Asignatura	Datos del alumno	Fecha
Ciberinvestigación	Apellidos: Iván Andrei	15/01/2025
	Nombre: Dragos Cornel	

Caso práctico: Investigación de un ciberataque

1. Nada más conocer los hechos, lo más urgente sería contener el posible daño causado por la filtración de datos sensibles y crear un equipo y un canal de comunicación, todo ello vital las primeras 24h.

En segundo lugar se va a reconstruir la secuencia temporal del ataque. Debería informarse al equipo interno de seguridad para que estos inicien una evaluación del impacto y busquen posibles vulnerabilidades explotadas. Instalaría herramientas como Wazuh y analizaría todos los logs. Además se deberían seguir los siguientes pasos:

a) Confirmar la veracidad del incidente empezando por la captura de pantalla recibida para comprobar su autenticidad. Acceder a los enlaces proporcionados (perfil y ubicación de Twitter) para corroborar la existencia del contenido filtrado.

b) Determinar si la información publicada pertenece efectivamente a clientes de Industrias OSCORP.

Este paso facilitará luego la identificación del autor, el tipo de ataque, motivación del atacante, etc.

En tercer lugar, sería propio aislar y proteger los sistemas sensibles si aún no están protegidos. De modo que se realizaría un análisis inicial de los sistemas internos para detectar posibles intrusiones o accesos no autorizados.

También sería interesante implementar **medidas de seguridad adicionales** como cambios de contraseñas (recomendable usar un gestor de contraseñas como Keepass), segmentación de redes, y revisión de permisos.

En cuarto lugar, al margen de la creación urgente de canal de comunicación del paso 1 pero estrechamente relacionado con ello, se debería convocar una reunión inmediata con el CEO y el equipo directivo para establecer una estrategia de acción. Además se debería evaluar la necesidad de informar a los clientes afectados tal

como lo recoge la normativa vigente, e informar a las autoridades correspondientes antes de 72h.

En último lugar sería clave empezar a trabajar recopilando las evidencias iniciales. Por ejemplo guardar una copia de la publicación en Twitter, incluyendo además capturas de pantalla y descarga de los metadatos disponibles. También convendría documentar en todo momento los hechos conocidos, tal como fechas y horas, personas involucradas en el manejo de la información, hashes y cadenas de custodia...

Para ejecutar estas acciones, se podrían emplear las siguientes opciones y recursos, entre otros:

a) Herramientas de análisis forense:

-Herramientas como FTK Imager o Autopsy para capturar y analizar la evidencia digital de forma segura.

-Empleo de navegadores configurados para preservar metadatos durante la descarga de páginas web y publicaciones de redes sociales.

b) Colaboración con especialistas:

-Involucrar un equipo especializado en análisis forense digital para garantizar que la evidencia recopilada sea admisible en caso de procedimientos legales.

c) Recursos internos de la empresa:

-Usar sistemas de seguridad ya implementados, como **firewalls, SIEM, Shodan, LeakSearch** y herramientas de monitoreo de red, para auditar e identificar puntos vulnerables.

d) Consultas con el proveedor del servicio (Twitter en este caso):

-Solicitar formalmente *la preservación* de los datos relacionados con la cuenta "@Anonymous_leaks" y sus publicaciones para evitar su eliminación.

e) Apoyo legal y normativo:

-Revisar las guías de gestión de incidentes de seguridad publicadas por organismos como INCIBE para actuar de acuerdo con las mejores prácticas.

