



UNIVERSIDAD
DE GRANADA

TRABAJO FIN DE MÁSTER
MÁSTER PROPIO EN CIBERSEGURIDAD

Ciberinteligencia y Threat Hunting. Herramientas y metodologías para facilitar sus procesos.

Autor

Fabián Olender (alumno)

Directores

Antonio Muñoz Ropa (tutor)



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE
TELECOMUNICACIÓN

Granada, Julio de 2022

Ciberinteligencia y Threat Hunting. Herramientas y metodologias para facilitar sus procesos.

Autor

Fabián Olender (alumno)

Director

Antonio Muñoz Ropa (tutor)

Ciberinteligencia y Threat Hunting. Herramientas y metodologías para facilitar sus procesos

Fabián Olender (alumno)

Palabras clave: Ciberinteligencia, OSINT, Threat Hunting, Hunt, Seguridad Ofensiva, Reconocimiento

Resumen

La información se ha vuelto uno de los activos más importantes para las organizaciones, con su valor creciendo aceleradamente. Debido a que en su mayoría existe en formato digital y con el notable aumento en brechas de seguridad y fugas de información, las organizaciones llevan tiempo desplazándose del concepto de “Si sucede” al “Cuando suceda”, generando que la ciberseguridad pase de tener un foco casi exclusivo en los controles preventivos hacia la distribución entre controles también reactivos y detectivos. En ese sentido, las prácticas de Ciberinteligencia y Threat Hunting se encuentran en pleno auge para combatir las amenazas de manera detectiva-proactiva.

Este trabajo se centra en analizar el estado de situación actual, las metodologías y procesos de ambas prácticas para identificar las dificultades que encuentran las organizaciones al intentar implementar programas de ciberseguridad suficientemente maduros para optar por ellas a fin de disminuir riesgos. El objetivo final es el desarrollo de una solución que facilite a los analistas de una o ambas prácticas la puesta en funcionamiento de un ambiente de trabajo con herramientas para asistir por un lado en el proceso de identificar el nivel de exposición de información de una organización y sus miembros mediante técnicas OSINT y por otro lado, en el proceso de búsqueda de adversarios que han superado las barreras de seguridad mediante metodologías de Threat Hunting no estructuradas.

Threat Intelligence and Threat Hunting. Tools and methodologies to facilitate its processes

Fabián Olender (student)

Keywords: Threat Intelligence, OSINT, Threat Hunting, Hunt, Offensive Security, Reconnaissance

Abstract

Information has become one of the most important assets for organizations, with its value growing rapidly. Due to the fact that it mostly exists in digital format and with the remarkable increase in security breaches and information leaks, organizations have been moving from the concept of “If it happens” to “When it happens”, causing cybersecurity to go from having an almost exclusive focus on preventive controls towards distribution between controls that are also reactive and detective. On those lines, Cyber Threat Intelligence and Threat Hunting are booming to combat threats with a proactive detective approach.

This thesis focuses on analyzing the current landscape, the methodologies and processes of both practices to identify the difficulties that organizations face when trying to implement cybersecurity programs that are mature enough to incorporate them in order to reduce risks. The goal is to develop a solution that facilitates analysts from one or both practices to establish a work environment with tools to assist, on one side, the process of identifying through OSINT techniques what information of an organization and its members is exposed publicly, and on the other side, the process of searching for adversaries that have overcome security barriers through unstructured Threat Hunting methodologies.

Yo, **Fabián Olender**, alumno del **Máster Propio en Ciberseguridad** de la **Universidad de Granada**, con NIE Y8984951S, autorizo la ubicación de la siguiente copia de mi *Trabajo Fin de Máster* en la biblioteca del centro para que pueda ser consultada por las personas que lo deseen.

Fdo: Fabian Olender

Granada a 1 de Julio de 2022.

D. Antonio Muñoz Ropa (tutor), Profesor del Master Propio de Ciberseguridad, jefe de servicio de seguridad informática del Centro de Servicios Informáticos y Redes de Comunicaciones de la Universidad de Granada..

Informa:

Que el presente trabajo, titulado *Ciberinteligencia y Threat Hunting. Herramientas y metodologías para facilitar sus procesos*, ha sido realizado bajo su supervisión por **Fabián Olender (alumno)**, y autorizo la defensa de dicho trabajo ante el tribunal que corresponda.

Y para que conste, expide y firma el presente informe en Granada a 1 de Julio de 2022.

El director:

Antonio Muñoz Ropa (tutor)

Agradecimientos

Agradezco a mi tutor, Antonio Muñoz Ropa, por guiarme a lo largo del proyecto, a mis colegas de Salesforce por brindarme consejos, a mi familia y amigos por ser el sostén para poder alcanzar esta meta, y especialmente a mi pareja, Eva Amanda Calomino, por acompañarme y apoyarme en todo el proceso.

Índice general

1. Introducción	1
1.1. Motivación y contexto del proyecto	2
1.2. Objetivos del proyecto y logros conseguidos	3
1.3. Estructura de la memoria	4
1.4. Contenidos teóricos para la comprensión del proyecto	6
1.4.1. Introducción a la Ciberseguridad	7
1.4.2. Introducción a la Ciberinteligencia	10
1.4.3. Introducción a la Seguridad ofensiva	18
1.4.4. Introducción al Threat Hunting	22
2. Planificación y costes	27
3. Análisis del problema	28
3.1. Definición del problema	29
3.2. Especificación de requisitos	34
3.3. Pruebas de concepto	37
3.3.1. Selección de sector	38
3.3.2. Selección de organismo	42
3.4. Análisis de soluciones existentes	46
3.4.1. Soluciones de Ciberinteligencia	47
3.4.2. Soluciones de Threat Hunting	80
4. Diseño	89
5. Implementación	91
6. Evaluación y pruebas	97
7. Conclusiones	103
Bibliografía	114
Glosario	123

Índice de figuras

1.1.	DIKW Pyramid (Wikipedia)	10
1.2.	5 Stages of The Threat Intelligence Lifecycle (SOCRadar) . .	13
1.3.	An Anatomy of the Internet (Cyber Research, Argonne National Laboratory)	16
1.4.	Cyber Kill Chain (Lockheed Martin)	19
1.5.	Unified Kill Chain	20
1.6.	Threat Hunting: la práctica de detectar amenazas ocultas en nuestra red (ESET)	22
1.7.	The Pyramid of Pain (David Bianco)	24
2.1.	Planificación presupuestaria para implementación de solución.	27
2.2.	Planificación de tiempo para el desarrollo del proyecto.	27
3.1.	Folleto de servicios de Ciberinteligencia ofrecidos por MSSP a Universidades públicas.	43
3.2.	Captura de pantalla del escritorio del Sistema Operativo Trace Labs.	49
3.3.	Captura de pantalla del menú de ayuda del Script ns21Osint.sh.	50
3.4.	Captura de pantalla del escritorio del Sistema Operativo luego de la ejecución del Script de Argos.	51
3.5.	Captura de pantalla del escritorio del Sistema Operativo Ofensint.	52
3.6.	Captura de pantalla de los escaneos (abortados manualmente) de Spiderfoot.	59
3.7.	Captura de pantalla con detalles de un escaneo de Spiderfoot, en el que destaca la cantidad de errores generados.	60
3.8.	Captura de pantalla de los resultados de un escaneo de Spiderfoot para recolectar correos electrónicos.	61
3.9.	Captura de pantalla de uno de los escaneos de theHarvester finalizando con errores.	63
3.10.	Captura de pantalla de Maltego con entidades agrupadas por tipo.	64

