Universidad Nacional de Colombia - sede Bogotá
Facultad de Ingeniería
Departamento de Sistemas e Industrial
Curso: Ingeniería de Software 1 (2016701)

ANÁLISIS AUTOMÁTICO DE NMAP CON IA	
ACTORES Auditor Administrador	**REQUERIMIENTO** Análisis de resultados generados por Nmap por medio de IA (Open AI) para devolver una bitácora cualitativa a partir de un prompt definido.

DESCRIPCIÓN
El usuario con rol de auditor y administrador debe poder tomar como entrada la salida del escaneo Nmap de una auditoría, y generar automáticamente una bitácora cualitativa mediante el uso de la API de OpenAI. El análisis debe basarse en un prompt predefinido que incluya el resumen de puertos abiertos, servicios y versiones, y debe generar un texto técnico que interprete el resultado desde la perspectiva de seguridad informática. El análisis generado debe quedar asociado a la auditoría como una observación automática, incluyendo fecha de generación y referencia al uso de IA. Esta operación requiere conexión a internet activa.

PRECONDICIONES

- La herramienta de escaneo de redes NMAP debe estar instalada previamente en el PATH de variables de entorno en el sistema operativo trabajado; en este caso, Windows 11.
  Instalar la herramienta aquí: https://nmap.org/dist/nmap-7.97-setup.exe
- Se debe contar con conexión a internet para poder realizar “pings” a IPs proporcionadas y consumir la API de OpenAI
- El usuario debe estar registrado como Auditor o Administrador (RF_08)
- La auditoría debe estar previamente registrada (RF_02)
- La auditoría debe estar en estado “En curso”, ”Pendiente”, “Archivado”. No se permite hacer modificaciones u observaciones si se encuentra en estado “Finalizado” (RF_12)
- El usuario se debe encontrar en la visualización específica de una auditoría.
- Debe haberse configurado correctamente la clave de API de OpenAI en el entorno de la aplicación.
  (Sin una API Key válida, la solicitud será rechazada por OpenAI).
- La aplicación debe incluir una función que genere un prompt estructurado a partir

del resultado de Nmap.
(Este prompt debe ser claro, técnico y estar orientado a obtener un análisis de ciberseguridad).

FLUJO NORMAL

{ESCANEO DE RED CON NMAP (CU_04)}

1. El sistema verifica que exista una salida válida de Nmap asociada a esa auditoría.
   ❌ Si no hay salida de Nmap disponible, se muestra un mensaje de advertencia:
   "Primero debe realizar un escaneo con Nmap para generar el análisis automático".
   → **Fin del flujo**.

2. El sistema genera automáticamente un prompt a partir del resultado del escaneo.

3. El sistema envía el prompt a la API de OpenAI usando la clave API configurada.
   ❌ Si la clave API está mal configurada o expirada, se muestra un mensaje:
   "Error de autenticación con OpenAI. Verifique la configuración de la API."
   → **Fin del flujo con error**.
   ❌ Si no hay conexión a internet, se muestra:
   "Conexión a internet no disponible. No se puede generar el análisis en este momento."
   → **Fin del flujo con error**.

4. La IA responde con un análisis técnico estructurado.

5. El sistema registra la observación como generada automáticamente, con metadatos:
   a. Fecha y hora de generación
   b. Texto completo del análisis
   c. Nombre del usuario que solicitó el análisis
   d. Referencia a que fue producido mediante OpenAI

6. El sistema añade esta observación al historial de observaciones de la auditoría (RF_03).

7. El sistema actualiza la vista y muestra al usuario un mensaje de confirmación:
   "Análisis cualitativo generado exitosamente con IA." junto a la respuesta recuperada por la misma.

8. Fin del flujo.

POSTCONDICIONES

- Se ha generado una observación automática de IA y se ha asociado a la auditoría correspondiente.
- Se ha actualizado el historial de observaciones.
- Se ha registrado en el log del sistema una entrada que indica que se generó un análisis automatizado.

- En caso de errores, se ha informado al usuario y registrado el fallo para auditoría interna.

NOTAS

- El análisis de IA no reemplaza el juicio del auditor, pero ofrece una primera interpretación basada en patrones de seguridad.
- La observación generada por IA no puede editarse ni eliminarse y deberá decir explicitamente que fue generada por OpenAI.
- La clave API de OpenAI debe almacenarse de forma segura y no debe estar hardcodeada por temas de seguridad del token de la cuenta usada.
- El prompt debe ser lo suficientemente claro y técnico para evitar resultados ambiguos.
- Puede requerir costos si se usa una versión avanzada para el prompt en OpenAI.
- Este caso de uso invoca al de **ESCANEO DE RED CON NMAP (CU_04)**