TECNOLÓGICO NACIONAL DE MÉXICO

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Instituto Tecnológico de Aguascalientes

INSTITUTO TECNOLÓGICO DE AGUASCALIENTES

Ingeniería en Tecnologías de la Información y Comunicaciones (TICS)

SEGURIDAD EN LAS APLICACIONES DE SOFTWARE TC2 (08:00 - 09:00)

Práctica Unidad II

Consultas Shodan

EQUIPO

Integrantes:

Campos Delgado Diego Alejandro, 20151718

Flores Rodríguez Agustín Quetzal, 20151633

García Betts Gabriel Sebastián, 20151621

Jimenez Herrera Cristian, 20151639

Ramos Sánchez Axel Gael, 20151630

DOCENTE

Ricardo Luna Carlos.

FECHA DE ENTREGA

Aguascalientes, Ags., a 4 de octubre de 2024.

Introducción

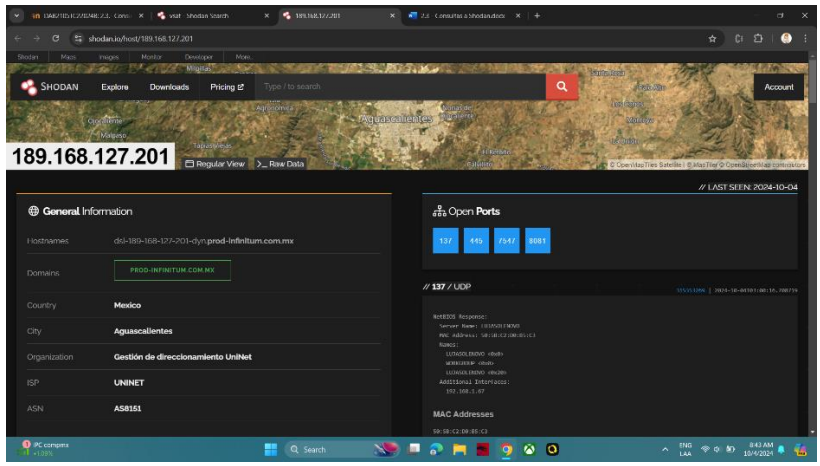
Shodan es un motor de búsqueda especializado que permite a los usuarios encontrar dispositivos conectados a Internet. A diferencia de los motores de búsqueda tradicionales, que indexan sitios web y páginas, Shodan recopila información sobre dispositivos conectados a la red, como servidores, cámaras de seguridad, enrutadores, impresoras, dispositivos IoT (Internet de las Cosas), entre otros.

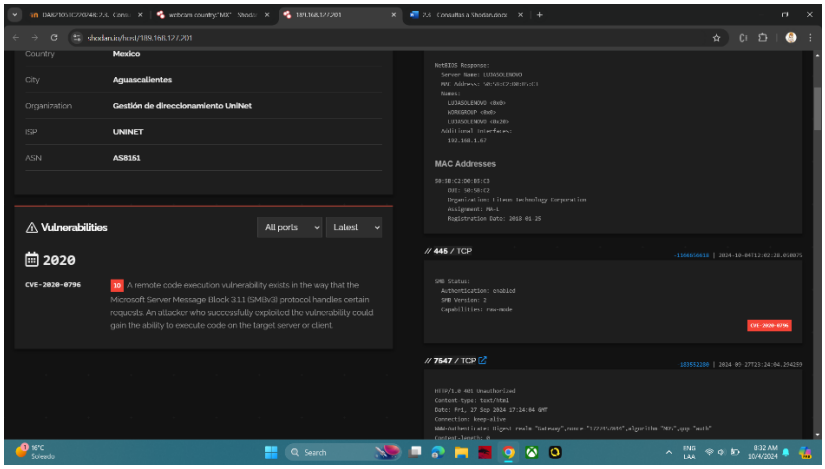
La plataforma fue creada por John Matherly en 2009 y se ha convertido en una herramienta popular en el campo de la ciberseguridad y la investigación en Internet. Shodan utiliza una amplia gama de servicios y protocolos, como HTTP, HTTPS, FTP, SSH, SNMP, entre otros, para rastrear y catalogar dispositivos que están conectados y son accesibles públicamente.

