

Actividad: Auditoría de Seguridad de una Red Informática

Enunciado

Realizar una auditoría de seguridad informática integral a una pequeña empresa (real o ficticia) o a una red doméstica, identificando vulnerabilidades y proponiendo medidas de mejora para fortalecer su seguridad.

Objetivo general:

- Comprender el ciclo completo de una auditoría de seguridad: desde la definición del alcance hasta la elaboración del informe final.
- Aplicar técnicas de reconocimiento, exploración y análisis de vulnerabilidades en entornos reales o simulados.
- Familiarizarse con herramientas de auditoría (como Nmap, Nessus, OpenVAS, Metasploit, entre otras) y realizar una correcta interpretación de sus resultados.
- Desarrollar habilidades de documentación y reporte, presentando hallazgos y recomendaciones de manera clara y profesional.

Duración: Todo el Módulo (actividad progresiva por fases)

Entregable final: Informe de auditoría con todos los apartados desarrollados

FASE 1: Planificación y alcance de la auditoría

Objetivo: Definir el entorno a auditar, los objetivos, el alcance y los recursos disponibles.

Tareas:

- Elegir el entorno (empresa, red doméstica o simulación)
- Establecer los objetivos de la auditoría (por ejemplo: evaluar seguridad perimetral, dispositivos IoT, políticas de acceso, etc.)
- Definir el alcance (qué dispositivos, servicios, sistemas se incluirán)
- Recopilar información básica de la red (número de dispositivos, tipo de conexión, servicios activos, etc.)
- **Autorización y Legalidad:** Es fundamental recalcar que, en caso de auditar una red real, debe existir la autorización expresa del propietario o responsable. En el caso de redes domésticas o

- entornos de laboratorio, se deben seguir buenas prácticas y evitar cualquier actividad que pueda causar daños.
- Será necesario firmar un contrato con el “cliente” y unas cláusulas de confidencialidad.

Herramientas sugeridas:

- Documentación con plantillas (pueden ser hojas de cálculo o procesadores de texto)
- Draw.io o Lucidchart para diagramas de red
- IP Scanner (ej. Advanced IP Scanner)

FASE 2: Reconocimiento y análisis de red

Objetivo: Obtener información detallada de la red y los sistemas conectados.

Reconocimiento

- **Paso 2.1: Reconocimiento pasivo:**
 - Investigar información pública (Whois, dominio, información en redes sociales, registros DNS, etc.).
 - Realizar búsquedas en bases de datos públicas (por ejemplo, Shodan, Censys) para identificar posibles dispositivos expuestos.
- **Paso 2.2: Reconocimiento activo:**
 - Realizar “footprinting” para identificar rangos de IP, sistemas operativos y servicios expuestos.

Tareas:

- Identificar dispositivos activos, direcciones IP y servicios abiertos
- Crear un diagrama de red detallado
- Detectar posibles puntos de entrada y debilidades

Herramientas sugeridas:

- Nmap / Zenmap
- Angry IP Scanner
- Wireshark (opcional para usuarios avanzados)
- Fing (para redes domésticas)
- WHOIS, Shodan, Maltego (para mapeo de relaciones y datos OSINT).
- Google Dorks y bibliotecas OSINT para la recopilación de información.

FASE 3: Detección de vulnerabilidades

Objetivo: Localizar fallos de seguridad y vulnerabilidades en los sistemas y servicios.

Tareas:

- Escaneo de puertos y servicios
- Detección de versiones desactualizadas
- Identificación de contraseñas débiles o configuraciones inseguras

Herramientas sugeridas:

- Nessus Essentials (gratuito con registro)
- OpenVAS
- Nmap + scripts NSE
- Lynis (para sistemas Linux)
- Inspectores de navegadores (para analizar routers o dispositivos IoT)

FASE 4: Pruebas de penetración básicas (opcional según nivel)

Objetivo: Verificar si las vulnerabilidades encontradas pueden ser explotadas.

Tareas (opcionales y simuladas):

- Realizar pruebas controladas de acceso no autorizado
- Evaluar configuración del router o cortafuegos
- Comprobar fuga de información mediante sniffing o escaneo

Herramientas sugeridas:

- Metasploit Framework (solo si el alumno tiene conocimientos avanzados)
- Hydra (para pruebas de fuerza bruta controladas)
- Exploit-DB para búsqueda de exploits conocidos

FASE 5: Evaluación y propuesta de mejoras

Objetivo: Valorar el nivel de seguridad actual y proponer medidas de mejora.