3.11. Captura de pantalla de Maltego con ejecución de transformaciones sobre algunas entidades descubiertas en la primera ejecución.	65
3.12. Captura de pantalla del menú de Recon-ng previo a la ejecución de sus módulos.	67
3.13. Captura de pantalla del módulo “mailfy” de OSRFramework en ejecucion.	68
3.14. Captura de pantalla con hallazgos de OSRFramework.	69
3.15. Captura de pantalla con resumen de hallazgos de sn0int.	70
3.16. Captura de pantalla con información inicial de hallazgos de FinalRecon.	71
3.17. Captura de pantalla del inicio del escaneo de un conjunto de IPs mediante nmap.	72
3.18. Captura de pantalla del inicio del escaneo de una IP específica mediante nmap.	73
3.19. Captura de pantalla con intentos de conexión manual a un puerto que nmap marco como abierto.	74
3.20. Captura de pantalla con escaneo de nmap sobre IP específica para reconocer servicios.	75
3.21. Captura de pantalla con escaneo de nmap sobre IP específica para reconocer servicios.	75
3.22. Captura de pantalla con escaneo de nmap sobre el conjunto de IPs y con una serie de parámetros para evitar la detección y bloqueo de los sistemas de seguridad.	76
3.23. Captura de pantalla con resultados de escaneos de vulnerabilidades en el puerto SSH de OpenVAS.	77
3.24. Captura de pantalla con detalles de las vulnerabilidades detectadas por OpenVAS en un objetivo.	78
3.25. Captura de pantalla con detalles del Sistema Operativo detectado por OpenVAS en un objetivo.	78
3.26. Captura de pantalla de Nessus con detalles de vulnerabilidades SSH en un objetivo.	79
3.27. Captura de pantalla de Nessus con todas las vulnerabilidades detectadas y detalles del ambiente conseguidos durante el análisis de un objetivo centrado en SSH.	79
3.28. Captura de pantalla con importación de logs en formato Zeek a RITA.	83
3.29. Captura de pantalla con estadísticas de posibles detecciones de balizas de RITA.	84
3.30. Captura de pantalla con estadísticas de conexiones entre IPs de RITA a fin de detectar posible exfiltración de información.	84
3.31. Captura de pantalla con estadísticas de conexiones de IPs de RITA a fin de detectar conexiones inusualmente extendidas.	85

3.32. Captura de pantalla de APT-Hunter analizando un conjunto de archivos con formato EVTX.	86
3.33. Captura de pantalla del reporte en formato XLSX generado por APT-Hunter.	87
3.34. Captura de pantalla de múltiples análisis realizados por DeepBlueCLI en base a múltiples archivos con formato EVTX. . .	88
3.35. Captura de pantalla con resultados de dnstwist.	88
5.1. Captura de pantalla de ejecución de HunTnisO sin parámetros.	96
5.2. Captura de pantalla de ejecución de HunTnisO con ambos parámetros en Ubuntu 20.04 LTS.	96
6.1. Captura de pantalla de estadísticas de ejecución del Script HunTnisO.	98
6.2. Captura de pantalla de ejecución del Script HunTnisO con parámetro “–osint”	99
6.3. Captura de pantalla de ejecución del Script HunTnisO con parámetro “–hunt”	99
6.4. Captura de pantalla de ejecución de HunTnisO en Ubuntu 22.04 LTS.	100
6.5. Captura de pantalla de ejecución del Script HunTnisO en Kali 2022.01.	101
6.6. Captura de pantalla de ejecución del Script HunTnisO en un Sistema Ubuntu con todas las dependencias y herramientas ya instaladas.	102

Índice de tablas

3.1.	Soluciones empaquetadas de Ciberinteligencia.	48
3.2.	Soluciones individuales existentes en las 13 soluciones empaquetadas relevadas.	55
3.3.	Soluciones individuales de instalación local listadas en “OSINT-Framework.com” no observadas previamente.	56
3.4.	Listado de recursos online que podrían proveer información adicional a las soluciones relevadas.	58
3.5.	Soluciones individuales para asistir en el Threat Hunting con metodología basada en datos.	83

Listados de código

- 5.1. Script en Bash para automatizar instalación de herramientas
de OSINT y Threat Hunting no estructurado 91

Capítulo 1

Introducción

1.1. Motivación y contexto del proyecto

La aceleración en la generación y consumo de información por parte de las organizaciones, combinado con el incremento del valor que esta posee y la creciente digitalización experimentada en las últimas décadas han resultado en diferentes tipos de actores maliciosos causando brechas de seguridad y fugas de información que representan pérdidas monetarias inmensas. Por estas razones diferentes campos dentro de la ciberseguridad focalizados en detectar proactivamente a estas amenazas están rápidamente ganando terreno, como la Ciberinteligencia y el Threat Hunting. Un análisis detallado de estas afirmaciones se encuentra desarrollado en la Sección 1.4.1.

Las prácticas de Ciberinteligencia y Threat Hunting tienen como prerequisito para las organizaciones un nivel medio de madurez en Ciberseguridad y requieren de personal altamente capacitado, y especializado en dichas prácticas, para poder ser incluido en sus programas. Teniendo en cuenta la alta demanda y baja oferta de recursos humanos en el sector de Ciberseguridad, resulta muy difícil el desarrollo interno de servicios o implementación interna de procesos que abarquen estas prácticas, razón por la cual las organizaciones tienden a recurrir a la tercerización. Esto representa un potencial problema para organizaciones grandes o con información especialmente sensible, ya que las empresas que brindan estos servicios tercerizados tienden a ser un blanco cautivador para actores maliciosos avanzados, debido a que una brecha de seguridad sobre los mismos podría representar también una fuga de información sobre las organizaciones contratantes. Internalizar estos servicios resulta especialmente difícil para organizaciones que no disponen de presupuestos suficientes en ciberseguridad para contratar personal ya capacitado de manera directa ni adquirir soluciones que simplifiquen estas tareas. En consecuencia, la contratación de personal sin capacitación previa en estas prácticas que pueda ser autodidacta a fin de desarrollar sus tareas mediante herramientas gratuitas o de bajo coste resulta la opción más viable para comenzar a migrar de servicios tercerizados a gestión de servicios internos con el fin de disminuir o mitigar el riesgo. De este modo se ve que existe una creciente necesidad por soluciones sencillas que contengan herramientas gratuitas y bien documentadas para el desarrollo de las prácticas de Ciberinteligencia y Threat Hunting. La Sección 3.1 profundiza sobre este análisis.

1.2. Objetivos del proyecto y logros conseguidos

A fin de abordar el problema expuesto, los objetivos establecidos para este trabajo son:

- (1) Investigar las prácticas de Ciberinteligencia y Threat Hunting para determinar qué metodologías y procesos estas organizaciones necesitan implementar, analizar las soluciones existentes para abarcar estas necesidades y establecer qué tipo de soluciones se requieren.
- (2) Desarrollar una solución que contenga herramientas de Ciberinteligencia y Threat Hunting reconocidas, gratuitas, de fácil uso y aprendizaje.

Se han logrado cumplir los objetivos establecidos, como se detalla a continuación:

- El objetivo (1) se encuentra desarrollado en la Sección 3.4 y se ha determinado que las organizaciones de este tipo usualmente requieren:
 - En términos de Ciberinteligencia, identificar el nivel de exposición de información de la organización y sus miembros a partir de inteligencia de fuentes abiertas.
 - En términos de Threat Hunting, llevar adelante investigaciones no estructuradas utilizando metodologías basadas en datos.
 - Las soluciones idealmente se encuentran empaquetadas, son fácilmente auditables, son simples de desplegar en sistemas reconocidos y se basan en herramientas conocidas y gratuitas (o de bajo coste).
- El objetivo (2) se ha detallado en las Secciones 4, 5 y 6. Se ha desarrollado un Script en Bash que en base a un Sistema Operativo Ubuntu 20.04 LTS que instala de manera automática un conjunto de herramientas de Ciberinteligencia (Spiderfoot, theHarvester, Maltego, nmap, Nessus) y Threat Hunting (RITA, APT-Hunter y dnstwist), así como todas las dependencias que estas requieren.

1.3. Estructura de la memoria

Capítulo 1: Introducción.

- En la Sección 1.1 se introduce brevemente el contexto y motivación que dan lugar a la problemática observada, conceptos ampliamente desarrollados en las secciones 1.4.1 y 3.1.
- En la Sección 1.2 se introducen brevemente los objetivos perseguidos con el trabajo y las soluciones propuestas, conceptos ampliamente desarrollados en las secciones 3.4, 4, 5 y 6.
- En esta Sección, 1.3, se detalla cómo se estructura la memoria a fin de situar al lector frente a la misma.
- En la Sección 1.4 se introducen contenidos teóricos necesarios para comprender el desarrollo de capítulos posteriores, pero pueden ser omitidos por lectores ya experimentados o con conocimientos en los campos de cada subsección, siendo 1.4.1 focalizada en Ciberseguridad, 1.4.2 focalizada en Ciberinteligencia, 1.4.3 focalizada en Seguridad ofensiva y 1.4.4 focalizada en Threat Hunting.