En esta práctica se documentan algunas consultas realizadas en este motor de búsqueda, así como las vulnerabilidades encontradas para cada uno de los casos encontrados y gravedad de cada uno de estos.

Shodan es una herramienta poderosa de búsqueda y análisis para dispositivos conectados a Internet que permite a los usuarios descubrir información y posibles vulnerabilidades en sistemas y dispositivos expuestos. Aunque inicialmente fue diseñada con fines legítimos, como ayudar a los administradores de sistemas a identificar y proteger posibles debilidades en sus redes, también puede ser utilizada de manera maliciosa por actores malintencionados para llevar a cabo ciberataques.

Webcam:

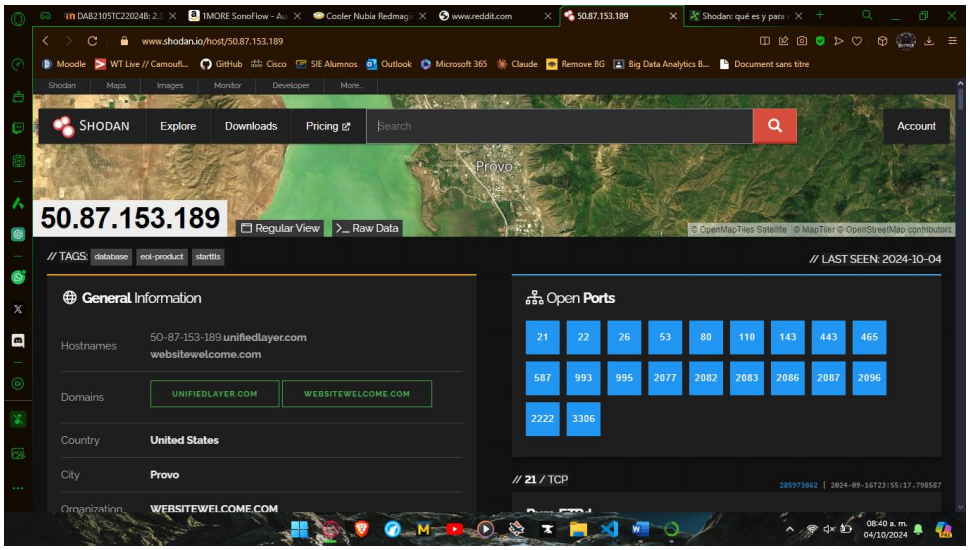


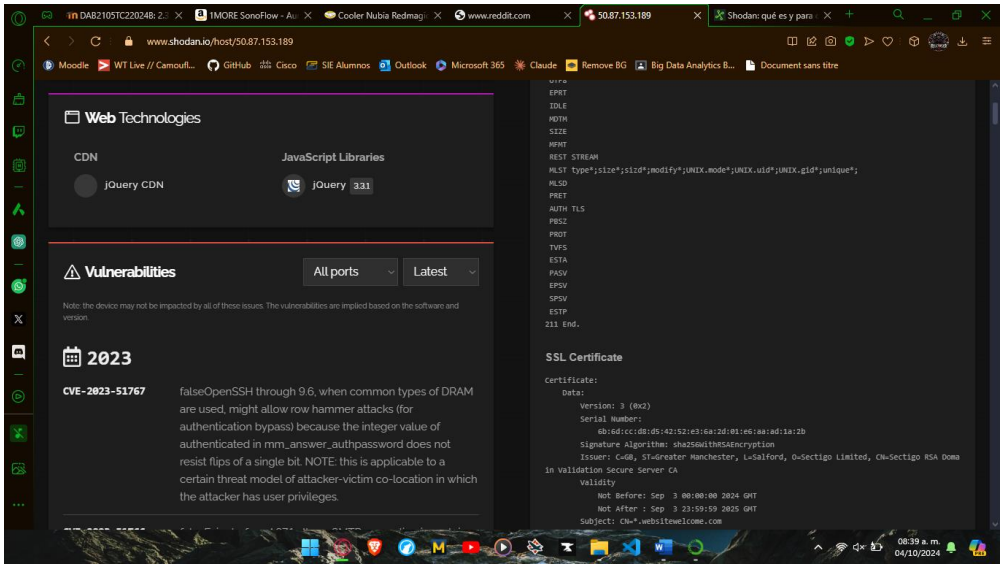


CVE-2020-0796:

- **Nombre común:** Vulnerabilidad SMBGhost
- **Descripción:** Esta vulnerabilidad afecta al protocolo de comunicación **SMBv3** en Windows, utilizado para compartir archivos e impresoras a través de una red. La falla se encuentra en la funcionalidad de compresión de SMBv3 y permite que un atacante no autenticado ejecute código de manera remota en el sistema vulnerable sin necesidad de interacción del usuario.
- **Impacto:** Un atacante puede enviar paquetes maliciosos al servidor SMB3 y obtener control total del sistema afectado, lo que resulta en la ejecución remota de código (RCE). Si se explota correctamente, esto podría permitir a un atacante propagar malware o ransomware (como el caso de WannaCry en el pasado).
- **Solución:** Microsoft lanzó parches de seguridad para mitigar este problema. Se recomienda actualizar los sistemas operativos afectados y desactivar la compresión SMBv3 si no es necesaria.

Servidor apache:

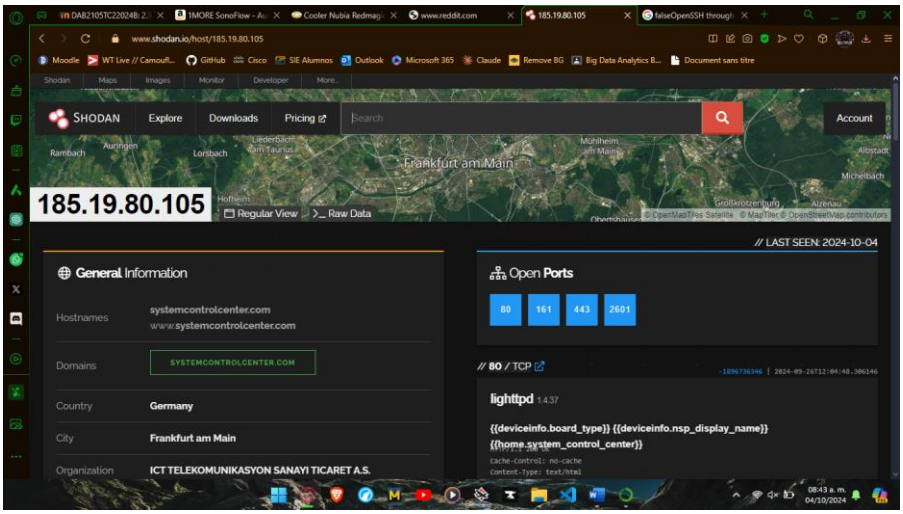


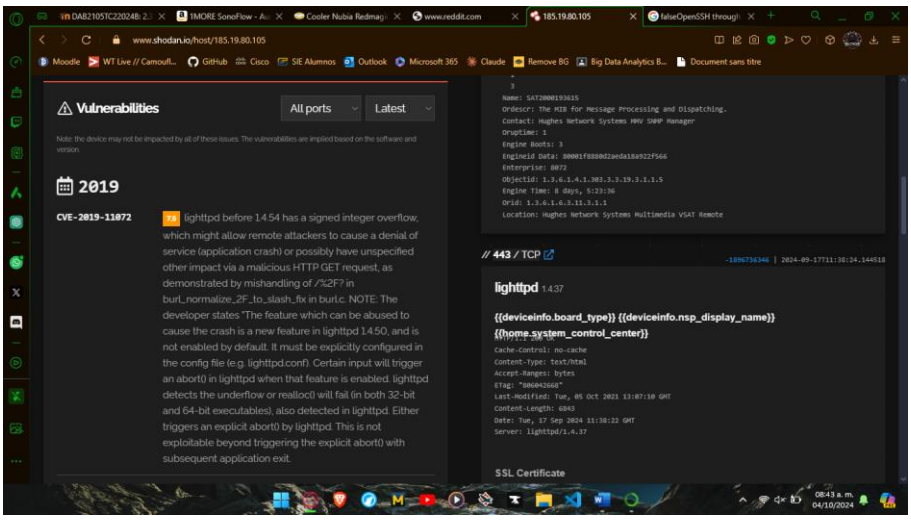


CVE-2023-51767:

- **Descripción:** Esta vulnerabilidad, de reciente descubrimiento en 2023, todavía tiene poca información pública disponible. Puede estar relacionada con un software específico o protocolo, pero actualmente no se han publicado suficientes detalles técnicos. Probablemente, está pendiente de una divulgación completa o pertenece a un entorno específico que aún no se ha explorado en profundidad.
- **Impacto:** La evaluación de impacto dependerá del tipo de vulnerabilidad (RCE, escalada de privilegios, etc.) y su vector de ataque.
- **Solución:** Mantente atento a actualizaciones y parches de seguridad publicados por los responsables de la tecnología o software afectado.

Vsat:

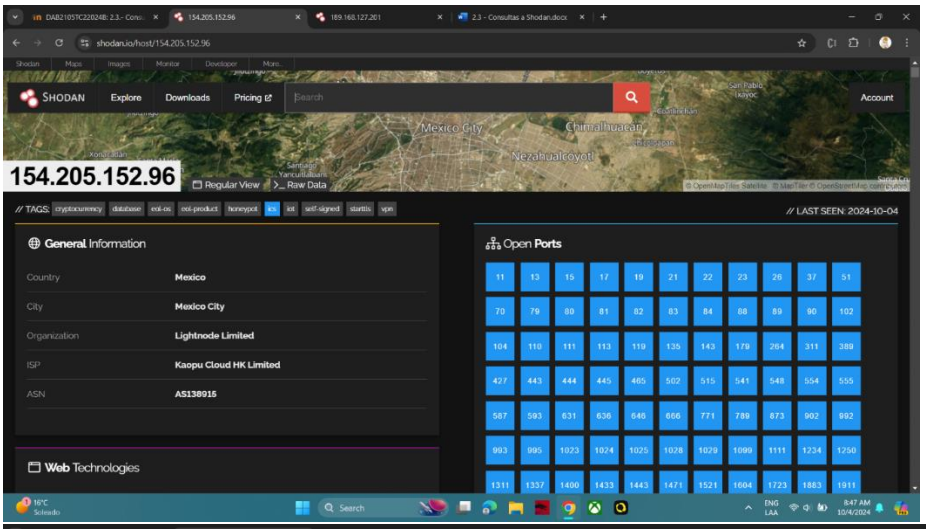


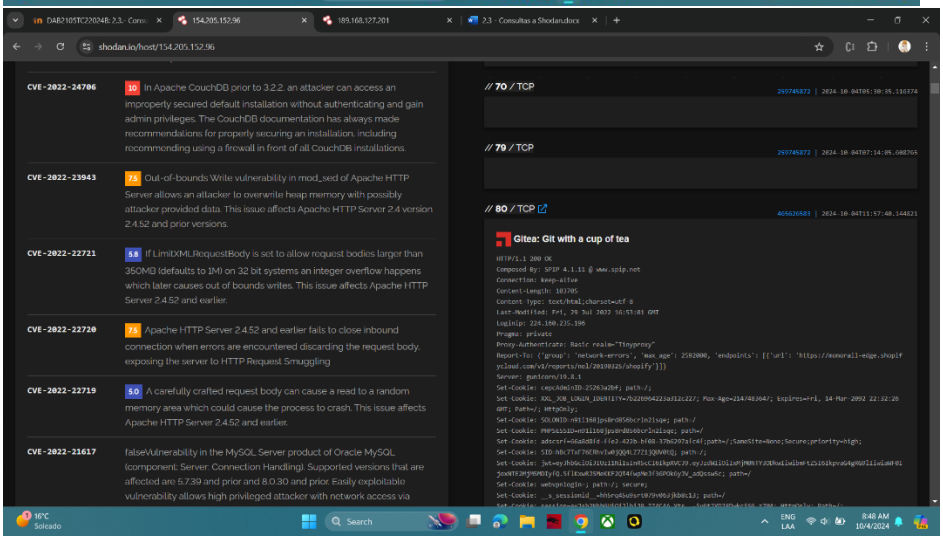


CVE-2019-11072:

- **Descripción:** Esta vulnerabilidad afecta al software **phpMyAdmin**, una herramienta de administración web para bases de datos MySQL. El problema radica en una falla de seguridad que permite a los atacantes llevar a cabo un **ataque de cross-site scripting (XSS)**, lo que facilita la inyección de scripts maliciosos que podrían afectar la integridad y confidencialidad de la base de datos.
