

Tarea 4: Shodan*

David Steven Solís Sosa, 202001569**

Shodan es una herramienta utilizada en el ámbito del hacking ético para identificar dispositivos y servidores conectados a Internet. A diferencia de los buscadores tradicionales, permitió explorar puertos y servicios expuestos, revelando configuraciones, versiones de software y credenciales predeterminadas. Su uso fue clave para detectar vulnerabilidades en sistemas mal configurados o con credenciales débiles, ayudando a reforzar la seguridad antes de que pudieran ser explotadas por atacantes.

I. OBJETIVOS

A. General

1. Conectarse a servidores con poca seguridad y conscientizar lo vulnerable que uno está al configurar mal un servidor.

B. Específicos

el papel de Shodan en el hacking ético, destacando su uso para pruebas de seguridad y auditorías en organizaciones. Identificar las principales vulnerabilidades que Shodan ha revelado en sistemas con configuraciones débiles o credenciales predeterminadas.

II. IMÁGENES DE SHODAN

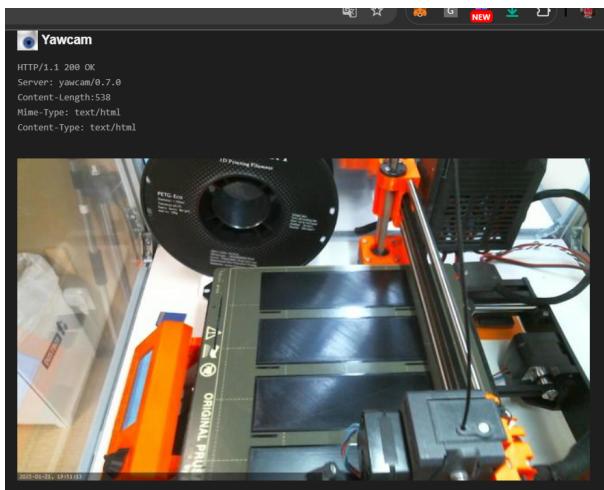


Figura 1: Webcam de una Impresora 3D ubicada en Japón

Fuente: Elaboración Propia, 2024.

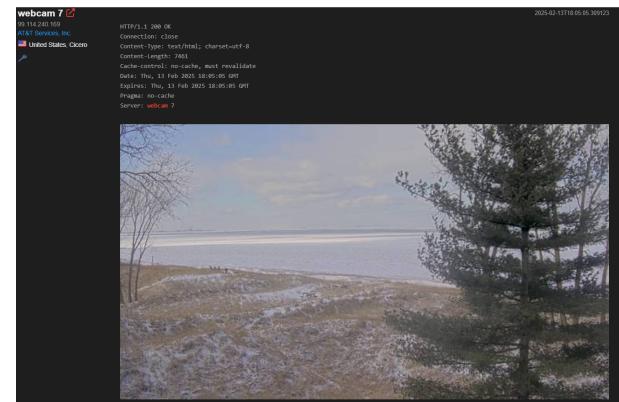


Figura 2: Webcam de un sistema de monitoreo ambiental en Estados Unidos

Fuente: Elaboración Propia, 2024.



Figura 3: Webcam advirtiendo que cazar a renos usando comida como anzuelo es ilegal

Fuente: Elaboración Propia, 2024.

* Telecomunicaciones y Redes Locales

** e-mail: 3021729200101@ingenieria.usac.edu.gt

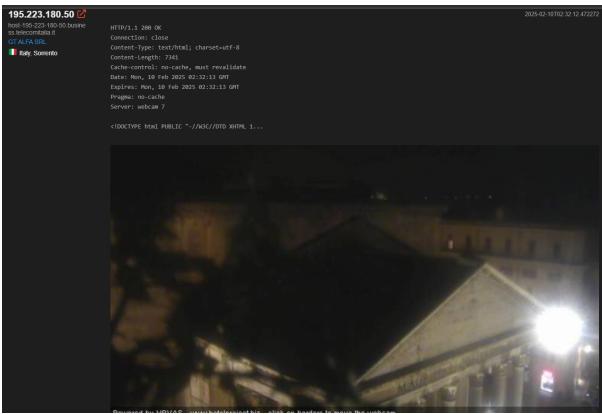


Figura 4: Cámara de Monitoreo de un edificio ubicado en Italia

Fuente: Elaboración Propia, 2024.



Figura 5: Webcam monitoreando el nido de un pájaro en Hungría

Fuente: Elaboración Propia, 2024.

III. RECOMENDACIONES

- Implementar credenciales seguras: Se recomienda cambiar las contraseñas predeterminadas en servidores y dispositivos conectados a Internet para evitar accesos no autorizados detectados por Shodan..
- Actualizar y fortalecer la configuración de seguridad: Es fundamental mantener los sistemas operativos, aplicaciones y firmware actualizados, además de configurar correctamente los servicios expuestos para reducir vulnerabilidades.
- Fomentar la concienciación sobre ciberseguridad: Es importante capacitar a los administradores de sistemas y usuarios sobre los riesgos de la exposición de datos en Internet y las mejores prácticas para mitigarlos.

IV. CONCLUSIONES

- Shodan es una herramienta poderosa que permite identificar dispositivos y servidores expuestos en Internet, facilitando tanto la detección de vulnerabilidades como su posible explotación.
- Las principales vulnerabilidades detectadas a través de Shodan están relacionadas con credenciales débiles, configuraciones incorrectas y versiones de software desactualizadas, lo que resalta la importancia de una gestión adecuada de la seguridad en servidores y dispositivos conectados.
- Si bien Shodan es útil para la seguridad, también representa riesgos, ya que los mismos datos que ayudan a fortalecer sistemas pueden ser utilizados por actores malintencionados para llevar a cabo ataques.