Capítulo 2: Planificación y costes.

Este Capítulo detalla cómo fue planificado este proyecto y cuáles serían los costos estimados para una organización que pretenda desarrollar de manera interna las prácticas de Ciberinteligencia y metodologías de Threat Hunting abarcadas en la solución propuesta.

Capítulo 3: Análisis del problema.

- En la Sección 3.1 se analiza la situación actual y el estado del arte para determinar el problema que afrontan las organizaciones para implementar programas de Ciberinteligencia y Threat Hunting.
- En la Sección 3.2 se relevan los requerimientos y requisitos que tendrían una posible solución a la problemática observada.
- En la Sección 3.3 se investigan múltiples reportes de amenazas de ciberseguridad, a fin de seleccionar un sector en la Sección 3.3.1 y un organismo en la Sección 3.3.2 para las pruebas de concepto de las soluciones existentes.
- En la Sección 3.4 se relevan y analizan las soluciones existentes, con aquellas orientadas a Ciberinteligencia en la Sección 3.4.1 y aquellas orientadas al Threat Hunting en la Sección 3.4.2.

Capítulo 4: Diseño.

Este Capítulo detalla el diseño que tiene la solución desarrollada, especificando tecnologías relacionadas al lenguaje de programación, las herramientas y Sistema Operativo utilizados como base.

Capítulo 5: Implementación.

Este Capítulo detalla cómo implementar y desplegar la solución desarrollada.

Capítulo 6: Evaluación y pruebas.

Este Capítulo muestra detalles de pruebas realizadas con la solución desarrollada en el ambiente predefinido, extendiendo también las pruebas a otros ambientes a fin de comprobar su adaptabilidad y compatibilidad.

Capítulo 7: Conclusiones.

En este Capítulo se reconocen las fortalezas y deficiencias del trabajo investigativo y la solución desarrollada, los espacios de mejora y posibles vías de investigación disponibles para extender el trabajo expuesto.

1.4. Contenidos teóricos para la comprensión del proyecto

1.4.1. Introducción a la Ciberseguridad

En el ámbito de los sistemas computacionales, **dato** es el término que refiere a entradas registradas sin procesar (hechos, eventos, transacciones) e **Información** es el término que refiere a los datos que han sido procesados de tal manera que pueden ser entendidos e interpretados, aunque es usual que ambos términos se usen indistintamente.

El reporte “The Digitization of the World from Edge to Core” [1] de Seagate de 2018 predijo que la cantidad de datos digital generada diariamente a nivel mundial aumentaría de 33 a 175 Zettabytes para 2025 y el reporte “Articulating Value from Data”[2] del World Economic Forum de 2021 detalla que el 90 % del valor de una organización radica en activos intangibles como sus datos, propiedad intelectual, marca y reputación. Por consiguiente, la protección de la información es un área de creciente interés a nivel global. De acuerdo a la norma ISO/IEC 27001:2013[3], la **Seguridad de la Información** se refiere a la confidencialidad, la integridad y la disponibilidad de la información de una organización, independientemente del formato que tengan (física o digital), y los términos **Seguridad Informática** y **Ciberseguridad** se refieren específicamente a estas protecciones de la información en formato digital. El objetivo de control A8.2 de esta norma (“Clasificación de la información”) establece la seguridad de la información de acuerdo a su clasificación, indicando que toda información debe recibir un nivel de protección adecuado de acuerdo a la clasificación que se le asigne. La información se puede clasificar según su valor, los requisitos legales, la sensibilidad y la criticidad que la misma tiene para la organización.

Una **brecha de seguridad** es el acto de un adversario accediendo sin autorización a una organización. La **exfiltración** es un tipo de **fuga de Información**, una acción que ocurre cuando el adversario copia o mueve información no pública de la organización fuera de su perímetro luego de una brecha (es decir, una salida no controlada de información de la organización). El gráfico “World’s Biggest Data Breaches & Hacks”[4] muestra cómo incluso las organizaciones más grandes del mundo han sido afectadas por masivas fugas de información, mayormente siendo exfiltraciones como consecuencias de una brecha de seguridad. Por otro lado, las fugas de información en **fuentes abiertas** son en casi todos los casos aprovechadas por los adversarios para preparar el ataque a la organización. En consecuencia, a fin de evitar brechas de seguridad, es fundamental evitar la fuga de información que tenga una clasificación no pública, lo que requiere mantener un control constante sobre qué información está disponible acerca de una organización y sus miembros en fuentes abiertas. En este aspecto, la gestión de la seguridad de la información de acuerdo a su clasificación depende de una amplia gama de **controles preventivos, detectivos y reactivos**.

Ejemplos de controles preventivos son el software de prevención de pérdida de datos (DLP), el cifrado en tránsito del canal de comunicación y el cifrado

en reposo de la información.

Ejemplos de controles reactivos son las actividades de contención y recuperación ante incidentes de seguridad, implementados usualmente por Equipos de respuesta a incidentes de seguridad informática (CSIRT).

Los controles detectivos se dividen en:

- Detectivos-reactivos: como pueden ser las actividades de triage en un Centro de Operaciones de Seguridad (SOC) y el despliegue de reglas de detección y alerta en un equipo de Detección de amenazas (*Threat Detection*).
- **Detectivos-proactivos:** como pueden ser la práctica de Ciberinteligencia, o la práctica de Caza de amenazas (Threat Hunting).

Los controles detectivos en general resultan muy importantes ya que sirven para monitorizar que los controles preventivos funcionan correctamente y alertar cuando no son suficientes o fallan. Las organizaciones cuya madurez en ciberseguridad alcanza cierto nivel en los controles preventivos, reactivos y detectivos-reactivos, implementan también controles detectivos-proactivos, que buscan activamente encontrar que controles detectivos o reactivos faltan, fallan o requieren mejoras.

Se considera que una amenaza existe cuando las siguientes condiciones se cumplen:

- Capacidad: El actor tiene los recursos necesarios para ofender (conocimientos técnicos, suficiente financiamiento).
- Oportunidad: Existe la disponibilidad de medios para ofender (técnicos y/o logísticos).
- Intención hostil: La finalidad del actor resulta dañina para el objetivo.

De cumplirse 2 de estos 3 atributos, la amenaza se considera potencial. La ciberinteligencia y el Threat Hunting son reconocidas como prácticas altamente eficientes y recomendadas en todas las industrias:

- El reporte anual de amenazas de CrowdStrike de 2022[5] concluye su introducción destacando que las prácticas de Ciberinteligencia y Threat Hunting proveen un mayor entendimiento de las motivaciones, objetivos y actividades de los adversarios, y como esta información puede empoderar una organización hacia la implementación de contramedidas proactivas para mejorar la defensas y detecciones. Asimismo la sección de recomendaciones remarca en el punto 8 la importancia de implementar Threat Hunting para la detección proactiva y temprana de amenazas.

- El reporte “Security Outcomes Study” de Cisco de 2021[6] demuestra en la figura 19 cómo la práctica de Threat Hunting tiene una relación directa con las actividades de detección y respuesta exitosa a incidentes de seguridad, con un 30 % de mejora en la eficiencia de sus actividades al ejecutar sus procesos al menos 1 vez por semana.
- El reporte de amenazas de Rapid7 de 2020[7] destaca que los procesos más avanzados de la práctica de Threat Hunting son solo implementables por organizaciones con un presupuesto alto y muy maduras en términos de ciberseguridad, ya que requieren de personal altamente capacitado y una base de herramientas que requieren de mucha inversión.

