



UNIVERSIDAD
NACIONAL
DE COLOMBIA

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

ESCANEEO DE RED CON NMAP

ACTORES

Auditor
Administrador

REQUERIMIENTO

RF_04:

Escaneo agresivo de puertos de la red a partir de la IP otorgada en el registro de la auditoría con la herramienta NMAP.

DESCRIPCIÓN

El usuario con rol de auditor y administrador debe poder ejecutar un escaneo de red agresivo utilizando la herramienta Nmap sobre las direcciones IP registradas previamente en una auditoría, por lo que deberá seleccionar una IP proveída en el registro. El escaneo debe realizarse de forma local desde la aplicación de escritorio mediante comandos del sistema operativo, y debe devolver los resultados de puertos abiertos, servicios activos, versiones detectadas, y posibles vulnerabilidades si están disponibles. El resultado del escaneo debe quedar asociado directamente a la auditoría desde la cual se ejecutó. El sistema debe mostrar al usuario un mensaje claro sobre el progreso y el resultado final del escaneo.

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
- 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.

FLUJO NORMAL

{VISUALIZAR AUDITORÍA (CU_07)}

1. El sistema carga la vista detallada de la auditoría seleccionada (RF_07),

incluyendo las IPs registradas.

2. El sistema verifica que la auditoría no esté en estado "Finalizado".
 Si lo está, el botón "Ejecutar escaneo" se desactiva y se muestra un mensaje: "No se puede escanear auditorías finalizadas".
→ **Fin del flujo.**
3. El usuario pulsa el botón "Ejecutar escaneo de red con NMAP".
4. El sistema verifica que la herramienta NMAP esté correctamente instalada.
 Si no se detecta NMAP, el sistema muestra un mensaje de error: "NMAP no está instalado o no se encuentra en el PATH del sistema. Verifique la instalación."
→ **Fin del flujo con error.**
5. El sistema ejecuta el comando NMAP en segundo plano utilizando las IPs registradas, con parámetros de escaneo agresivo (-A).
6. Durante el escaneo, el sistema muestra un indicador de carga en progreso ("command + scanning...").
7. Una vez finalizado el escaneo, el sistema captura el resultado de salida del comando NMAP.
 Si ocurre un error de red, el sistema muestra: "Error al ejecutar el escaneo. Verifique su conexión a Internet o que las IPs estén activas."
→ **Fin del flujo con error.**
8. El usuario recibe el mensaje: "Escaneo completado exitosamente. Los resultados están disponibles en la sección de escaneo".
9. Fin del flujo.

POSTCONDICIONES

- Se ha notificado visualmente al usuario sobre el resultado de la operación.

NOTAS

- El escaneo se ejecuta con el parámetro -A de NMAP, lo que implica detección de servicios, versiones, sistema operativo y posibles scripts.
- El proceso puede tardar varios minutos dependiendo de la red y número de IPs.
- NMAP debe ejecutarse con permisos suficientes para realizar escaneos profundos (recomendada ejecución como administrador en algunos entornos).
- El resultado del escaneo se podrá analizar luego con IA (ver RF_05).
- Las IPs mal formateadas deben ser filtradas y validadas antes de ejecutar NMAP.
- Este caso de uso invoca al de **VISUALIZAR AUDITORÍA (CU_07)**

