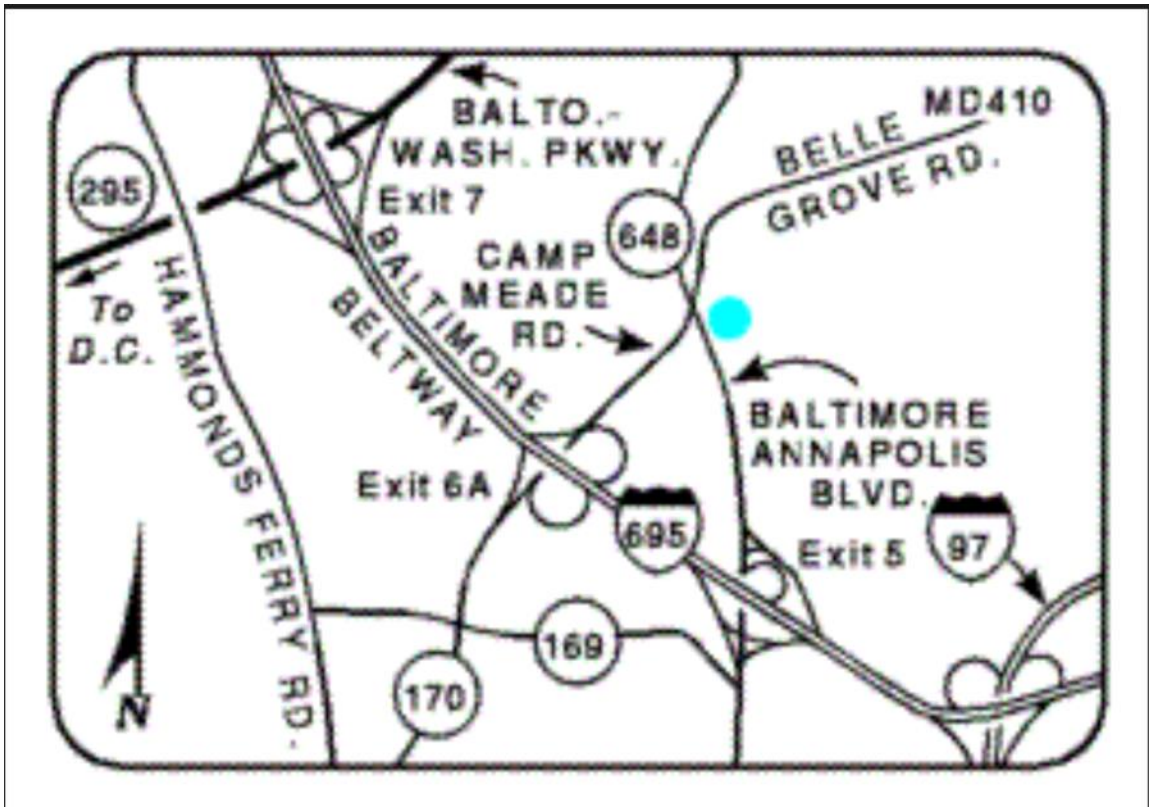
Reto 3: Información sobre esta imagen

Antes de comenzar, cabe resaltar que la página web de esta imagen ya no existe. No obstante, a través de WayBackMachine, he tratado de resolver las tareas propuestas.

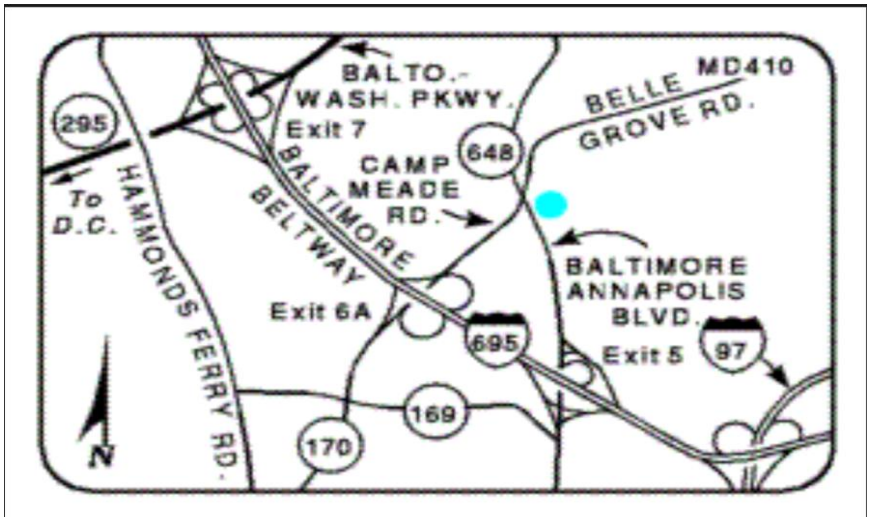


Task 1: What is the originating website? (¿Cuál era la página web original?)