1.4.2. Introducción a la Ciberinteligencia

El término Ciberinteligencia proviene de combinar las palabras cibernético e inteligencia, es decir la inteligencia aplicada al campo cibernético. La definición de cibernético se refiere a lo que forma parte del mundo de las computadoras (u ordenadores) y de la realidad virtual. La definición de inteligencia tiene múltiples acepciones y es aún muy debatida, pero en este aspecto se refiere al concepto de inteligencia originado del ámbito militar. En ese sentido, el artículo “A New Definition of Intelligence”[8] publicado por Allan Breakspear en Researchgate lo define como “la capacidad para pronosticar cambios a tiempo a fin de hacer algo al respecto. La capacidad implica previsión y perspicacia, y tiene por objeto identificar los cambios inminentes, que pueden ser positivos, representando una oportunidad, o negativos, representando una amenaza.”. El proceso de inteligencia genera información a partir de datos, conocimiento a partir de información y sabiduría a partir del conocimiento, con el fin de asistir en la toma de estas decisiones. Se representa gráficamente en la Figura 1.1. en lo que se conoce como Pirámide DIKW.



Figura 1.1: DIKW Pyramid (Wikipedia)

La práctica de **Ciberinteligencia** es conocida también como inteligencia de amenazas, *Threat Intelligence* o *Cyber Threat Intelligence* (CTI) y debido a las múltiples acepciones que el término inteligencia en sí mismo contiene, no existe tampoco una definición única. Gartner lo define como “conocimiento basado en evidencia, incluyendo contexto, mecanismos, indicadores, implicaciones y consejos accionables, acerca de una amenaza o peligro existente o emergente para los activos, que se puede utilizar para informar al sujeto a fin de que este pueda tomar decisiones informadas en respuesta a esa amenaza o peligro” [9].

De acuerdo a la presentación “The Cycle of Cyber Threat Intelligence” [10] de Katie Nickels, los requerimientos de inteligencia (IRs, por sus siglas del inglés *Intelligence Requirements*) son “los objetivos que se buscan satisfacer a través de los procesos de inteligencia”. Estos objetivos serán presentados por terceros en diferentes formatos, comúnmente como requisitos de infor-

mación o conocimiento específico, o bien una pregunta (general o puntual) que necesita ser respondida. Se detallan a continuación algunos procesos usualmente utilizados para cumplir estos objetivos:

- I Examinar el contexto general en diferentes escalas (global, regional, local) y mantener conciencia situacional sobre el ámbito e industria en que la organización opera.
 - II Recolectar información e identificar Indicadores de compromiso (IoCs) sobre actores maliciosos emergentes y existentes.
 - III Establecer perfiles de adversarios específicos para la organización (*Threat Landscape*), entender sus motivaciones, trazar su modus operandi e identificar indicadores de ataque (IoAs).
 - IV Modelar los riesgos y amenazas que existen para la organización (*Threat Modeling*).
- V Identificar el nivel de exposición de información de la organización y sus miembros.**

Esta lista no sigue un orden específico, es orientativa y menciona procesos generalmente ejecutados por equipos de ciberinteligencia, pero no pretende ser exhaustiva ya que los procesos son muy variados entre organizaciones. De esta lista puede observarse que el proceso II suele ser el primero en implementarse por ser el más fácil de automatizar, y el más simple de adaptar ya que en pocas situaciones requiere ser personalizado a cada organización. Por estas razones es también el proceso que más se externaliza y terceriza, siendo además el que menos riesgos implica para la organización por no aumentar la superficie de ataque ni exposición. Por otro lado, el proceso V suele ser el siguiente en implementarse, ya que también existen herramientas que facilitan su automatización (en menor medida que el proceso anteriormente mencionado) y si bien existen múltiples formas de tercerizar parcialmente, requerirá compartir información sensible con la organización que se contrate (y autorizarlos a buscar aun más información activamente). Además, dado que este proceso requiere ser personalizado a cada organización, tiende a tener un coste bastante más elevado. Los procesos I, III y IV son más avanzados y tienden a requerir de personal contratado directamente por la organización.

Dependiendo del proceso, se podrá optar por distintas disciplinas de inteligencia, siendo las más utilizadas:

- A Inteligencia de fuentes abiertas (**OSINT**, acrónimo del inglés *Open Source Intelligence*), recolectada a partir de información pública.
- B Inteligencia de señales (**SIGINT**, acrónimo del inglés *Signals Intelligence*), recolectada en la intercepción de señales de comunicación.

- C Inteligencia humana (HUMINT, acronimo del inglés *Human Intelligence*), recolectada por una persona en una locación física.
- D Inteligencia de Redes Sociales (**SOCMINT**, acronimo del inglés *Social Media Intelligence*), recolectada a partir de información existente en redes sociales. Es generalmente considerada una **subdisciplina de OSINT**.

El ciclo de vida de Ciberinteligencia asiste en la ejecucion de estos procesos con el fin de cumplir los objetivos establecidos. Existen ciclos con más o menos fases, siendo especialmente conocidos los implementados por el Centro Nacional de Inteligencia (CNI)[11] de España y la Agencia Central de Inteligencia (CIA)[12] de Estados Unidos de America, pero en líneas generales se reconocen 5 fases, representadas gráficamente en la Figura 1.2:

1. Planificación: Establecer el objetivo y asociarlo a uno de los procesos, determinar qué disciplinas se utilizaran y establecer prioridades respecto a qué información se buscará y como.
2. Recolección: Seleccionar qué fuentes de información y herramientas se utilizarán, recolectar y almacenar la información.
3. Procesamiento: Procesar la información (manualmente o mediante herramientas) agregando contexto y filtrando lo que no sea relevante para el objetivo.
4. Análisis: Se interpreta la información para generar conocimiento, desarrollando informes que asistan en la toma de decisiones.
5. Diseminación y Retroalimentación: Distribución de los informes a las partes interesadas, con acciones recomendadas específicas cuando sea necesario. Se revisan los resultados obtenidos para adoptar mejoras en alguna de las fases previas. De especial importancia resulta la opinión (*feedback*) que provean los destinatarios de los informes.



Figura 1.2: 5 Stages of The Threat Intelligence Lifecycle (SOCRadar)

Se definen 3 niveles de inteligencia, que deberán tenerse en cuenta durante la fase de Planificación, dado que están relacionados a qué información se recolecta en la fase de Recolección y a quién se presentarán los resultados en la fase de Diseminación:

- Estratégico: Información de alto nivel relacionada a riesgos cambiantes, intenta responder a las preguntas “¿Quién?” y “¿Por qué?”. Ejemplos de personal estratégico que reciben este nivel de información son los ejecutivos de alto nivel y la gerencia.
- Táctico: Información técnica de alto nivel que asiste en la toma de decisiones e intenta responder a las preguntas “¿Cómo?” y “¿Dónde?”. Ejemplos de personal táctico que reciben este nivel de información son los arquitectos, ingenieros y administradores de sistemas y redes.
- Operacional: Información técnica de bajo nivel que intenta responder a las preguntas “¿Qué?” y “¿Cuándo?”. Ejemplos de personal operacional que reciben este nivel de información son los diferentes equipos de ciberseguridad.

Algunas organizaciones sin embargo reconocen un 4 nivel denominado “Técnico” en el que se especifican IoCs.

Un aspecto importante en la generación y recolección de información reside en si la misma es estructurada (estandarizada en algún formato específico) o no estructurada (formato libre como portales de noticias, foros, web feeds, blogs, etc.). Dado que diferentes tipos de información requieren diferentes campos, múltiples estándares de código abierto y propietarios se han desarrollado. El reporte “Exploring the opportunities and limitations of current Threat Intelligence Platforms”[13] de ENISA detalla tanto estándares como herramientas para generar y consumir información estructurada.

Se han creado múltiples modelos de maduración de ciberinteligencia que definen como una organización podría desarrollar estas capacidades, destacándose entre ellos el CREST CTI Maturity Model[14], el ThreatConnect Threat Intelligence Maturity Model (TIMM)[15] y el Cyber Threat Intelligence Lab (CTIL) Maturity Model”[16]. La sección “Creating and Scaling Your Intelligence Program” del libro “The Intelligence Handbook”[17] provee lineamientos para la implementación de un programa de ciberinteligencia.

El reporte “Cyber Threat Intelligence Survey”[18] de SANS de 2022 observa que el 75 % de las organizaciones consideran que las prácticas de Ciberinteligencia mejoraron su postura de ciberseguridad (sumando también un 21 % que no eran capaces de medirlo). Adicionalmente se destaca que el 71,7% de las organizaciones utilizan en mayor o menor medida OSINT como disciplina para la recolección de información (sobre sí mismas o sus adversarios).