- **Impacto:** Un atacante podría aprovechar esta vulnerabilidad para ejecutar scripts en el navegador de un administrador autenticado, robando información sensible o realizando cambios no autorizados en la base de datos.
- **Solución:** Se debe actualizar a la versión más reciente de phpMyAdmin que haya corregido esta vulnerabilidad.

Web site:

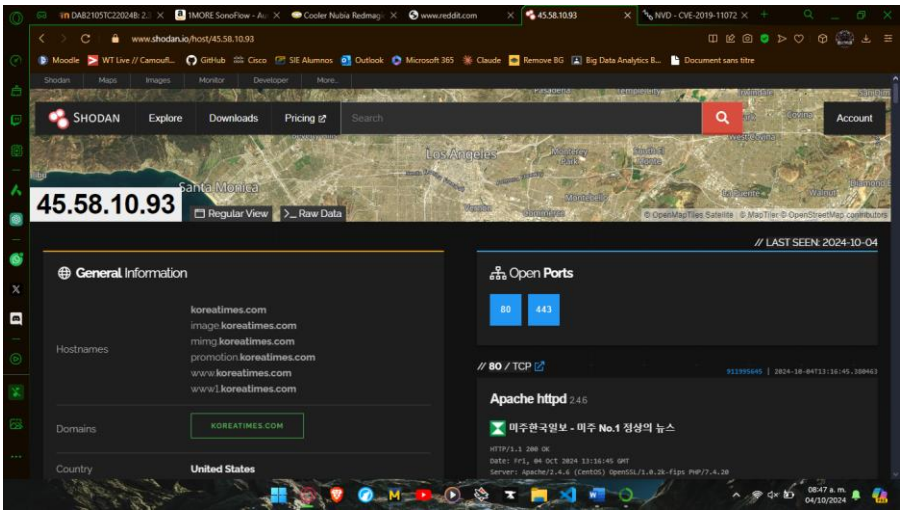


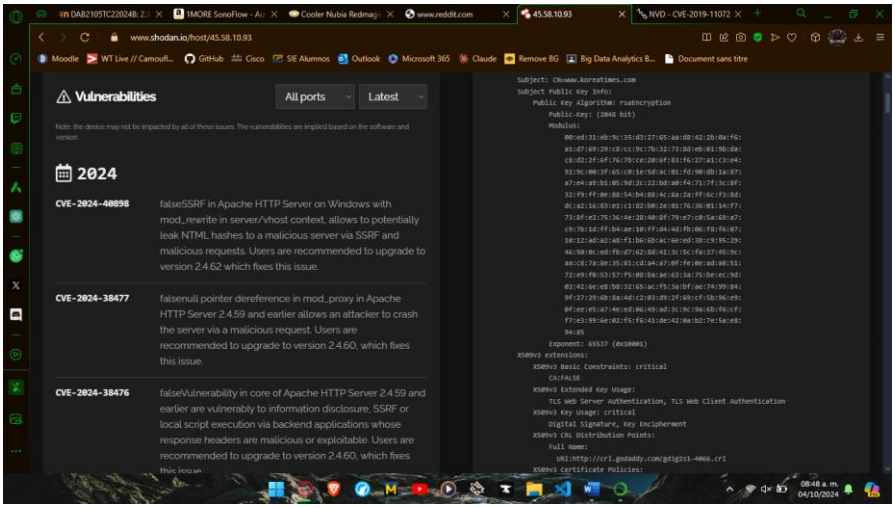


CVE-2022-24706:

- **Descripción:** Esta vulnerabilidad afecta a **Spring Framework**, un popular marco de trabajo en Java. Específicamente, la vulnerabilidad se encuentra en el componente de **Spring Cloud Gateway**, que permite la manipulación no autorizada de solicitudes HTTP.
- **Impacto:** Permite la explotación de un **ataque de Server-Side Request Forgery (SSRF)**, lo que podría permitir a un atacante enviar solicitudes desde el servidor afectado a otros servicios en la red interna o externa. Esto puede llevar a la exposición de información sensible o incluso a ataques de escalada en la red.
- **Solución:** Spring lanzó actualizaciones para mitigar este problema. Se recomienda actualizar el componente afectado y revisar la configuración de seguridad del entorno.

Smartphone:





CVE-2024-40898:

- **Descripción:** Esta vulnerabilidad corresponde a una falla de seguridad descubierta en 2024, pero al igual que CVE-2023-51767, no hay mucha información pública disponible aún sobre ella. Dado que se trata de una vulnerabilidad reciente, es posible que se encuentre en proceso de análisis y que más detalles se publiquen en un futuro cercano.
- **Impacto y Solución:** Sin información clara sobre el tipo de ataque o tecnología afectada, es importante estar pendiente de los informes de seguridad y las actualizaciones de software asociadas para mitigar cualquier riesgo potencial.

Conclusión

El uso de Shodan como herramienta de búsqueda para identificar dispositivos conectados a internet expone de manera clara las vulnerabilidades asociadas a cada tipo de sistema explorado. Durante la práctica, al buscar dispositivos como webcams, servidores Apache, VSAT, websites y smartphones, se reveló el riesgo latente de la falta de configuraciones seguras o actualizaciones, lo que deja abierta la posibilidad de ataques maliciosos.

Cada dispositivo presenta diferentes niveles de peligrosidad. Las webcams, por ejemplo, suelen estar expuestas a accesos no autorizados que comprometen la privacidad de los usuarios. Los servidores Apache, si no son actualizados y configurados correctamente, pueden ser vulnerables a ataques como la inyección SQL o cross-site scripting (XSS), lo que permite a los atacantes obtener el control del servidor. Las redes VSAT, al ser utilizadas en comunicaciones críticas, pueden ser explotadas para interceptar datos sensibles, mientras que los smartphones y websites expuestos pueden ser blanco de ataques que comprometan tanto la seguridad personal como la integridad de la información almacenada.

El conocimiento de estas vulnerabilidades resalta la importancia de la implementación de prácticas de ciberseguridad robustas, como la actualización constante de software, la protección de accesos con contraseñas seguras y la utilización de protocolos de cifrado. En definitiva, la detección temprana de estas debilidades mediante herramientas como Shodan permite no solo entender la magnitud del riesgo, sino también fortalecer las defensas frente a posibles ataques.

Referencias

Fernández, Y. (2022, 18 julio). *Shodan: qué es y para qué se puede usar este buscador de dispositivos conectados a Internet*. Xataka. https://www.xataka.com/basics/shodan-que-se-puede-usar-este-buscador-dispositivos-conectados-a-internet

Michel, D. (2023, 7 agosto). Shodan 101: A step-by-step beginner's guide - Diego Michel - Medium. *Medium*. https://medium.com/@digomic_88027/shodan-101-a-step-by-step-beginners-guide-83079332e2dd

Shodan. (s/f). Shodan. Recuperado el 4 de octubre de 2024, de https://www.shodan.io