocolo antiguo, presenta ciertas vulnerabilidades que deben ser abordadas para garantizar la seguridad. En esta documentación, se describen las medidas de seguridad para un servidor FTP, se explica un posible incidente de seguridad, se detalla un ataque común, y se comparan los beneficios de utilizar FTPS (FTP Secure) en lugar de FTP.

2. Medidas de Seguridad para un Servidor FTP

Para proteger un servidor FTP, es crucial implementar las siguientes medidas de seguridad:

Uso de Contraseñas Fuertes: Asegurarse de que las contraseñas sean complejas y cambien regularmente.

Control de Acceso: Limitar el acceso a usuarios autorizados y definir permisos específicos para cada usuario.

Directivas de Conexión: Establecer límites de conexión y tiempo de sesión para prevenir ataques de denegación de servicio (DoS).

Uso de FTPS: Para cifrar los datos en tránsito, utilizar FTPS, que añade una capa de seguridad al FTP mediante el uso de TLS/SSL.

Validación de Certificados: Asegurarse de que los certificados TLS/SSL sean válidos y estén configurados correctamente.

Registro de Actividades: Habilitar y revisar los registros de acceso para detectar actividades sospechosas.

Actualización Regular: Mantener el software del servidor FTP y el sistema operativo actualizados con los últimos parches de seguridad.

Revisión de Configuración: Revisar periódicamente la configuración del servidor para asegurar que sigue las mejores prácticas de seguridad.

3. Posible Incidente de Seguridad

Un posible incidente de seguridad en un servidor FTP podría ser la exfiltración de datos. Un atacante puede explotar vulnerabilidades en el servidor FTP para acceder a archivos confidenciales y transferirlos a un servidor externo.

Ejemplo: Un atacante explota una vulnerabilidad en la configuración del servidor FTP para acceder a directorios sensibles. Luego, utilizando una cuenta comprometida, descarga datos confidenciales y los transfiere a un servidor externo, causando una brecha de datos.

Medidas para Mitigar:

Configuración adecuada de permisos de archivo y directorio.

Uso de FTPS para cifrar los datos en tránsito.

Monitoreo y análisis continuo de los registros de acceso.

4. Descripción de un Ataque Común al Servidor FTP

Un ataque común a los servidores FTP es el ataque de fuerza bruta. En este ataque, el atacante usa herramientas automatizadas para probar múltiples combinaciones de nombres de usuario y contraseñas hasta encontrar una válida.

Proceso del Ataque:

Reconocimiento: El atacante identifica la dirección del servidor FTP.

Enumeración: El atacante intenta adivinar nombres de usuario válidos, a veces utilizando técnicas de enumeración. (Haciendo investigación se podría averiguar qué parámetros requiere el usuario o la contraseña para ese server, etc.)

Fuerza Bruta: El atacante utiliza herramientas para probar contraseñas comunes o predefinidas hasta encontrar una combinación válida.

Prevención:

Implementar límites de intentos fallidos de inicio de sesión.

Usa contraseñas fuertes y únicas.

Implementa mecanismos de bloqueo o retraso tras varios intentos fallidos.

5. Beneficios de Usar FTPS en Lugar de FTP

FTPS (FTP Secure) ofrece varias ventajas en comparación con FTP en términos de seguridad:

Cifrado de Datos

Cifrado de Sesiones: FTPS utiliza TLS/SSL para cifrar tanto las credenciales como los datos en tránsito, protegiendo la información contra intercepciones y ataques de sniffing.

Protección Adicional

Autenticación Segura: FTPS proporciona autenticación segura mediante certificados digitales, que ayuda a garantizar que solo los usuarios y servidores autenticados puedan establecer conexiones.

Integridad de Datos: FTPS protege la integridad de los datos mediante el uso de algoritmos de hash, asegurando que los archivos no sean alterados durante la transferencia.

Resistencia a Ataques

Seguridad de Sesiones: FTPS proporciona una mayor seguridad en comparación con FTP, que es vulnerable a ataques de secuestro de sesión, gracias al cifrado de las sesiones.

Aunque el FTP puede ser asegurado mediante varias prácticas, FTPS ofrece una capa adicional de seguridad mediante cifrado y autenticación segura, convirtiéndolo en una opción preferible para la transferencia de archivos segura.

Rodrigo Vila.-