La ejecución de las fases 1 a 4 del ciclo de Ciberinteligencia sobre el proceso V mediante la disciplina OSINT (y SOCMINT) resulta especialmente importante ya que mantiene una relación directa y se considera muy similar a las fases iniciales de los marcos de referencia más reconocidos en el campo de Seguridad ofensiva, por lo que es también una actividad realizada por adversarios de distintas capacidades en la mayoría de las brechas de seguridad. Esta actividad puede realizarse con métodos de recolección de información pasivos (sin interactuar directamente con el objetivo) o activos (interactuando directamente con el objetivo) y se divide en 2 subprocesos:

- *Footprinting*: Exploración inicial con el fin de crear un perfil del objetivo e identificar la mayor cantidad de activos posibles. Incluye fases como la identificación de personal y el escaneo de redes.
- *Fingerprinting*: Análisis profundo de cada activo encontrado para crear perfiles específicos. Incluye fases como el escaneo de puertos, identificación y enumeración (de sistemas operativos, servicios, versiones, usuarios, etc.) y escaneo de vulnerabilidades.

Los métodos pasivos de Fingerprinting tienden a requerir de bastante más tiempo y suelen proveer menos información que los activos, por lo que es frecuente que en este subproceso dominen métodos activos. Sin embargo los métodos activos, al interactuar directamente con el activo, son considerados más intensivos (pudiendo llegar a ser intrusivos o disruptivos) en las redes y sistemas donde se realiza, razón por la cual es usual que algunas de las fases más avanzadas, como parte de la identificación y enumeración o el escaneo de vulnerabilidades sean delegadas en equipos especializados en el campo de la Seguridad Ofensiva o bien en equipos de Gestión de Vulnerabilidades. Dado que los métodos de recolección de información mencionados son actividades informáticas realizadas con conexión a redes abiertas, es prudente comprender la definición de los siguientes términos, cuya representación visual se observa en la Figura 1.3:

- Internet: Conjunto descentralizado de redes de comunicaciones interconectadas, incluye todos los protocolos y direcciones enrutables globalmente.
- World Wide Web (WWW): La porción de Internet accesible mediante un navegador web.
- Surface Web: La porción de la WWW que es indexada por motores de búsqueda.
- Deep Web: La porción de la WWW no indexada por motores de búsqueda, pero accesible mediante un navegador web.
- DarkNet: Red utilizada para enrutamiento de tráfico y/o contenido en el que todos los servicios y sitios son accesibles sólo a través de direcciones no enrutables globalmente, o a través de redes superpuestas (como por ejemplo TOR e I2P).
- Dark Web: Servicios y sitios de la DarkNet (Denominados “Servicios ocultos”), accesibles únicamente mediante el uso de redes superpuestas.

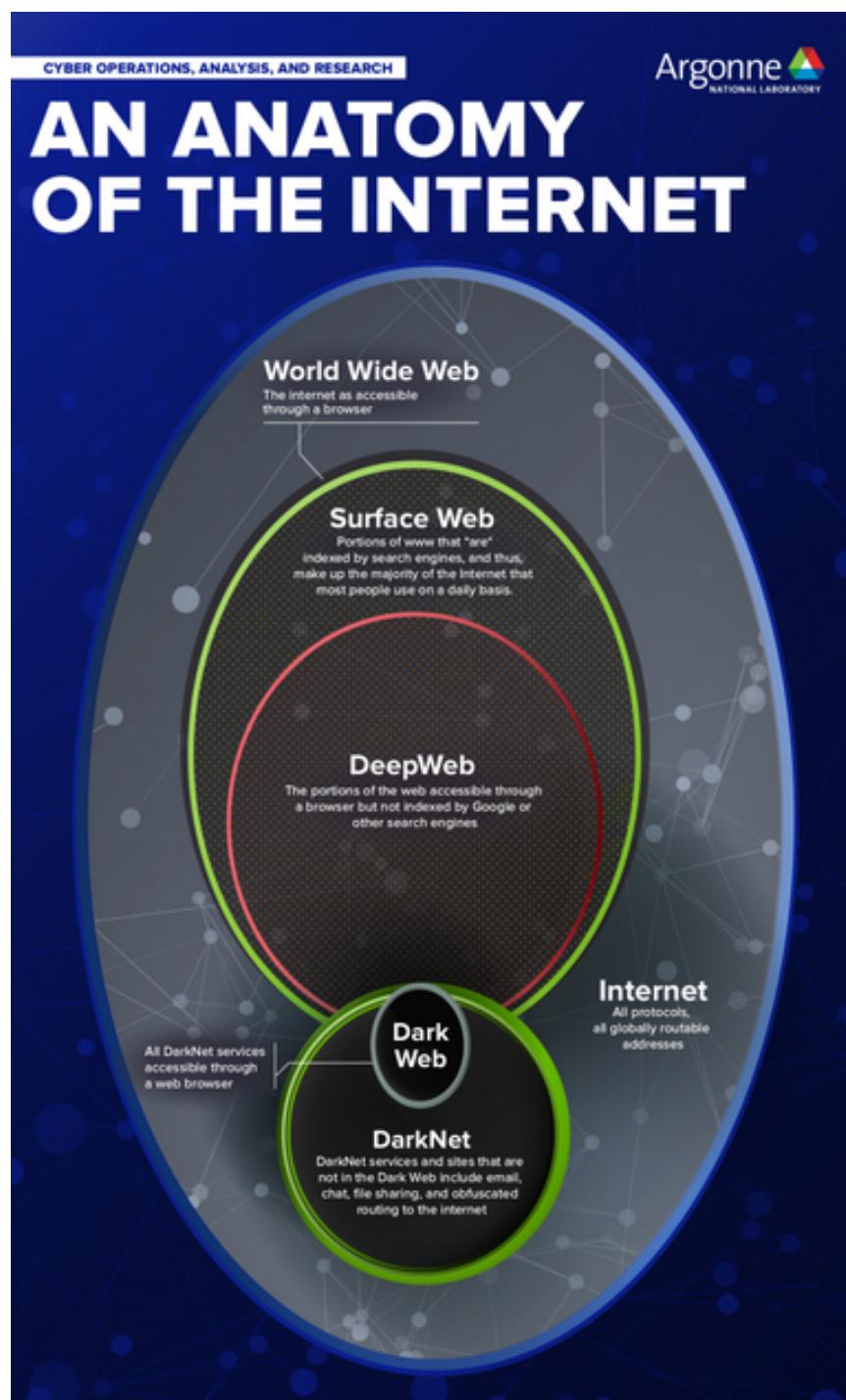


Figura 1.3: An Anatomy of the Internet (Cyber Research, Argonne National Laboratory)

Existen múltiples recursos disponibles para el aprendizaje de ciberinteligencia:

- El curso SANS SEC487 (“Open-Source Intelligence (OSINT) Gathering and Analysis”) prepara al alumno para la certificación “GIAC Open Source Intelligence” (GOSI) y el curso SANS FOR578 (“Cyber Threat Intelligence”) prepara al alumno para la certificación “GIAC Cyber Threat Intelligence” (GCTI). Ambas entidades son autónomas pero GIAC considera los cursos de SANS los únicos que proveen el curso oficial de preparación para la certificación.
- La certificación “CREST Practitioner Threat Intelligence Analyst” (CPTIA) y sus versiones más avanzadas, “CREST Registered Threat Intelligence Analyst” (CRTIA) y “CREST Certified Threat Intelligence Manager” (CCTIM). CREST no provee cursos, pero tiene múltiples socios oficiales que autoriza para proveer el curso que prepara al alumno para las certificaciones.
- El curso y certificación “EC-Council Certified Threat Intelligence Analyst” (CTIA).

Esta lista comprende solo algunos cursos que tienen una certificación asociada en diferentes rangos de precio, provistos por organizaciones de enseñanza reconocidas en ciberseguridad, pero no pretende ser exhaustiva y pueden hallarse oportunidades de aprendizaje a rangos de precio que se ajustan a las necesidades del alumno, incluso gratuitamente.

