Informe Ejecutivo de Pentesting

Responsable del informe: Luis Fernando Espinoza Arias

Objetivo

El objetivo de esta evaluación fue identificar vulnerabilidades de seguridad en un servidor proporcionado por la empresa, evaluar el impacto de posibles ataques y proponer medidas para prevenir incidentes de seguridad que puedan afectar la confidencialidad, integridad o disponibilidad de los activos digitales de la organización.

Resumen

Durante el ejercicio de pentesting se detectaron múltiples vulnerabilidades en los servicios del servidor analizado (IP: 192.168.1.203). Se logró comprometer el sistema a través de un servicio FTP mal configurado y una instalación de WordPress con endpoints expuestos. Las pruebas comprobaron que se podría:

- Acceder de forma anónima al servidor FTP.
- Realizar ataques de fuerza bruta sobre WordPress.
- Subir archivos maliciosos (reverse shell) y tomar control remoto del servidor.
- Obtener acceso a información confidencial y potencialmente escalar privilegios.

Riesgos Identificados

- Acceso no autorizado vía FTP: Robo o alteración de archivos.
- Exposición de WordPress: Compromiso de cuentas por fuerza bruta.
- Subida de archivos maliciosos: Ejecución remota de comandos.
- Falta de cifrado en FTP: Robo de credenciales por sniffing de red.
- Permisos débiles en el servidor web: Alteración de contenido, puerta trasera.

Acciones Realizadas

Se realizó la explotación controlada de los servicios vulnerables:

- Se obtuvo acceso FTP con usuario y contraseña vulnerados por fuerza bruta con Hydra.
- Se subió una shell PHP al servidor web a través de WordPress (uploads).
- Se estableció una conexión reversa (reverse shell) con acceso a la terminal remota.
- Se documentaron los hallazgos con evidencia.

Remediaciones

- Deshabilitar el acceso anónimo en FTP.
- De forma opcional se recomienda cambiar el puerto por defecto del servicio FTP.
- Restringir los permisos de escritura en directorios de WordPress como /uploads.
- Cambiar a SFTP para asegurar el cifrado en tránsito.
- Implementar cortafuegos (iptables o ufw), para controlar el acceso por IP y puerto.
- Actualizar plugins de seguridad en WordPress y ocultar información sensible.
- Actualizar a contraseñas robustas y autenticar múltiples factores para el acceso remoto.

Conclusión

La evaluación concluyo que el servidor presentaba un nivel crítico de exposición. Las vulnerabilidades podrían comprometer los sistemas, la información podría ser manipulada.

Se recomienda reforzar la seguridad general de los sistemas y revisar la arquitectura con un enfoque de defensa en profundidad.