UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Título de la actividad:	Tarea 3: resultados obtenidos
Nombre de la materia:	Programación para ciberseguridad
Nombre de los alumnos:	Julio Abraham Puente Guerrero – 2225457 Alberto Jessier Lucio Sital – 2153884 Sebastián Alighieri Ramírez - 2225388
Nombre del tutor:	Dra. Perla Marlene Viera González
Datos de entrega:	Monterrey, N. L. a 02 de noviembre de 2025.

Introducción

Durante la elaboración del ejercicio se hizo uso de distintas herramientas que tienen diferente enfoque en el área de la seguridad, por lo que, para la ejecución de cada script del repositorio se tenia el objetivo de entregar diferentes resultados al usuario. Es por ello por lo que destacaremos la comprensión que tenemos sobre estos datos recabados.

Desarrollo

El proyecto esta divido en dos tipos de tareas, las pasivas y activas. Las tareas pasivas tienen el objetivo de obtener información que sea publica sobre el sitio de interés, así como datos que la página y su host puedan proporcionar sin llegar a sacar provecho de las tecnologías y herramientas con las que trabaja. Mientras que las tareas activas son las actividades que intentan explotar vulnerabilidades u obtener información a través de brechas que se hayan localizado gracias a las tareas pasivas. Una vez entendido este punto podemos empezar a describir algunas de las características de los datos obtenidos de un sitio web que se puso en funcionamiento para la elaboración de este proyecto.

Para el primer script, llamado ”whois_py” hacemos uso de la librería “whois”, pero en específico de “IPwhois” debido a que nuestro sitio no tiene dominio, haciendo que nos sea posible hacer la consulta sin el problema de tener incompatibilidades con otros scripts que llegasen a necesitar de dominios.
De este script logramos recabar daos como el “asn”, que nos indica el proveedor del servicio de internet, permitiendo que el sitio sea accesible por el rango de ip asignado y el enrutamiento hasta él. Podemos también destacar el host del sitio objetivo, el cual es Digital ocean, el cual es sumamente reconocido por el servicio en la nube, y su facilidad para la gestión de aplicaciones web.

Para el segundo script se utilizó como protagonista el módulo “built_with” el cual nos proporciona las tecnologías que utiliza un sitio web objetivo para funcionar. De los resultados obtenidos, destacamos la

detección del uso de Apache como servidor web para la distribución de los sitios web por el protocolo HTTP, así también, el uso del framework “Bootstrap” para el diseño de la pagina y disminuir el uso de css para cada elemento de la página. Finalmente, se detecto el uso de jQuery para la interacción de JavaScript con el HTML, lo cual permite el uso de animaciones y alertas que la pagina llega a devolver cuando realizas ciertas acciones dentro de ella.

La búsqueda pasiva realizada mediante la API de Shodan sobre la dirección IP seleccionada permitió extraer metadatos relevantes del host como el servicio expuesto, puertos abiertos, ASN y geolocalización aproximada, para consolidarlos en un archivo JSON estandarizado. Dado que la dirección corresponde a un recurso interno de la institución y no tiene dominio público ni registro WHOIS asociado, las técnicas OSINT basadas en dominio (historial DNS, certificados públicos, referencias en buscadores o redes sociales) no son aplicables.

Los hallazgos obtenidos mediante Shodan proporcionan una vista útil del perímetro visible desde Internet que puede indicar servicios expuestos, versiones de software y el bloque de red/organización a la que pertenece la IP. Sin embargo, la precisión de ciertos campos (por ejemplo, geolocalización y nombres inversos) puede ser limitada cuando se trata de direcciones privadas o de entornos gestionados internamente.

Por último, tenemos los datos recabados por el script activo, de los cuales algunos de ellos ya fueron capturados superficialmente por algunos de los scripts pasivos, pero la información sobre los puertos abiertos es la mas relevante, siendo el puerto 22 y 3306 los mas importantes, hablando del puerto 22, tenemos la información acerca del sistema operativo del servidor, siendo un Ubuntu Linux. Y por parte del puerto 3306, recibimos que a través del protocolo tcp, los datos son gestionados a través de MySQL para las conexiones entre clientes y aplicaciones.