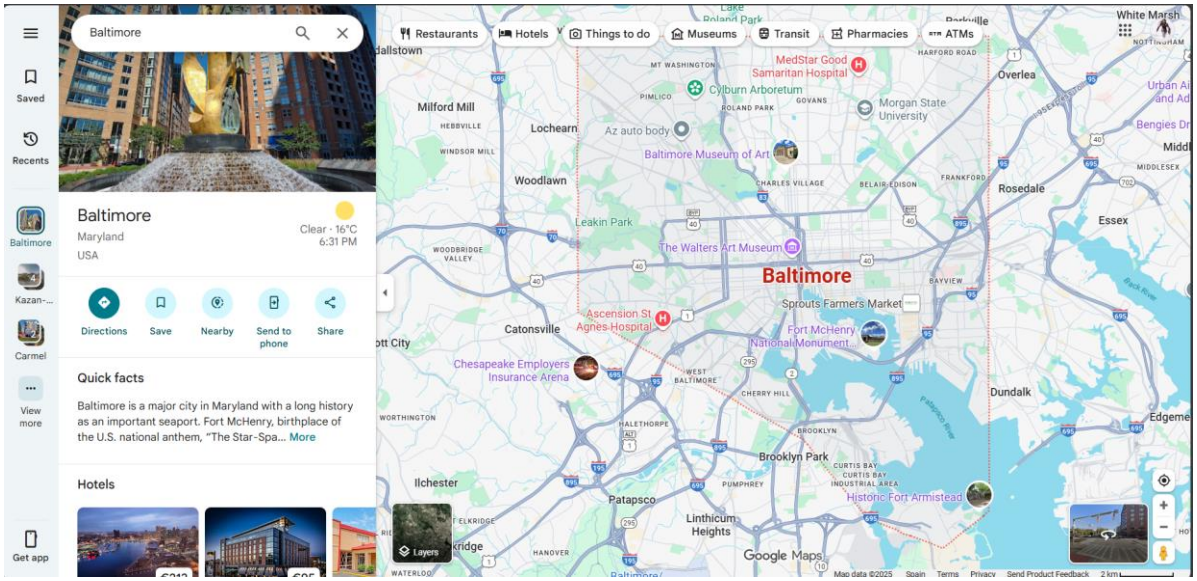
Para este enunciado, gracias al mapa que tenemos, voy a averiguar dónde está y de qué lugar se trata (un hotel, una oficina, un restaurante, etc). Puesto que, tal y como he mencionado antes, la página web de este sitio ya no existe, voy a intentar usar una alternativa a la búsqueda inversa de imagen, la cual sólo nos podría conducir a un sitio de la ESCS donde está el reto original solucionado y no nos interesa.

Así que, lo que he hecho en su lugar ha sido tratar de averiguar la ubicación a través del mapa, de donde estuviese este sitio que ya no existe.

Como podemos ver en el mapa, hay bastantes carreteras con el nombre de Baltimore, así que podemos intuir que debe ser el nombre de una ciudad o pueblo. Y las siglas MD es posible que identifiquen un estado de EEUU, ya que allí los estados se suelen simplificar con siglas de dos letras (NV Nevada, CA California, etc). Así probablemente MD se trate de algún estado.