Asignatura	Datos del alumno	Fecha
Ciberinvestigación	Apellidos: Iván Andrei	15/01/2025
	Nombre: Dragos Cornel	

2. Para interponer una denuncia y garantizar que se inicie una investigación formal, es necesario cumplir con los siguientes requisitos:

a) Recopilar evidencias sólidas: Capturas de pantalla de las publicaciones comprometedoras, junto con sus metadatos. Registro de los enlaces directos al perfil y las publicaciones implicadas. Informe técnico inicial que detalle los datos filtrados y su posible origen.

b) Redacción de un informe preliminar: Describir los hechos de manera detallada, incluyendo fechas, horas y las posibles consecuencias del incidente. Identificar los sistemas comprometidos y cualquier vulnerabilidad detectada durante la evaluación inicial.

c) Consulta con el departamento legal: Coordinarse con el equipo legal de la empresa para garantizar que la denuncia cumpla con los requisitos normativos y legales. Asegurarse de que se está respetando la confidencialidad de la información sensible involucrada.

d) Momento oportuno para interponer la denuncia: La denuncia debería presentarse tan pronto como se haya confirmado la veracidad del incidente y recopilado evidencia suficiente para respaldar la reclamación, dentro de las primeras 72 horas.

Esto permitirá a las autoridades actuar con rapidez para preservar datos críticos que puedan ser eliminados por el responsable.

e) Contenido de la denuncia:

-Identificación de la empresa afectada y descripción del incidente.

-Detalle de la evidencia recopilada, incluyendo copias de las publicaciones y enlaces relevantes.

-Impacto potencial del incidente sobre la empresa y sus clientes.

-Solicitud formal de investigación para identificar al responsable y mitigar los daños.

Asignatura	Datos del alumno	Fecha
Ciberinvestigación	Apellidos: Iván Andrei	15/01/2025
	Nombre: Dragos Cornel	

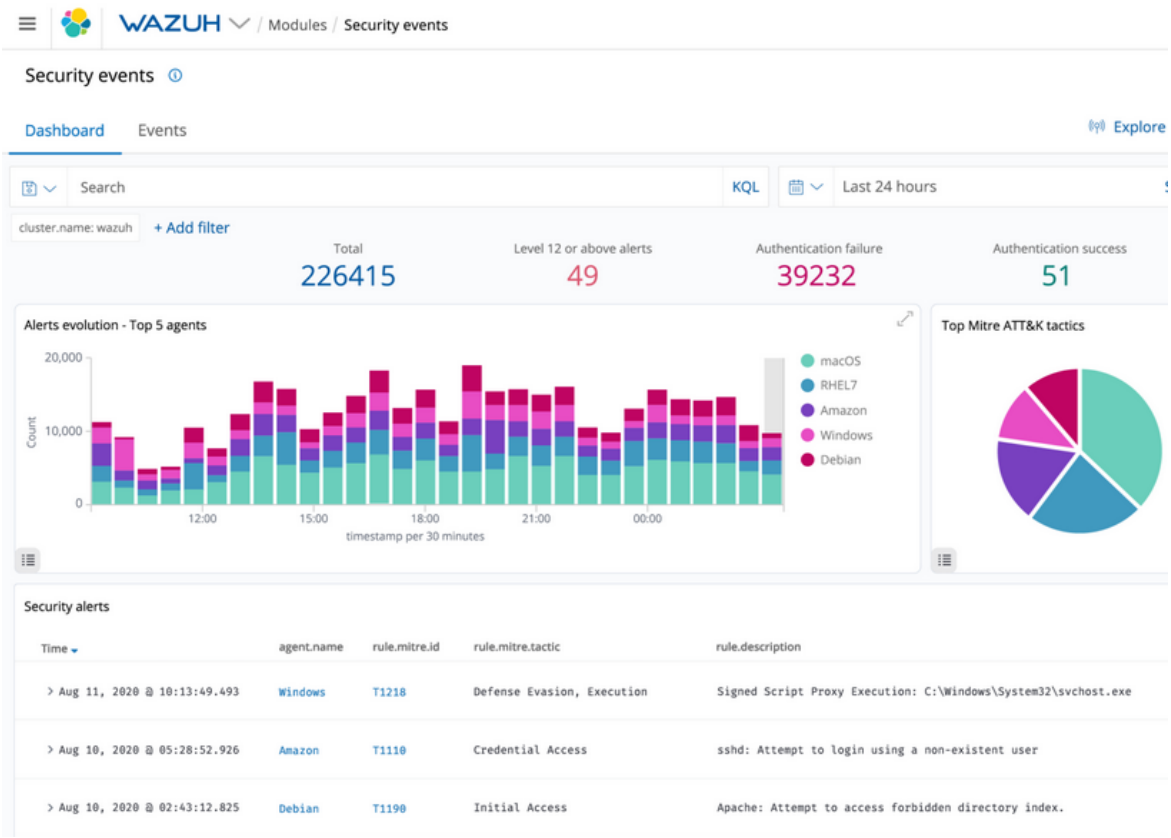
3. Trabajar con la información.

