***Fuente**: Bing Chat AI*

INSTRUCCIONES PARA LOS TRABAJOS EN GRUPO

DEPARTAMENTO DE INFORMÁTICA. UNIVERSIDAD DE OVIEDO

Seguridad de Sistemas Informáticos | 2023 – 2024 (V4.0 *"S-81 Isaac Peral"*)

Contenido

Objetivo del trabajo de la asignatura

El trabajo de la asignatura es hacer **un documento PDF** que describa los pasos que habéis dado para realizar el trabajo que se os ha pedido, **basado en capturas de pantalla** y en **explicar qué habéis hecho** para obtener el resultado mostrado en las capturas. Podéis pensar en hacerlo como una especie de explicación paso a paso de los resultados que os van saliendo en las imágenes, incluyendo lo que habéis hecho para que os salga, como los KT de prácticas.

No hay límite de hojas, aunque se recomienda **que se trate de ser conciso en la medida de lo posible**, e ir al grano en las explicaciones. El objetivo es destacar la información qué habéis encontrado y para qué podría usarlo "un malo/a" 😊.

Material disponible

Dado que todos **los trabajos son de investigación usando datos de fuentes abiertas (OSINT)**, se os entrega un documento de ayuda para hacer los trabajos, que ya está disponible en campus de la asignatura. Este documento (**A-21 "Poseidón"**) contiene toda la información que necesitareis (y alguna más 😊) para hacer esos trabajos, de forma que no tengáis que buscar demasiado cómo hacer ciertas cosas y centraros en hacerlas. Es un documento extenso que se ha creado con la intención de que os quede para el futuro, por lo que aunque tenga muchos contenidos, centraros sólo en aquellos que son relevantes para vuestro trabajo.

Obviamente, siempre que se cumplan las normas establecidas en la próxima sección, podéis usar cualquier otra técnica o herramienta que os encontréis o consideréis oportuna.

Trabajos propuestos

Los trabajos están sujetos a unas normas, **están divididos en modelos,** y cada modelo tiene un **código**. Por favor, mirad bien el código que os ha tocado en el documento de asignación de grupos a trabajos para saber exactamente qué trabajo tenéis que hacer.

Normas

Todos los trabajos propuestos tienen las siguientes **normas obligatorias**..

- "***Do not engage***": Está terminantemente prohibido **interactuar con personas** que puedan ser objetivo de una investigación a consecuencia de tu trabajo. **Incluso bajo una identidad falsa**. Siempre deben ser **técnicas pasivas de descubrimiento**. Sabemos que el documento tiene descripciones de técnicas activas, pero se incluyen para vuestra formación posterior y por si algún día fuerais víctimas de ellas. **No uses ese conocimiento para interactuar, ni por supuesto dañar, a otros**.
    - A modo de ejemplo, se consideran **técnicas aceptables** en cualquier web
        - Navegar normalmente por una web con un navegador cualquiera
        - Examinar los contenidos de una web con proxys HTTP como *Burp* o las herramientas del desarrollador del navegador
        - Duplicar una web en tu disco duro para hacer análisis *offline* de sus contenidos
        - Examinar las propiedades y los contenidos de cualquier archivo público enlazado en la web
        - Provocar errores 404 navegando a páginas que sabes que no existen
        - Probar URLs manualmente para ver si existen
    - Se consideran **técnicas inaceptables** contra webs que no sean vuestras
        - En general, cualquier técnica que implique un gran nº de peticiones en un corto periodo de tiempo con el objeto de probar la validación de datos del sistema o cualquier otra razón.
        - *Fuzzing*, enumeración de directorios, prueba automatizada de vulnerabilidades, etc. No es además el objetivo de este trabajo hacer esta clase de tests, que siempre necesitan un contrato con un cliente para hacerlo legalmente.
        - Hacerles `nmap`
        - Probar *malware*, *exploits*, etc.
- "***Do not disclose***": Está terminantemente prohibido **publicar información sensible** con la que os hayáis podido encontrar. En vuestros trabajos, de encontrar información sensible, debe "**censurarse**" las capturas para que solo se vea una parte mínima de la misma de manera que no sea reconocible, pero sí que pruebe que habéis encontrado "cosas" (poned especial cuidado en el póster, por si pudiéramos exponerlo en el futuro).
- "***Do not harm***": Hacer daño directa o indirectamente a cualquier persona o entidad.