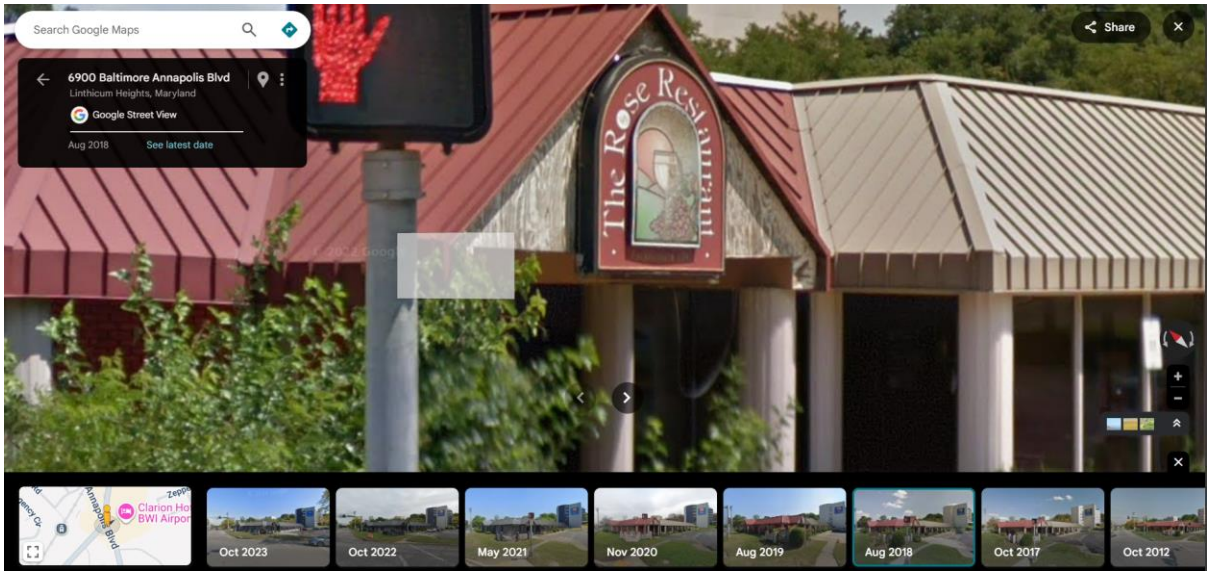
Y efectivamente, así ha sido. Buscando “Baltimore, MD” En Google Maps, resulta que hay una ciudad llamada Baltimore en el estado de Maryland, el cual para ser sincero desconocía de su existencia. Creo que debe ser de los únicos estados que no conocía.



Desde el Aeropuerto de Baltimore, siguiendo un poco las carreteras del mapa, he encontrado la zona donde podía estar el sitio, guiándome en el mapa original.

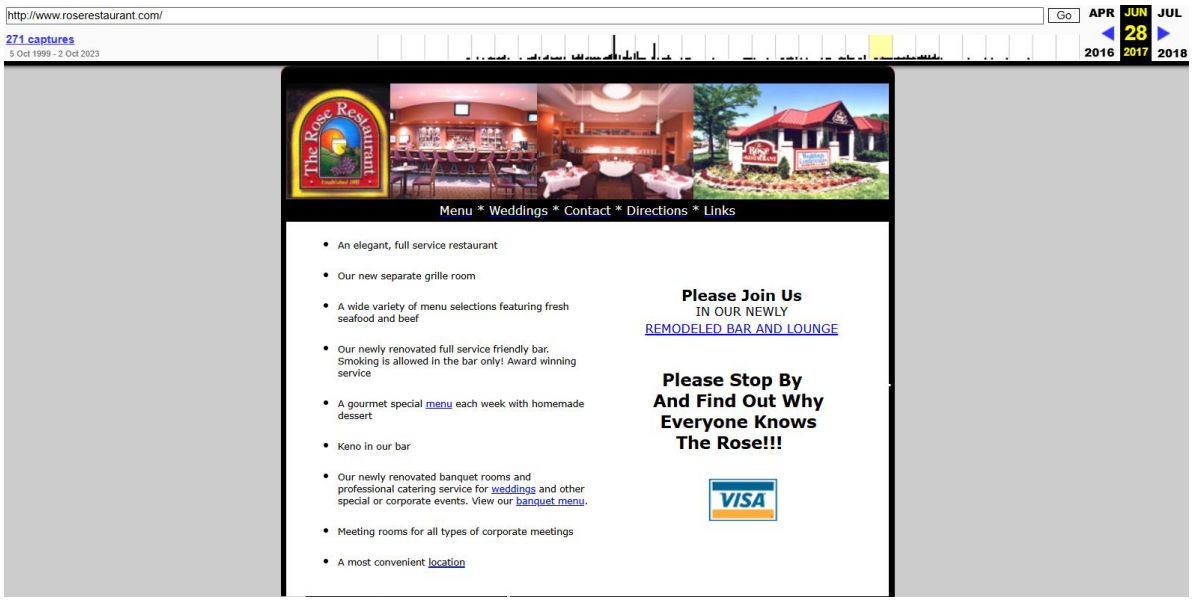
Si en StreetView vemos la zona, podemos ver que hay un restaurante actualmente llamado “9Five Kitchen & Bar”, que tienen página web.

Pero.. En esa página web, no hay ni rastro del mapa… Así que… ¿y si viajamos al pasado? ¿Y si vamos por ejemplo al 2018 en Street View y comprobamos si ese restaurante lleva ahí desde entonces?