a) Análisis de los metadatos disponibles: Examinar los metadatos asociados a las capturas de pantalla y publicaciones de Twitter para obtener información útil como ubicaciones, fechas de creación y dispositivos utilizados. Usar herramientas de análisis forense como Magnet AXIOM, o EnCase para procesar y examinar las evidencias, ExifTool para metadatos de imágenes. Localizar el ID del autor en Twitter.

b) Seguimiento del perfil en redes sociales: Analizar las actividades públicas del perfil de Twitter "@Anonymous_leaks" para identificar patrones de comportamiento, horarios de actividad y posibles relaciones con otras cuentas. Documentar cualquier interacción o vínculo con perfiles asociados a OSCORP o terceros relevantes. Usar aplicaciones OSINT como Maltego para buscar relaciones del atacante con otras personas, buscar información en LeaKSearch creando un archivo de keywords como "@Anonymous_leaks", añadiendo otras bases de datos en el archivo sources.conf a medida que se avanza en la investigación.

c) Revisión de registros internos de las empresas: Inspeccionar los logs (Wazuh muy buena herramienta) de acceso a los servidores internos de OSCORP en busca de actividades sospechosas, especialmente accesos no autorizados o transferencias de datos inusuales. Verificar posibles puntos de entrada explotados, como vulnerabilidades en software o credenciales comprometidas.

Asignatura	Datos del alumno	Fecha
Ciberinvestigación	Apellidos: Iván Andrei	15/01/2025
	Nombre: Dragos Cornel	



d) Colaboración con autoridades y expertos legales: Trabajar con las autoridades policiales para acceder a información adicional, como datos obtenidos a través de mandamientos judiciales. Asesorar al equipo legal de OSCORP sobre las solicitudes específicas que podrían hacer para obtener datos adicionales de los proveedores de servicios. Es esencial recomendar al abogado de la empresa solicitar a Twitter información técnica y administrativa del perfil implicado, incluyendo datos como la dirección de correo electrónico asociada, número de teléfono, IP utilizada para registrar y acceder a la cuenta, historial de dispositivos usados y metadatos de publicaciones. Además, deberían pedir interacciones relevantes del perfil y detalles sobre intentos de anonimización como uso de VPNs o Tor. Paralelamente, será clave coordinar la obtención de órdenes judiciales para obtener datos de los proveedores de servicios de internet vinculados a las IPs detectadas y realizar un cruce de información con herramientas OSINT para rastrear conexiones entre cuentas o identificar patrones de actividad que vinculen al atacante.

e) Entrevistas y evaluaciones internas: Realizar entrevistas con empleados de OSCORP para identificar posibles sospechas de fuga de información interna, ya sea intencional o accidental. Investigar antecedentes laborales y acceso a información sensible de los empleados actuales y pasados.

f) Solicitudes formales a twitter: Solicitar a nuestro equipo legal que prepare las peticiones de información relacionada con la cuenta "@Anonymous_leaks", incluyendo la dirección IP usada, el correo electrónico asociado, y cualquier otra actividad registrada en la plataforma.

g) Cruzamiento de datos técnicos: Usar la información técnica obtenida (como direcciones IP y horarios de conexión) para rastrear la ubicación y el posible proveedor de internet responsable. Corroborar esta información con otros datos disponibles, como logs internos y actividades sospechosas previamente detectadas.

4. Para la identificación del titular del perfil @Anonymous_leaks se deberían solicitar los siguientes datos técnicos y administrativos al proveedor de servicios de Twitter, siempre dentro del marco legal y con la debida autorización judicial cuando corresponda:

a) Información de registro del perfil:

-Dirección de correo electrónico asociada al perfil.