En estos trabajos es posible que no consigáis mucha información del objetivo que habéis elegido. Para ello os tenemos que decir lo siguiente:

- **Elegid bien el objetivo**: empezad por alguien o algo que veáis que tiene presencia en la red o es popular.

- **No se trata tanto de encontrar información, sino de desarrollar adecuadamente una investigación**: El objetivo es ejecutar técnicas de búsqueda correcta y razonadamente. Si no aparece nada o casi nada después de eso no es algo malo (¡bien por la entidad o persona investigada! 😊). En otras palabas, **el resultado de un trabajo puede ser perfectamente felicitar a alguien o a alguna entidad por gestionar bien su presencia en la red**.

Objetivos generales

Aunque cada investigación puede tomar vías distintas en función de lo que vayáis encontrando de cada persona o entidad estudiada, en general se trata de responder a estas cuestiones, aunque podéis añadir toda la información extra que consideréis relevante:

- Si la persona o entidad estudiada hace **un uso adecuado** de las redes sociales o, en general Internet, en el sentido de exponer demasiada información que se pueda usar potencialmente para algún fin malicioso.
- Si es fácil **identificar el "entorno"** de la persona o entidad estudiada, en el sentido de con quien está relacionada/asociada, con quien trabaja, etc., y si de ello crees que puede causar algún problema de seguridad al objetivo del estudio.
- Si crees que algo de lo que has encontrado **facilitaría un ataque de *spear phishing*** contra la persona o entidad estudiada (alguno de sus miembros), o un delito físico (robos, etc.).

Modelos de trabajos (elige uno)

Modelo de trabajo 1: Investigar a un político

Hacer una investigación con datos **exclusivamente de fuentes abiertas** y siempre **SIN contactar** con el investigado de ninguna forma (ver normas) **de alguien que elijáis vosotros** asociado a **algún partido político** (en la actualidad o en el pasado), ya sea a nivel nacional o regional.

- **MODEL1_POLIT_PSOE**: PSOE
- **MODEL1_POLIT_PP**: PP
- **MODEL1_POLIT_VOX**: VOX
- **MODEL1_POLIT_PODEMOS**: PODEMOS
- **MODEL1_POLIT_SUMAR**: SUMAR
- **MODEL1_POLIT_ERC**: ERC
- **MODEL1_POLIT_AST**: FORO ASTURIAS o cualquier diputado Asturiano

Modelo de trabajo 2: Investigar a un *streamer* Español

Hacer una investigación con datos **exclusivamente de fuentes abiertas** y siempre **SIN contactar** con el investigado de ninguna forma (ver normas) **de uno de estos *streamers***.

- **MODEL2_STREAMER_IBAI**: Ibai Llanos
- **MODEL2_STREAMER_ZELING**: Alicia Gonzáles Zeling
- **MODEL2_STREAMER_ILLO**: illojuan

- **MODEL2_STREAMER_NISSAXTER:** Nissaxter
- **MODEL2_STREAMER_AURON**: AuronPlay
- **MODEL2_STREAMER_PARACETAMOR:** Paracetamor
- **MODEL2_STREAMER_RUBIUS**: ElRubius
- **MODEL2_STREAMER_LITTLERAGER:** Littleragergirl
- **MODEL2_STREAMER_GREFG**: TheGrefg
- **MODEL2_STREAMER_MAYICHI:** Mayichi
- **MODEL2_STREAMER_JWILD**: Jordi Wild
- **MODEL2_STREAMER_CRISTININI:** Cristinini
- **MODEL2_STREAMER_DJMARIIO**: ERC

Modelo de trabajo 3: Investigar la presencia web de un sindicato

Hacer una investigación con datos **exclusivamente de fuentes abiertas** y siempre **SIN técnicas activas** (Ej.: `nmap`, ver normas) de una máquina, máquinas o servicios (Ej.: RRSS) que pertenezcan a la **infraestructura web** de algún **sindicato español**. La investigación puede incluir personas si a través de ellas se logra averiguar algún dato de la web estudiada, o es un proveedor o similar (alguien relevante) de la web.