1.4.3. Introducción a la Seguridad ofensiva

La **Seguridad ofensiva** (*Offensive security* u *OffSec*) es el campo de la ciberseguridad que incluye cualquier actividad realizada con enfoque ofensivo hacia un objetivo (el término del inglés hace referencia también a la empresa estadounidense creadora de la distribución Kali Linux y el repositorio ExploitDB, entre otros). El hacking ético (*Ethical Hacking*) es una disciplina dentro del campo de la seguridad ofensiva en la que, existiendo autorización previa, se evalúan los riesgos en que se encuentran los activos de una organización. Las pruebas de penetración (*Penetration test* o *Pentest*) son un tipo específico de evaluación de seguridad realizada para determinar las debilidades en las defensas implementadas. Por otro lado, se denomina equipo rojo (*Red Team*) al grupo de personas autorizadas que realizan operaciones (o campañas) mediante la emulación de un adversario para realizar las actividades ofensivas contra un objetivo, a fin de proveer retroalimentación en términos de seguridad desde la perspectiva adoptada.

Existen múltiples diferencias entre un ejercicio de Red Team y uno de Pentesting, siendo las más relevantes que el primero intenta, con la mayor fidelidad posible, imitar a una amenaza puntual para la organización, no suele ser anunciada al equipo de seguridad defensiva ya que intentará probar su respuesta y capacidad, tendrá menos restricciones (por ejemplo, se suele permitir la penetración física y la ingeniería social), tendrá una duración bastante mayor y no se centrará en la búsqueda de vulnerabilidades. Previo a la ejecución de un Pentest o una operación de Red Team es necesario que se definan las reglas de enfrentamiento (ROE por sus siglas en inglés, *Rules of engagement*), que definen las directrices y restricciones en relación a las pruebas que se realizarán y otorga autoridad al equipo ejecutor para proceder sin necesidad de permisos adicionales.

Existen múltiples marcos de referencia y metodologías reconocidas para realizar estas evaluaciones, siendo algunos de los más reconocidos:

- Cyber Kill Chain: Desarrollado por Lockheed Martin, adoptó el concepto militar de Kill Chain, que identifica la estructura de un ataque, a la seguridad de la información para crear esta metodología. Se representa gráficamente en la Figura 1.4 y se denomina *Reconnaissance* a la primera fase.

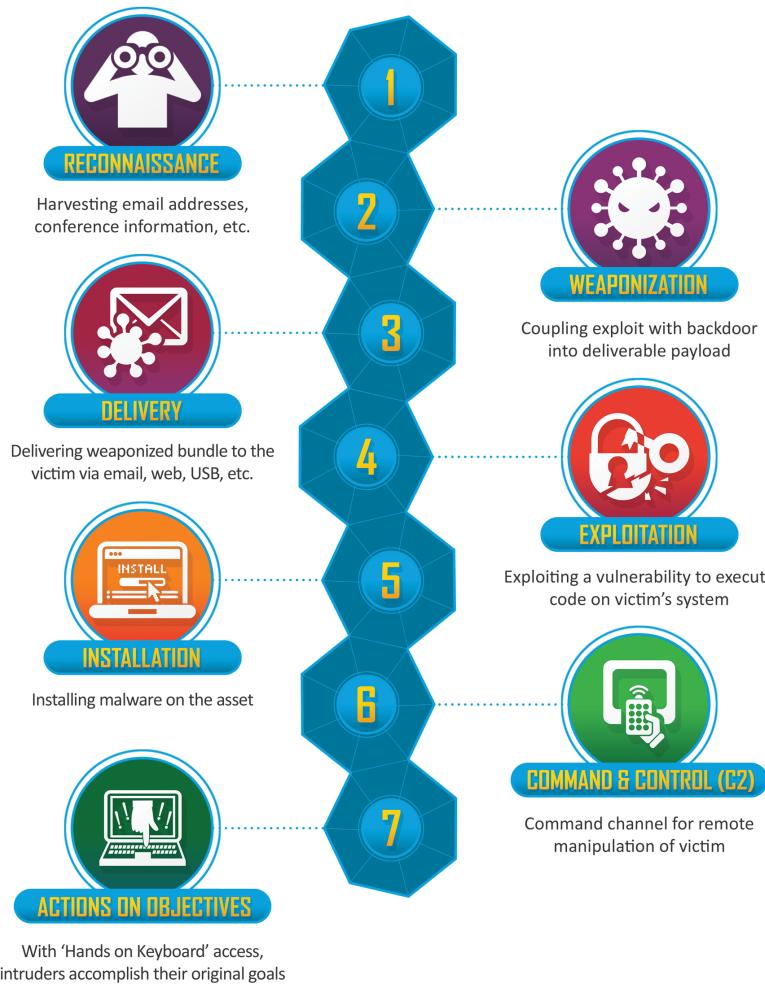


Figura 1.4: Cyber Kill Chain (Lockheed Martin)

- MITRE ATT&CK: Marco de referencia con conocimiento estructurado para clasificar tácticas, técnicas y procedimientos utilizados por adversarios, basado en observaciones reales. Se desarrollaron 3 matrices: “Enterprise”, “Mobile” y “PRE-ATT&CK”. Esta última contiene conocimiento relacionado con actividades que los adversarios hacen antes de perpetrar un ataque y se divide en 2 fases, siendo la primera denominada *Reconnaissance*.
- Unified Kill Chain: En base a la Cyber Kill Chain y a MITRE ATT&CK, Paul Pols desarrolló esta metodología que combina aspectos de ambos, siendo también la primer fase denominada *Reconnaissance* y se representa gráficamente en la Figura 1.5.

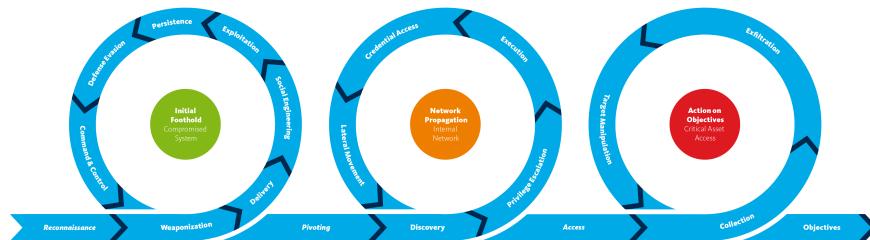


Figura 1.5: Unified Kill Chain

- The Penetration Testing Execution Standard (PTES): Estándar diseñado por un grupo diverso de especialistas en ciberseguridad para proveer un lenguaje y alcance común en las pruebas de penetración. Las primeras dos fases son *Pre-engagement Interactions* e *Intelligence Gathering*.

Luego de las preparaciones que se requieran según el caso, se observa que la fase inmediata siguiente de todos estos modelos guarda relación directa y gran similitud con las fases 1 a 4 del ciclo de Ciberinteligencia sobre el proceso V mediante la disciplina OSINT. Sin embargo, se destaca en este caso que tanto el Footprinting como el Fingerprinting son ejecutados en profundidad y casi sin limitaciones, siendo las fases que más tiempo y dedicación consumen.

Resulta especialmente relevante comprender esta relación para que el proceso de ciberinteligencia mencionado cubra apropiadamente el footprinting y fingerprinting desde el punto de vista de una amenaza o un adversario.

El rango de conocimientos que suele requerir este campo es muy amplio, por lo que múltiples recursos están disponibles para el aprendizaje de seguridad ofensiva:

- El curso y certificación de “EC-Council Certified Ethical Hacker” (CEH).
- El curso SANS SEC560 (“Network Penetration Testing and Ethical Hacking” prepara al alumno para la certificación “GIAC Penetration Tester” (GPEN)).
- El curso “PEN-200” prepara al alumno para la certificación “Offensive Security Certified Professional” (OSCP).

Esta lista comprende únicamente cursos que tengan una certificación asociada en diferentes rangos de precio, para diferentes niveles de conocimiento, provistos por organizaciones ampliamente reconocidas en ciberseguridad

y que abarcan temas de manera generalizada, por lo que no pretende ser exhaustiva y pueden hallarse oportunidades de aprendizaje a rangos de precio que se ajustan a las necesidades del alumno (incluso gratuitamente), focalizados en tecnologías o campos más específicos y cuyos prerrequisitos de conocimiento en la materia sean mayores.