-Número de teléfono usado para la creación o verificación de la cuenta, si aplica.

-Fecha y hora de creación de la cuenta.

b) Historial de actividad del perfil:

-Dirección IP usada para el registro de la cuenta.

-Historial de direcciones IP desde las cuales se accedió al perfil, incluyendo fechas, horas y duración de las sesiones.

-Registro de dispositivos utilizados para iniciar sesión (modelo, sistema operativo, navegador).

c) Información del contenido publicado:

-Metadatos de la publicación implicada en el incidente (fecha, hora, ubicación geográfica, dispositivo utilizado, etc.).

-Cualquier dirección o eliminación de contenido que pueda estar relacionada con la publicación de datos sensibles.

d) Conexiones de la cuenta:

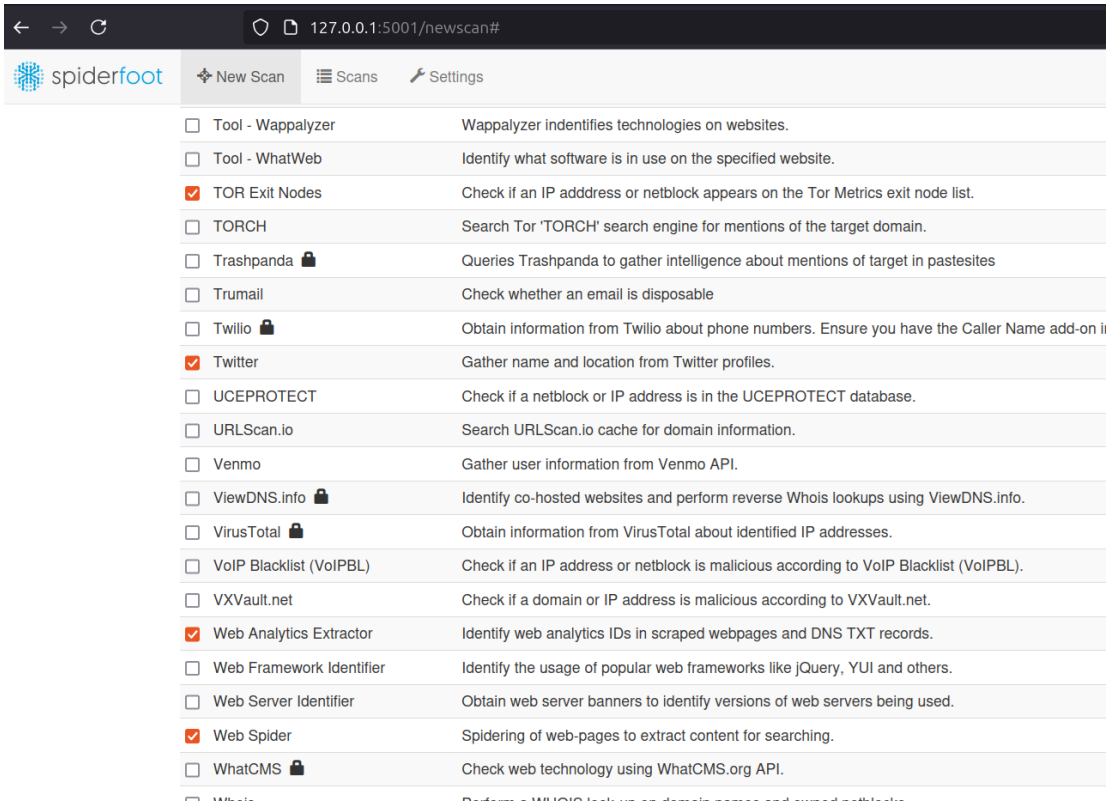
-Información sobre interacciones relevantes del perfil, como retweets, respuestas o mensajes directos relacionados con la filtración de datos.

-Listado de cuentas vinculadas al perfil mediante dispositivos o direcciones IP compartidas.