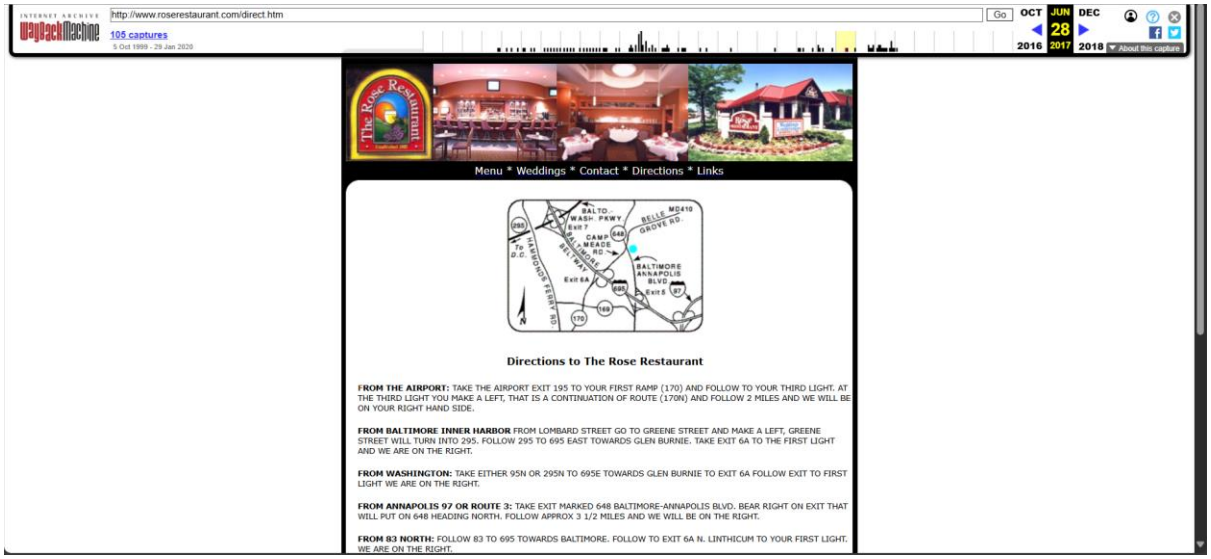


Pues, resulta que ese sitio antes se llamaba de otra manera, Rose Restaurant. Si estuviésemos en el 2018, podríamos visitar su página web a comprobar si el mapa aparece, pero como es el caso, tendremos que recurrir a WaybackMachine.

Vamos a imaginar que estamos haciendo OSINT en el 2018 y en Google Maps accedemos a la página web de este sitio, roserestaurant.com

