WRITEUP: Un detective y medio
Categoría: Osint

Enunciado

Un grupo de detectives de inteligencia tiene planeada una operación de intervención conductual. Hemos descubierto que recurrirán a la distribución de propaganda con tal de moldear el contexto socio-económico a favor de unos ideales determinados. Utilizarán para ello una red social en concreto. Para ello, emplearán la conocida **Falacia de la verdad a medias** como método y estrategia de manipulación social, en la cual se presenta algo creíble y se toma eso como buena razón para creer que el resto de la información es verdadera. Nuestra misión será ponernos el traje de detectives e investigar la verdad a través de estas mentiras. Al parecer, la página web de SUGUS esconde algo de información confidencial sobre todo este entramado. ¿Serás capaz de resolver el caso?

Resolución

El primer paso será interpretar la falacia de la verdad a medias, e informarse en qué consiste. Aún así, el propio enunciado lo resume de forma bastante precisa y concisa. Queda en labor del concursante indagar algo más si lo desea, sin ser esto necesario.

El siguiente paso puede ser 'ir al grano' e investigar bajo la web de SUGUS que información se puede ocultar. Esto podría hacerse de forma manual visitando `https://sugusuva.es` y navegando por las diferentes páginas.

Otro método más efectivo puede ser enumerar el *sitemap* de la web de SUGUS mediante Google Dorks o métodos similares, como por ejemplo mediante la búsqueda:

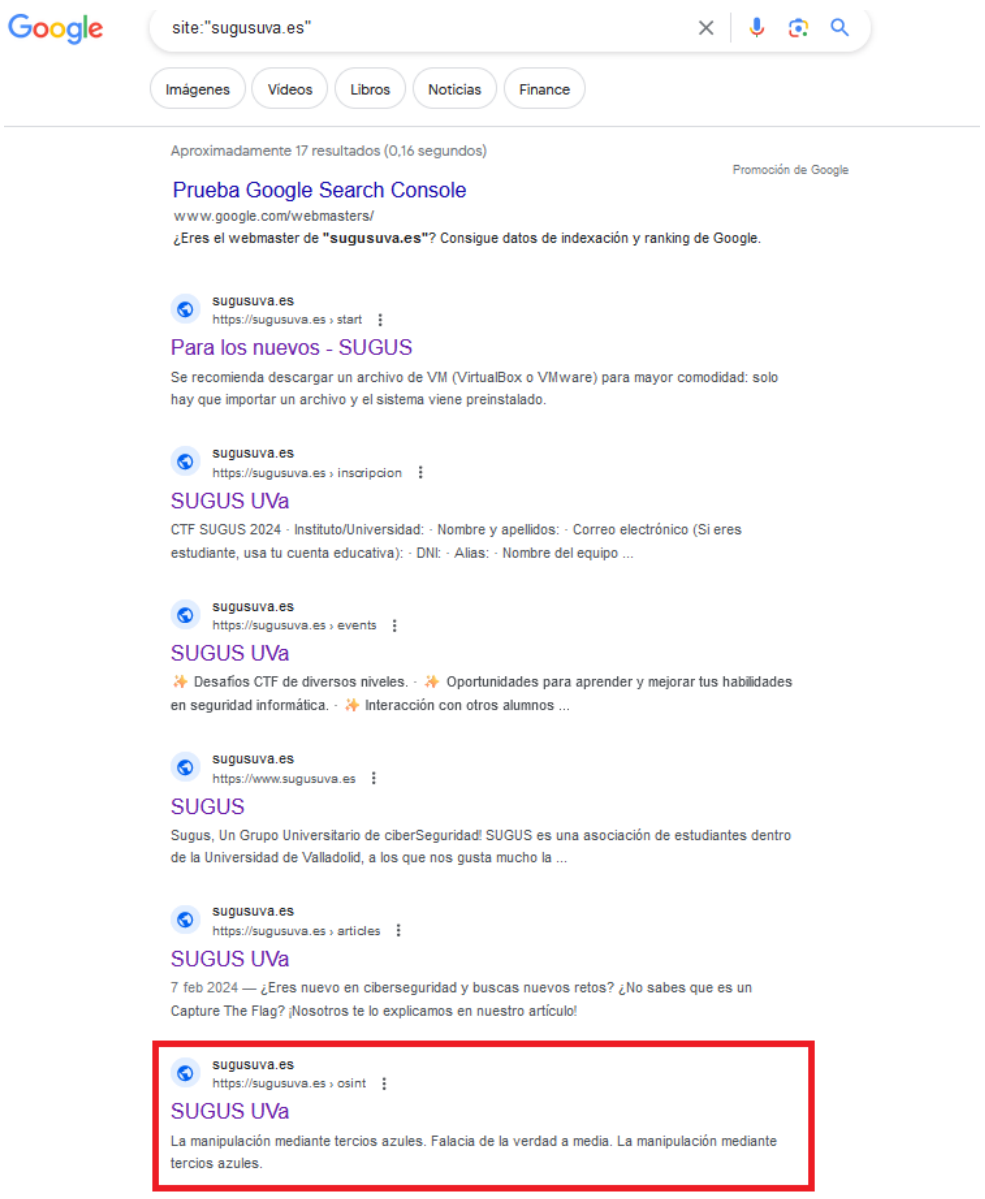


Figura 1: Análisis web SUGUS mediante Google Dorks

Una vez accedemos a `https://sugusuva.es/osint` observamos una breve introducción, con el título de la página como "FALACIA DE LA VERDAD A MEDIAS". Nos encontramos con 3 publicaciones de información encontrada por nuestros detectives. Dos de ellas contiene algún tipo de puntualización o afirmación que puede corroborarse.

En el caso de la primera publicación, la parte de "Además, según señaló Aasheesh Pittie, los pájaros como mascota son capaces de alertarte de ciertos peligros, como el exceso de gases contaminantes en zonas urbanas. Los ingleses llaman a este tipo de situaciones "Canary in the coal mine"." , podría corroborarse con búsquedas sencillas en Google. Evidencia:

`https://india.mongabay.com/2018/10/interview-urban-birds-can-be-the-ideal-canary-in-the-mine-i`

Además, la expresión en inglés también es verídica:

`https://share.america.gov/english-idiom-canary-coal-mine/`

En el caso de la segunda publicación, nos iríamos a la cita de "Según Damon Wise, "Esta sofisticada fantasía de animación adopta un enfoque macabro que incluso Collodi encontraría un poco excesivo. Con búsquedas sencillas de dicha cita y sus relaciones, se puede encontrar la siguiente evidencia:

`https://www.filmaffinity.com/es/pro-reviews.php?movie-id=563328`

Además, el thriller también es verídico:

`https://www.eldiario.es/cultura/pinocho-disney-guillermo-toro-viaje-xenofobia-antifascismo_1_9737385.html`

Por tanto, parece que tenemos dos publicaciones verdaderas. La tercera es falsa. No contiene ninguna cita que pudiera corroborarse, y habla de una ley de bienestar para permitir tener canarios, además de un tono coloquial y con cierto toque o intento de humor. Esta publicación falsa es el paso correcto en el reto, ya que la propia falacia de la verdad a medias trata precisamente de eso: en este caso, de intentar 'colar' la tercera afirmación (publicación) como una verdad.

Tenemos 3 detectives pues. Alguien podría pensar ya que el detective con la información secreta es Raymond C. Schindler. Estaría en lo correcto. Aún así, si se anduviese algo perdido en el reto, la investigación de las redes sociales podría realizarse sobre los tres.

A continuación queda una tarea libre de métodos y herramientas sobre investigación de las redes sociales de dichos detectives. Lo normal podría ser revisar Twitter, Facebook, Instagram, etc. El enunciado afirma que se empleará una única red social. La red social adecuada es Twitter, por lo que si se detecta un perfil acorde en cualquiera de las redes sociales mencionadas, ya sabremos que esa red es la indica.