Por nuestra parte, vamos a usar Spiderfoot entre otras herramientas para intentar adelantar trabajo al margen de la espera de aprobación de procedimientos judiciales. Tengamos en cuenta que ahora mismo estamos trabajando con poca información, ya que solo tenemos la cuenta "@Anonymous_leaks" y poco más. Pero a medida que vamos encontrando correos electrónicos, teléfonos, direcciones IP, etc. lo iremos implementando retroactivamente a aplicaciones como Spiderfoot, para encontrar aún más información de manera exponencial.

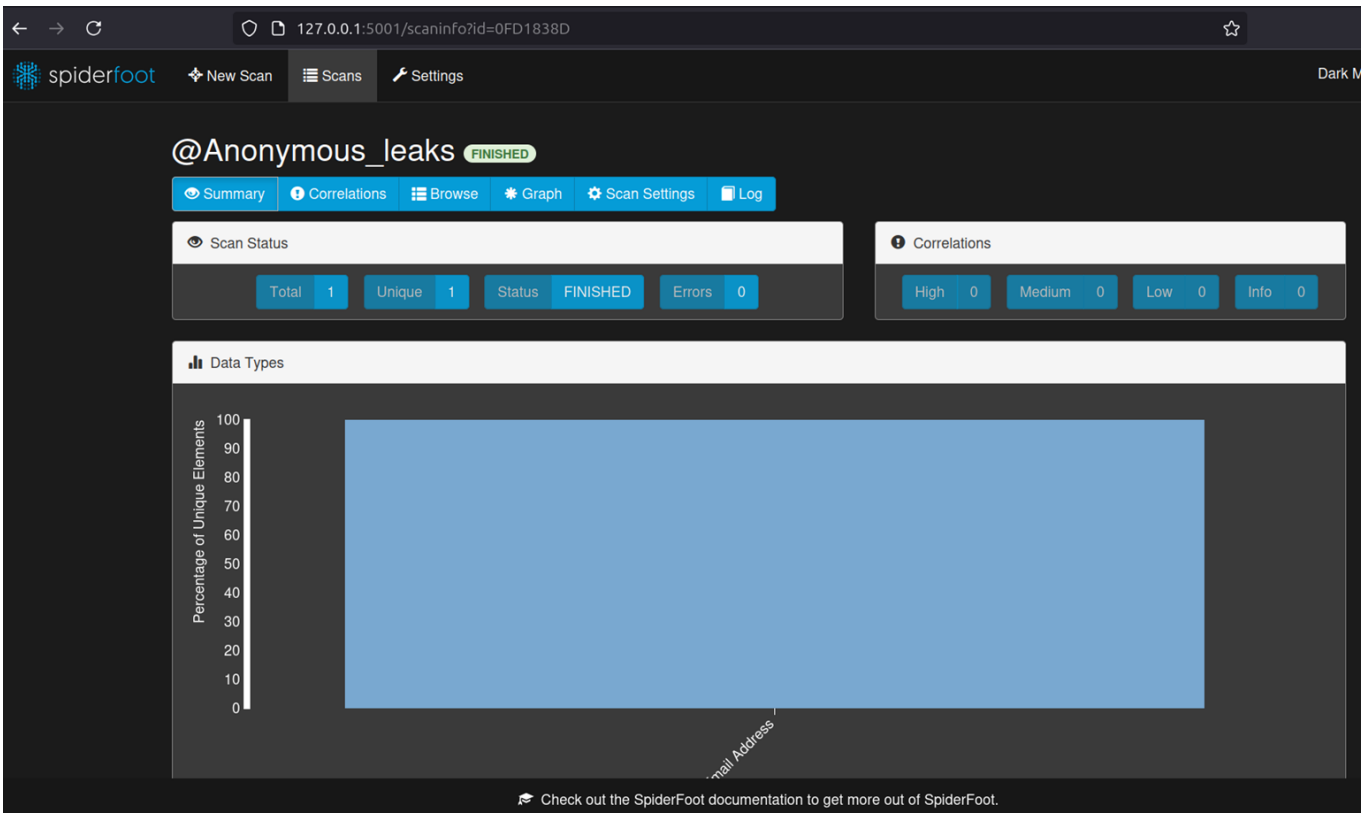
Vamos a seleccionar brevemente en Spiderfoot todos los módulos que creamos que nos puede interesar.