1.4.4. Introducción al Threat Hunting

La primera referencia a *Threat Hunting* en el ámbito de la Ciberseguridad la realizó Richard Bejtlich en el artículo “Become a Hunter” [19] de la revista “Information Security” en su edición julio/agosto de 2011. En él indica que los CSIRT deberían realizar operaciones de búsqueda activa de amenazas para poder contrarrestar a los adversarios más avanzados. La evolución de esta práctica y sus metodologías, la llevó a que a estar fuertemente vinculada también a los equipos de Ciberinteligencia, de modo que el Threat Hunting consume el conocimiento que provee la ciberinteligencia y son sus hallazgos los que detectan las amenazas que serán tratadas por los CSIRT.

En la actualidad, la práctica de Threat Hunting se define como el proceso iterativo y proactivo de buscar artefactos y amenazas (internas y externas) que han superado las defensas de seguridad y han logrado evadir los métodos de detección implementados. El objetivo principal es acortar el tiempo de permanencia entre el momento en que el adversario se infiltra en la red y el tiempo en que es descubierto (*dwell time*), visualizable en la Figura 1.6.

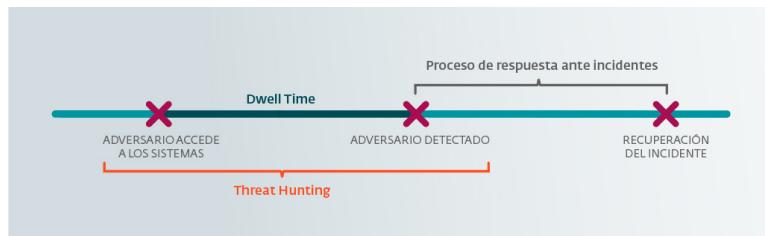


Figura 1.6: Threat Hunting: la práctica de detectar amenazas ocultas en nuestra red (ESET)

Entre otros objetivos se encuentran el de mejorar las capacidades de detección automatizada mediante la creación de prototipos de nuevas detección (estos prototipos podrán ser luego convertidos en detecciones mediante equipos de detecciones de amenazas) y descubrir nuevos IoCs e IoAs dentro de la organización que deban ser informados al equipo de ciberinteligencia. El Threat Hunting se categoriza como **no estructurado**, que utiliza **metodologías basadas en inteligencia o basadas en datos**, o **estructurado**, que utiliza **metodologías basadas en hipótesis**.

- A Basada en inteligencia (*Intel-driven*): La investigación suele partir de IoCs reconocidos para buscarlos históricamente en los registros de eventos (logs). Esta metodología es considerada la más sencilla de implementar ya que el proceso II de ciberinteligencia suele proveer ciertos indicadores de compromiso necesarios. Adicionalmente es la más simple de automatizar.
- B Basada en datos (*Data-driven*): La investigación combina técnicas simples como *Searching* (se ejecuta una consulta a partir de un evento o

artefacto para pivotar en nuevas búsquedas) y *Filtering* (filtrar los resultados para afinar la siguiente búsqueda) y técnicas estadísticas como *Grouping* (agrupar eventos o artefactos que comparten características para determinar patrones que permitan filtrarlos y pivotar las búsquedas), *Clustering* (Basado en tecnologías de aprendizaje automático no supervisado para generar grupos de datos relacionados que permitan re-focalizar la búsqueda) y *Stacking* (implica contar la cantidad de ocurrencias de eventos u observaciones de artefactos para detectar valores atípicos) con el fin de detectar anomalías. Existen herramientas para maximizar la automatización de las detecciones (aunque en la mayoría de los casos se requiere la intervención humana para analizar los hallazgos) y asisten en el análisis mediante aplicación de técnicas avanzadas de ciencia de datos (*Data Science*), como los sistemas de análisis de comportamiento de los usuarios y entidades (UEBA), pero debido a que se basan en logs suelen ser una adición a los sistemas de gestión de información y eventos de seguridad (SIEM) ya existentes.

- C Basada en hipótesis: La investigación pretende reconocer comportamientos basados en IoAs o técnicas, tácticas y procedimientos (TTPs) aliñeadas con MITRE ATT&CK. Esta metodología suele apoyarse también en técnicas mencionadas en la metodología basada en inteligencia o la metodología basada en datos, pero es considerado más avanzada ya que se realiza mediante una planificación estructurada que requiere conocer el ambiente sobre el que se ejecutan las fases descritas, que se considera normal y qué contramedidas existen implementadas (para evitar crear una hipótesis que no sería factible en primer lugar). En ese sentido, resulta de mucha utilidad referenciar las bases de hipótesis con MITRE D3FEND para comprobar que no se parte de parte de una premisa impracticable desde el punto de vista de un adversario. El informe “ATT&CK and D3FEND Report: Incorporating Frameworks into Your Analysis and Intelligence” [20] de SANS de 2022 resalta la importancia de combinar ambos marcos de referencia de MITRE. El proceso III de ciberinteligencia provee las bases para aplicar esta metodología con la mayor eficiencia posible, ya que la hipótesis podrá centrarse en adversarios específicos de la organización y no solo en amenazas reconocidas públicamente. También es recomendable revisar, de existir, los resultados y el modus operandi de las operaciones ejecutadas en pruebas de penetración y/o por equipos rojo. Por otra parte, es usual crear o replicar parcialmente ambientes productivos para emular adversarios de manera controlada y luego verificar las posibles detecciones, y si bien estas simulaciones son generalmente parte de las operaciones de un equipo rojo, esta metodología explora estas mismas simulaciones de modo más concreto y acotado en el tiempo, simulando parcialmente solo algunas de las técnicas que en una operación de equipo rojo formarán parte de una simulación más

completa y extendida de un adversario. Esta diferencia puede observarse con mayor claridad al observar el “Adversary Emulation Plans”[21] de MITRE que podría llevar adelante un equipo rojo en contraposición con el “Cyber Analytics Repository”[22] (CAR) de MITRE que podría utilizar un equipo de Threat Hunting. Es frecuentemente utilizado el “MITRE ATT&CK Navigator”[23] para explorar y realizar anotaciones sobre las hipótesis a desarrollar. A fin de utilizar la metodología basada en hipótesis de manera eficiente, resulta imprescindible comprender la calidad de los datos con los que la organización dispone. Ejemplos de Hunts basados en hipótesis específicas pueden observarse en el sitio web “Threat Hunter Playbook”[24] (Roberto Rodriguez y Jose Luis Rodriguez) y en el repositorio de GitHub “ThreatHuntingProject/ThreatHunting”[25].

Se reconoce también la metodología basada en entidades o situaciones (*Entity-driven* o *Situational-driven*), que refiere a la construcción de búsquedas priorizando los riesgos en los activos de mayor valor para una organización, pero se puede considerar que es un enfoque que puede aplicarse a cualquiera de las metodologías mencionadas.

La sección “Setting Up Your Threat Hunting Program” del artículo “Hunt Evil: Your Practical Guide to Threat Hunting”[26] de Sqrrl provee lineamientos para la implementación de un programa de Threat Hunting. La sección “Leveraging Machine Learning for Cyber Threat Hunting” del libro Huntpedia[27] (Sqrrl) es particularmente interesante para programas más avanzados ya que detalla cómo se podría automatizar y aplicar técnicas de aprendizaje automático en Hunts.

Resulta de gran importancia comprender cómo estas metodologías afectarán al adversario. La Figura 1.7 muestra “La Pirámide del Dolor”, que representa de forma gráfica cuánto daño se causa a un adversario y cuando le costaría a este recuperarse cuando se identifican y bloquean sus métodos.