Los perfiles de los detectives se pueden lograr con una búsqueda simple de sus nombres:

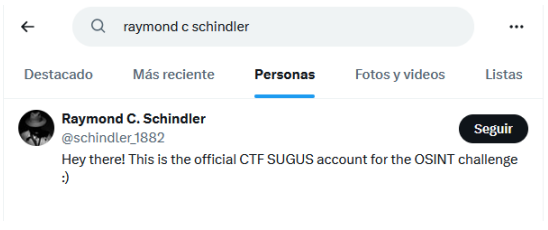


Figura 2: Perfil Raymond C. Schindler

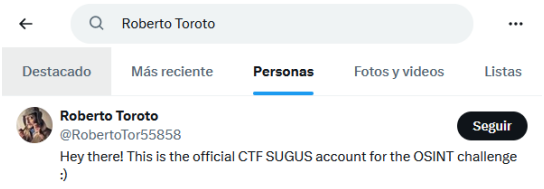


Figura 3: Perfil Roberto Toroto

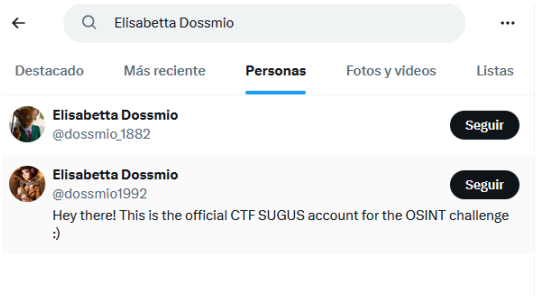


Figura 4: Perfil Elisabetta Dossmio

Observamos que en su primer tweet, tanto Elisabetta como Roberto escriben lo siguiente:

`I'm sorry, but I am not the princess you are looking for`

Mientras que Raymond S. Schindler escribe lo siguiente:

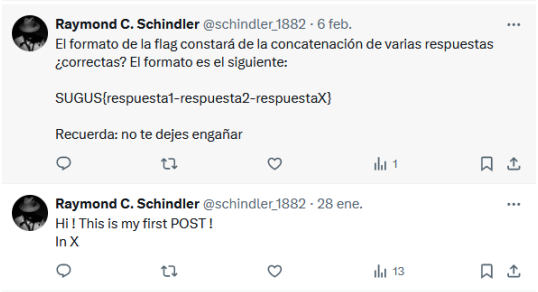


Figura 5: Información inicial

Además, Elisabetta y Roberto no existen como detectives en la vida real, mientras que Raymond C. Schindler sí. Nótese que debemos leer los tweets de más antiguos a más recientes. Nos dice que posee la flag, y que se construye mediante un determinado formato, pero respondiendo a preguntas tipo test. Más adelante se comprobaría que hay dos respuestas verdaderas y una falsa, por cada pregunta. Adivinen qué. La respuesta que buscamos es la falsa para construir nuestra flag, ya que se sigue el hilo de la falacia de la verdad a medias, prosiguiendo también con la regla concreta de 2 verdades y 1 mentira que ya nos hemos encontrado en las publicaciones de los detectives previamente.

Las respuestas correctas (las mentiras) de cada pregunta, pueden encontrarse en la siguiente documentación, la cual es fácilmente identificable en búsquedas de Google sobre el detective Raymond C. Schindler:

`https://gavinreese.com/2020/07/10/raymond-c-schindler/`

`https://authorjenniferchase.com/2016/01/09/3-amazing-detectives-who-impacted-history/`

`https://rqinvestigations.com/private-investigations/famous-private-investigators-list-favorites`

`https://www.yurtopic.com/society/history/solving-biggest-cases.php`

La flag resultante es la siguiente:

```
SUGUS{Ontario-1965-carnicero-smartphone-presidencia}
```