Tareas:

- Clasificar vulnerabilidades por riesgo
- Recomendar soluciones técnicas y organizativas
- Proponer mejoras de configuración, segmentación, control de accesos y backups

Herramientas sugeridas:

- OWASP Top 10 (para tener en cuenta las vulnerabilidades comunes)
- Normas básicas ISO/IEC 27001 para inspirar políticas

FASE 6: Informe final de auditoría

Objetivo: Documentar todos los hallazgos y presentarlos de forma profesional.

Contenido sugerido:

- Introducción y alcance
- Metodología empleada
- Análisis y hallazgos
- Grado de riesgo
- Recomendaciones
- Conclusiones

Formato: Word o PDF. Se valorará claridad, profundidad técnica y presentación.

Actividad asociada al:

- CE1.1 Describir procedimientos de verificación del inventariado del aplicativo en equipos para comprobar versiones y confirmar

que dicho inventario está actualizado, explicando los pasos a seguir.

- CE1.2 Describir procedimientos de comprobación del aplicativo, ya sea "software" de base, aplicaciones genéricas o específicas de seguridad, indicando como determinar si un aplicativo es legítimo y está actualizado.
- CE1.3 Explicar técnicas de revisión de la instalación y configuración de sistemas operativos, detallando los parámetros y valores o configuraciones que afectan a su seguridad.
- CE1.4 Definir los conceptos de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know"), explicando cómo determinar si una aplicación o un usuario lo cumple.
- CE1.5 Clasificar el "software" de seguridad contra programas maliciosos tales como antivirus/"antimalware", EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection and Response"), entre otros, indicando su utilidad y ámbito de aplicación.
- CE1.6 Explicar procedimientos de instalación y configuración de "software" de seguridad contra programas maliciosos, indicando parámetros y valores a comprobar, verificando que tiene activas unas funciones.
- CE1.7 Indicar los pasos a seguir para comprobar las cuentas de usuario de sistemas y aplicaciones, determinando su robustez y la aplicación del principio de "mínimo privilegio".
- CE1.8 En un supuesto práctico de aplicación de técnicas de comprobación de seguridad en el aplicativo de sistemas informáticos, revisando su configuración, para verificar la integridad, confidencialidad, disponibilidad, trazabilidad y no repudio de la información gestionada:
 - ✓ Revisar un inventariado de activos, verificando el aplicativo en unos equipos existentes y sus características, comprobando las versiones que se ejecutan, para confirmar que está actualizado y no hay programas que no aparezcan en el mismo.
 - ✓ Revisar la instalación y configuración de los sistemas operativos, confirmando que el "software" instalado es legítimo, está actualizado y tanto los usuarios como las aplicaciones cuentan con los permisos de "mínimo privilegio" para desempeñar sus funciones en el sistema.
 - ✓ Comprobar la instalación y configuración de un "software" de seguridad contra programas maliciosos tales como antivirus/"antimalware", EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection and Response"), entre otros, verificando que el "software" es legítimo, está actualizado y tiene activas unas funciones indicadas.
 - ✓ Revisar un conjunto de aplicaciones, comprobando licencias y versiones para confirmar que son legítimas, están actualizadas y únicamente pueden ser accedidas por un determinado personal y que ese acceso tenga unas limitaciones basadas en el principio de "mínimo privilegio" y "mínimo conocimiento" o "necesidad de saber" ("need-to-know").

- ✓ Comprobar unas cuentas de usuario, verificando que son individuales, cuentan con una política de contraseñas robusta y han sido elaboradas bajo el principio de "mínimo privilegio" y segregación de funciones.
- ✓ Documentar las pruebas realizadas, incluyendo referencias a los activos del sistema, los parches y actualizaciones instalados en los sistemas operativos y aplicaciones, las configuraciones implementadas, y las vulnerabilidades y no conformidades detectadas junto con su criticidad, así como, las contramedidas aplicadas para dichas vulnerabilidades.

Criterios de corrección:

la valoración máxima de esta actividad es de 10 puntos repartidos entre los siguientes criterios:

- ✓ Estructurar la información aportada con orden jerárquico y sentido. (2 puntos)
- ✓ Dar respuesta coherente y justificada a lo requerido. (4 puntos)
- ✓ Grado de profundidad de la exposición. (3 puntos)
- ✓ Cumplimiento de entrega plazos establecidos (1 punto)