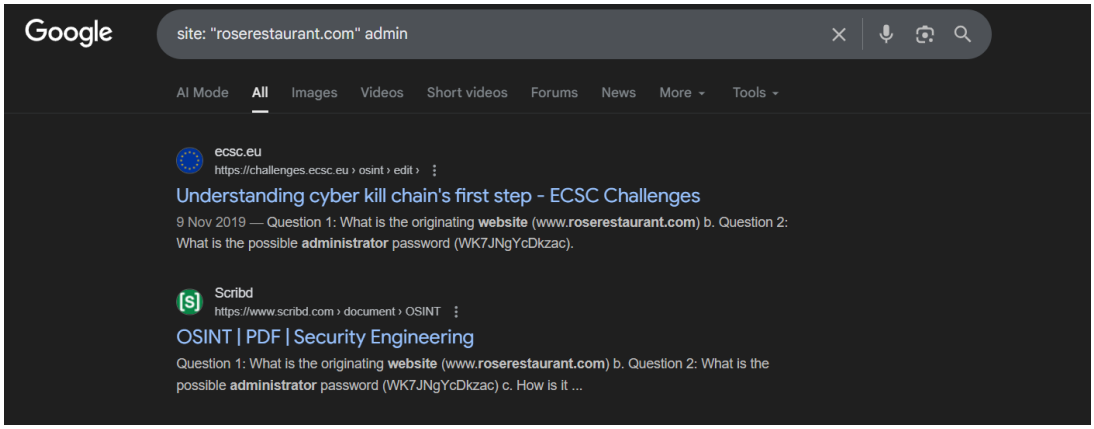


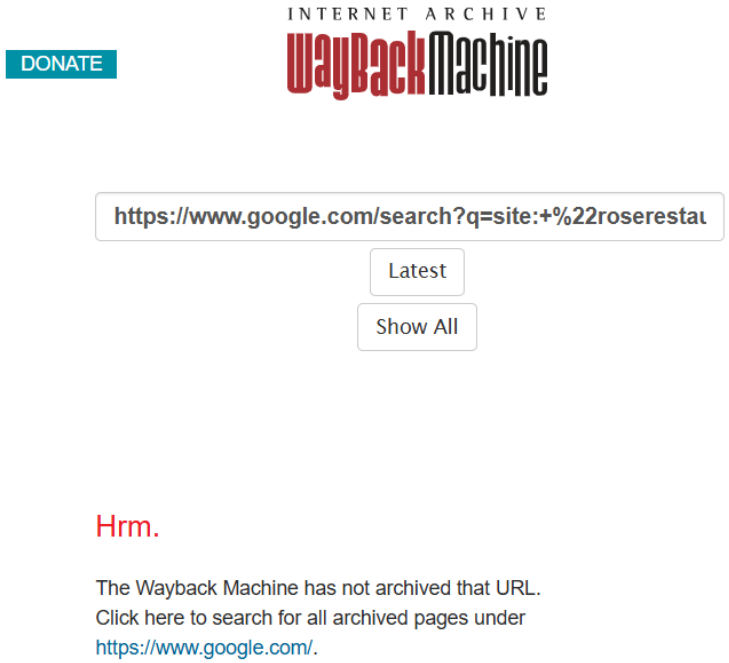
Podemos ver que hay una pestaña de Directions. Y si entramos en ella... Ahí lo tenemos, el mapa original. Así que podemos confirmar que, en efecto, el mapa pertenecía a roserestaurant.com



Task 2: ¿Cuál es probablemente la contraseña de administrador?

Desafortunadamente, ya no es posible intentar encontrar la contraseña de este sitio (porque partiendo de la base, ya no existe), y aunque intentásemos hacer búsquedas con Google Dorks en WayBackMachine, tampoco es posible encontrar nada. Una búsqueda con Google Dorks muy sencilla a probar en la época, hubiese sido **site: "roserestaurant.com" admin** , filtrando así por el dominio y el usuario admin por defecto.





Task 3: ¿Cómo es posible obtener información con los métodos OSINT?

Bueno, principalmente por toda la información pública que dejamos nosotros (nombres, edad, sitios que viajamos, etc). A poco que haya algo público nuestro, es relativamente sencillo emplear los motores de búsqueda (por ejemplo con el Dorking) para indexar todo aquello que hayamos hecho público, y recopilar información nuestra. Más allá de las filtraciones, los propios motores de búsqueda pueden llegar a indexar archivos de configuración o backups, por lo que a la mínima que haya algo suelto que no deba estarlo, es fácil que alguien encuentre la manera de atacarnos.

Task 4: ¿Qué google dorks se utilizan para descubrir información relevante?

Unos de los más útiles para encontrar información privilegiada serían

-site: que restringe para un dominio en específico (como roserestaurant.com)

-intitle: que busca que esté la palabra específica en el título de la página (por ejemplo, database, o password)

-intext: Como intitle, pero que esté en el propio texto de la página en vez del título (por ejemplo username, email, password)

-filetype: Para filtrar por tipo` de archivo, para buscar PDFs comprometidos por ejemplo

-Y los operadores lógicos OR y AND para ayudar con el filtrado

Task 5: ¿Puedes usar la contraseña obtenida para investigar el problema?

Sin permiso explícito del restaurante, no, no podemos. En todo deberíamos informar a los del restaurante y explicarles la situación, y si ellos lo consideran oportuno, que nos "contraten" a nosotros para ocuparnos de investigarlo más a fondo.

Task 6: ¿Dónde se encuentra la contraseña de Administrador?

En _vti_private/service.pwd

Task 7: ¿Qué funcionalidad permite al atacante descubrir la contraseña de administrador?

Que el archivo está expuesto de forma pública cuando no debería estarlo, y que los motores de búsqueda son capaces de indexarlo con los filtros correctos.

Task 8: ¿Cómo podrías resolver este incidente?

Lo primero y más importante sería restringir las rutas delicadas como la carpeta _vti-private para que no puedan accederse desde fuera, sólo desde local o por ssh/rdp. Y si no fuese posible, por lo menos bloquear el acceso externo con autenticación o reglas (para que muestre el ERROR: FORBIDDEN ante un intento acceso no autorizado), y evitar también que los backups puedan estar expuestos (que suelen ser puntos de vulnerabilidad comunes indexados de manera pública).

Y además y no por ello menos importante, hacer auditorías periódicamente para asegurarse de que no haya vulnerabilidades expuestas (como esta, durante muchos años además)