- **MODEL3_WEBSINDICATO_CCOO:** Comisiones Obreras (CCOO)
- **MODEL3_WEBSINDICATO_UGT:** Unión General de Trabajadores (UGT)
- **MODEL3_WEBSINDICATO_USO:** Unión Sindical Obrera (USO)
- **MODEL3_WEBSINDICATO_CSIF:** Central Sindical Independiente y de Funcionarios (CSIF)
- **MODEL3_WEBSINDICATO_CGT:** Confederación General del Trabajo (España) (CGT)

Modelo de trabajo 4: Investigar a la infraestructura web de un partido político nacional

Hacer una investigación con datos **exclusivamente de fuentes abiertas** y siempre **SIN técnicas activas** (Ej.: `nmap`, ver normas) de una máquina, máquinas o servicios (Ej.: RRSS) que pertenezcan a la **infraestructura web** de algún **partido político español**. La investigación puede incluir personas si a través de ellas se logra averiguar algún dato de la web estudiada, o es un proveedor o similar (alguien relevante) de la web.

- **MODEL4_WEBPOLIT_PSOE**: PSOE
- **MODEL4_WEBPOLIT_PP**: PP
- **MODEL4_WEBPOLIT_VOX**: VOX
- **MODEL4_WEBPOLIT_PODEMOS**: PODEMOS
- **MODEL4_WEBPOLIT_SUMAR**: SUMAR

Modelo de trabajo 5: Investigar la presencia web de un partido político

Hacer una investigación con datos **exclusivamente de fuentes abiertas** y siempre **SIN técnicas activas** (Ej.: `nmap`, ver normas) de **una máquina, máquinas o servicios** (Ej.: RRSS) que pertenezcan a la **infraestructura web** de algún **partido político** ya sea a nivel nacional o regional. La investigación puede incluir personas si a través de ellas se logra averiguar algún dato de la web estudiada, es un proveedor o similar (alguien relevante) de la web.

- **MODEL2_WEB_PSOE**: PSOE
- **MODEL2_WEB_PP**: PP

- **MODEL2_WEB_VOX**: VOX
- **MODEL2_WEB_PODEMOS**: PODEMOS
- **MODEL2_WEB_CIUDADANOS**: CIUDADANOS
- **MODEL2_WEB_ERC**: ERC

Modelo de trabajo 6: Investigar la presencia web de un ayuntamiento

Hacer una investigación con datos **exclusivamente de fuentes abiertas** y siempre **SIN técnicas activas** (Ej.: `nmap`, ver normas) de una máquina, máquinas o servicios (Ej.: RRSS) que pertenezcan a la **infraestructura web** de algún **ayuntamiento Asturiano**. La investigación puede incluir personas si a través de ellas se logra averiguar algún dato de la web estudiada, o es un proveedor o similar (alguien relevante) de la web.

- **MODEL3_WEB_OVIEDO:** Oviedo
- **MODEL3_WEB_GIJÓN:** Gijón
- **MODEL3_WEB_AVILÉS:** Avilés
- **MODEL3_WEB_SIERO:** Siero
- **MODEL3_WEB_LANGREO:** Langreo
- **MODEL3_WEB_MIERES:** Mieres
- **MODEL3_WEB_CASTRILLÓN:** Castrillón

Modelo de trabajo 7: Investigar a un trabajador de una empresa relevante

Hacer una investigación con datos exclusivamente de fuentes abiertas y siempre **SIN contactar** con el investigado de ninguna forma (ver normas) **de alguien** que elijáis vosotros con **un puesto de alguna responsabilidad** asociado a **alguna empresa grande** (en la actualidad o en el pasado), ya sea a nivel nacional o regional.

- **MODEL4_EMP_ECI**: El corte inglés
- **MODEL4_EMP_ZARA**: Zara
- **MODEL4_EMP_REPSOL**: Repsol Petróleo SA.
- **MODEL4_EMP_CEPSA**: Compañía Española de Petróleos SAU. (CEPSA)
- **MODEL4_EMP_MERCADONA**: Mercadona SA.
- **MODEL4_EMP_ENDESA**: Endesa Energía SAU.
- **MODEL4_EMP_ENEL**: Enel Iberoamérica SRL.
- **MODEL4_EMP_INDRA**: INDRA S. A.
- **MODEL4_EMP_TOTAL**: Total Energies (la antigua EDP)
- **MODEL4_EMP_ELCOMERCIO**: El Comercio
- **MODEL4_EMP_LNE**: La Nueva España
- **MODEL4_EMP_LAVOZ**: La Voz de Asturias