Asignatura	Datos del alumno	Fecha
Ciberinvestigación	Apellidos: Iván Andrei	15/01/2025
	Nombre: Dragos Cornel	



Tras finalizar el escaneo, deberíamos encontrar algo así, pero con mucha más información:

Asignatura	Datos del alumno	Fecha
Ciberinvestigación	Apellidos: Iván Andrei	15/01/2025
	Nombre: Dragos Cornel	



5. El siguiente paso una vez obtenidos los datos técnicos de Twitter sería realizar indagaciones específicas para correlacionar dicha información con el posible autor. Las acciones a realizar serían las siguientes:

a) Análisis de direcciones IP. Por un lado identificar el proveedor de servicios de internet (ISP) asociado a las direcciones IP obtenidas. Luego, solicitar mediante una orden judicial al ISP los datos del titular de la conexión correspondiente a las direcciones IP, incluyendo nombre, dirección física y detalles de la conexión (fechas y horas específicos). Además usaría herramientas OSINT para investigar las direcciones IP, de nuevo usaría Spiderfoot, LeakSearch, Shodan.

b) Identificación de dispositivos. Analizar los datos sobre dispositivos utilizados (modelos, sistemas operativos, navegadores) para buscar coincidencias con otros incidentes reportados o información recopilada previamente. Además se debería investigar si los dispositivos mencionados han sido registrados o utilizados en otros servicios en línea que puedan vincularse al sospechoso.

c) Correlación con patrones de actividad. Examinar los registros de actividad del perfil, como horas de acceso y ubicaciones geográficas, para establecer patrones de uso que puedan coincidir con la rutina o ubicación de una persona específica. Esta información se puede comparar con datos internos de la empresa u otros incidentes reportados.

d) Investigación de cuentas vinculadas. Analizar posibles vínculos entre la cuenta de Twitter en cuestión y otras cuentas en las redes sociales, correos electrónicos o plataformas que hayan utilizado los mismos dispositivos o direcciones IP. Se podría además buscar coincidencias con datos disponibles en bases de datos públicas o privadas que puedan vincular perfiles en línea con identidades reales.

e) Revisión de las herramientas utilizadas. Si en la actividad del perfil se refleja que se utilizaron herramientas de anonimización como VPNs o Tor, sería necesario rastrear estas conexiones hasta su origen, colaborando con los operadores de nodos o servicios involucrados.

f**) Monitorización y vigilancia**. Implementar vigilancia digital en torno al perfil de Twitter y otras cuentas sospechosas para identificar nuevas publicaciones, interacciones o datos que puedan revelar información adicional sobre el autor.

6. La investigación de un ciberdelito como el expuesto requiere un enfoque crítico y analítico para evaluar tanto las posibilidades como las limitaciones inherentes al proceso. Por un lado, la recopilación y análisis de evidencias digitales, como metadatos, registros de actividad y patrones de comportamiento, permite reconstruir eventos y establecer vínculos con posibles autores. Sin embargo, la efectividad de estas acciones depende de factores externos como la cooperación de proveedores de servicios, la integridad de las evidencias recopiladas y las restricciones legales que regulan el acceso a datos sensibles. Este contexto exige adoptar un enfoque inductivo, partiendo de datos fragmentarios para construir hipótesis sólidas, y analítico, desglosando las interacciones técnicas y humanas involucradas en el ataque. A pesar de estas capacidades, es fundamental reconocer

limitaciones como la dificultad de rastrear usuarios que emplean tecnologías de anonimización, lo que resalta la necesidad de una colaboración interdisciplinaria entre expertos técnicos, legales y las autoridades competentes para abordar las complejidades del caso.