Auditoría de Sistemas con WinAudit

Nombre del Estudiante: Edison Morocho
Materia: Auditoría Informática

Resumen Ejecutivo

Se realizó una auditoría al sistema informático de la empresa **TechCorp** utilizando la herramienta **WinAudit**. El objetivo fue evaluar la configuración del sistema, el software instalado, la seguridad y las configuraciones de red, identificando posibles vulnerabilidades y proponiendo mejoras.

Los hallazgos principales incluyen:

- **Software desactualizado**: Adobe Reader y Java Runtime Environment no están actualizados.
- **Configuraciones de seguridad débiles**: El firewall no está correctamente configurado y hay puertos innecesarios abiertos.
- **Usuarios con permisos excesivos**: El usuario "Guest" tiene permisos de escritura en carpetas críticas.

Se recomienda actualizar el software, fortalecer la configuración del firewall y revisar los permisos de los usuarios para mejorar la seguridad del sistema.

Metodología Utilizada

1. **Instalación de WinAudit**:
    - Se descargó e instaló WinAudit en el sistema auditado.
    - WinAudit es una herramienta portátil que no requiere instalación compleja.
2. **Configuración de la Auditoría**:
    - Se configuró WinAudit para auditar las siguientes áreas:
        - Información del sistema.
        - Hardware.
        - Software instalado.
        - Configuración de red.
        - Seguridad.
        - Usuarios y grupos.
3. **Recopilación de Datos**:
    - Se ejecutó WinAudit y se generó un informe en formato HTML.
4. **Análisis del Informe**:

- Se analizó el informe generado por WinAudit para identificar configuraciones, software instalado y posibles vulnerabilidades.

Resultados de la Auditoría

1. Información del Sistema

Componente	Detalles
Sistema Operativo	Windows 10 Pro
Procesador	Intel Core i7-9700K
Memoria RAM	16 GB
Almacenamiento	SSD 512 GB
Software Instalado	Microsoft Office, Adobe Reader, Java Runtime Environment, Google Chrome

---

2. Software Instalado y Estado de Actualización

Software	Versión	Última Actualización	Estado
Google Chrome	95.0.4638.54	2023-10-01	Actualizado
Adobe Reader	21.007.20099	2023-09-15	Desactualizado
Java Runtime	8.0.301	2023-08-20	Desactualizado
Microsoft Office	16.0.14326.20404	2023-10-10	Actualizado

---

3. Configuración de Red

Parámetro	Valor
Dirección IP	192.168.1.100
Máscara de Subred	255.255.255.0
Puertos Abiertos	80 (HTTP), 443 (HTTPS), 22 (SSH)
DNS	8.8.8.8

---

4. Usuarios y Grupos

Usuario	Grupo	Permisos
AdminUser	Administradores	Control Total

Usuario	Grupo	Permisos
User1	Usuarios	Lectura/Escritura
Guest	Invitados	Lectura/Escritura

5. Vulnerabilidades Identificadas

Vulnerabilidad	Severidad	Impacto	Recomendación
Software Desactualizado	Alta	Riesgo de explotación de vulnerabilidades conocidas	Actualizar software a la última versión
Configuración de Firewall Débil	Media	Posible acceso no autorizado	Revisar y fortalecer reglas de firewall
Contraseñas Débiles	Alta	Riesgo de acceso no autorizado	Implementar políticas de contraseñas seguras
Puertos Abiertos Innecesarios	Media	Posible acceso no autorizado	Cerrar puertos no utilizados

Recomendaciones

1. **Actualización de Software**:
    - Actualizar **Adobe Reader** y **Java Runtime Environment** a sus versiones más recientes.
    - Implementar un sistema de actualización automática para evitar futuros desfases.
2. **Refuerzo de la Seguridad de Red**:
    - Configurar correctamente el firewall para bloquear accesos no autorizados.
    - Cerrar los puertos innecesarios (por ejemplo, el puerto 22 si no se utiliza SSH).
3. **Políticas de Contraseñas**:
    - Implementar políticas de contraseñas seguras (mínimo 12 caracteres, combinación de mayúsculas, minúsculas, números y símbolos).
    - Requerir autenticación de dos factores para usuarios con permisos elevados.
4. **Revisión de Permisos de Usuarios**:
    - Restringir los permisos del usuario "Guest" para que solo tenga acceso de lectura en carpetas críticas.

Conclusiones

La auditoría realizada con WinAudit permitió identificar varias áreas de mejora en el sistema auditado. Aunque el hardware y el sistema operativo están en buen estado, se encontraron vulnerabilidades críticas relacionadas con software desactualizado, configuraciones de seguridad débiles y permisos de usuarios excesivos.

Las recomendaciones propuestas, como la actualización de software, el refuerzo de la seguridad de red y la revisión de permisos, ayudarán a mitigar los riesgos identificados y a mejorar la seguridad general del sistema.