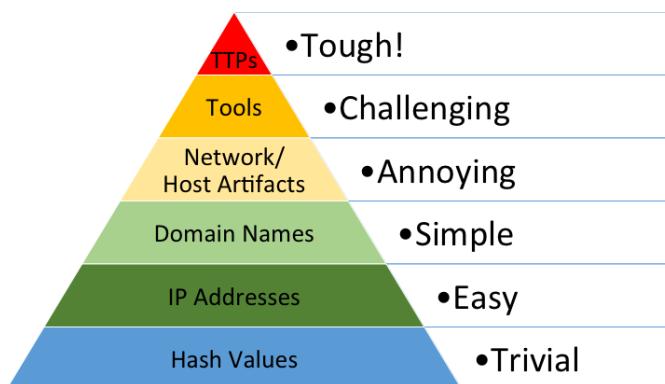


Figura 1.7: The Pyramid of Pain (David Bianco)

Existen múltiples marcos de referencia que pueden utilizarse para la implementación de Threat Hunting basado en hipótesis como “TaHiTI” [28], “The Hunting Loop” [29] y “A Practical Model for Conducting Cyber Threat Hunting” [30]. En general, pueden resumirse en 3 fases:

1. Planificación: Se define el propósito, el alcance, los objetivos y una estrategia inicial.
2. Investigación: Se ejecutan ciclos de búsqueda y refinación en base a resultados obtenidos. Todas las líneas investigativas deben ser perseguidas hasta confirmar si la actividad observada es maliciosa o no.
3. Resolución: Si la actividad observada es benigna, se determina si es necesario implementar excepciones en las detecciones. Si la actividad observada es maligna, se inicia el proceso de respuesta a incidentes de seguridad. En ambos casos, se retroalimentan las defensas y las condiciones de detección para automatizar la repetición de la misma investigación.

“The Hunting Maturity Model” [31] (David Bianco) describe un modelo con 5 niveles el modelo de maduración que una organización puede alcanzar. Se centra principalmente en las habilidades de los analistas, la calidad de los datos y las herramientas que tienen a disposición.

El reporte “Survey: Threat Hunting in Uncertain Times” [32] de SANS de 2021 destaca que 73 % de las organizaciones realiza alguna metodología de Threat Hunting notando una mejora entre 10 % y 25 % en su postura de ciberseguridad, siendo el 93,1 % de ellas con personal interno específicamente dedicado a la tarea. Sin embargo, solamente un 14,4 % indica que la madurez del programa es alta (utilizando metodologías basadas en hipótesis) y el 50,6 % de las organizaciones utilizan inteligencia obtenida de disciplinas OSINT. Además, se observa que la principal barrera para implementar o mejorar los procesos de Hunting actuales es considerada la falta de personal disponible, según el 51 % de las organizaciones.

Los conocimientos requeridos para realizar Threat Hunting suelen estar parcialmente incluidos en cursos previstos en el marco de otras prácticas como Ciberinteligencia, Análisis forense digital y respuesta a incidentes (DFIR), etc; por lo que se puede encontrar cursos y certificaciones exclusivamente orientadas a esta práctica o bien donde la misma está incluida como parte de la currícula:

- El curso SANS FOR508 (“Advanced Incident Response, Threat Hunting, and Digital Forensics”) prepara al alumno para la certificación “GIAC Certified Forensic Analyst” (GCFA) y el curso SANS FOR572 (“Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response”) prepara al alumno para la certificación “GIAC Network Forensic Analyst” (GNFA). Ambas entidades son autónomas pe-

ro GIAC considera los cursos de SANS los únicos que proveen el curso oficial de preparación para la certificación.

- La certificación “eLearnSecurity Certified Threat Hunting Professional” (eCTHPv2). Actualmente solo una entidad es socia oficial y brinda el curso que prepara al alumno para el examen.

Esta lista comprende únicamente cursos que tengan una certificación asociada en diferentes rangos de precio, provistos por organizaciones ampliamente reconocidas en ciberseguridad, que no hayan sido específicamente listadas previamente en entre los posibles cursos y certificaciones de ciberinteligencia, pero no pretende ser exhaustiva y pueden hallarse oportunidades de aprendizaje a rangos de precio que se ajustan a las necesidades del alumno (incluso gratuitamente).

Capítulo 2

Planificación y costes

La planificación de presupuesto estimativo para implementar la solución propuesta puede observarse en la Figura 2.1.

Costes estimativos			
Categoría	Concepto	Monto (anual)	Unidades
Personal	Salario de especialista en ciberseguridad	€35,000	2
Hardware	Estaciones de trabajo	€500	2
Capacitacion	Adquisicion de libros para formacion	€40	3
Capacitacion	Formacion mediante cursos y/o certificaciones	€850	2
Software general	Licencias para estaciones de trabajo	€1,100	2
Ciberinteligencia	Licencias para herramientas específicas	€800	1
Threat Hunting	Licencias para herramientas específicas	€250	1
Servicios externos	Respuesta a Incidentes por detecciones de alta severidad	€1,500	1
Total		€77,570	

Figura 2.1: Planificación presupuestaria para implementación de solución.

La planificación de tiempo para el desarrollo del proyecto puede observarse en la Figura 2.2.

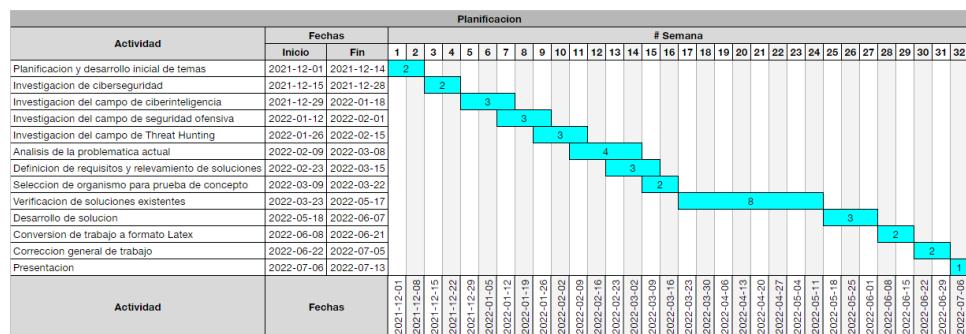


Figura 2.2: Planificación de tiempo para el desarrollo del proyecto.

Capítulo 3

Análisis del problema

3.1. Definición del problema

Las prácticas de Ciberinteligencia y Threat Hunting se consideran avanzadas e implementables por organizaciones maduras en Ciberseguridad, ya que requieren profesionales con mucha experiencia para la ejecución de sus procesos y se pueden implementar cuando ya existe, al menos, un plan de respuesta a incidentes, un sistemas de detección y alerta de amenazas, un SIEM, un sistemas de detección y respuesta (EDR) y un Centro de Operaciones de Seguridad (SOC).

Los equipos que gestionen estos procesos estarán proveyendo un servicio a la organización. Las organizaciones pueden gestionar servicios internamente (requiere la contratación directa de profesionales calificados), mediante la tercerización de servicios (implica la subcontratación de otra organización) o como una combinación de ambas.

Las organizaciones que proveen servicios que se adecuen a este proceso suelen utilizar diferentes denominaciones para describirse a sí y sus actividades o servicios, pero se puede nombrar a su conjunto como Proveedores de Servicios Gestionados de Seguridad (MSSP, por sus siglas del inglés *Managed Security Service Provider*). Su principal ventaja para las organizaciones que las subcontratan es la disminución total de gastos, favoreciendo los gastos operativos (*Operational expenditures*) sobre los gastos de capital (*Capital expenditures*) y la posibilidad de disminuir el riesgo al delegar la monitorización de su información con personal altamente capacitado.

No se requiere tener en cuenta de manera particular a aquellas organizaciones que administran información con un nivel de clasificación tal que esté regido por normas (como podría ser la información categorizada como “secreta” por una agencia de inteligencia nacional o la información categorizada como “de salud” por un organismo que brindar servicios relacionados a la salud), ya que la oferta de MSSPs disponible en el mercado es lo suficientemente amplia para abastecer la variada demanda de las organizaciones que pueden requerir certificaciones especiales para el manejo de su información. Existen múltiples marcos de referencia que podrán ser utilizados para determinar la madurez de una organización en términos de ciberseguridad, no obstante en pocos se menciona de manera específica el nivel de madurez en relación a las prácticas de Threat Hunting y Ciberinteligencia. En particular, el Cybersecurity Maturity Model Certification (CMMC)[33] establece 5 niveles de madurez, representando el nivel 1 (“Basic Cyber Higiene”) el de menor madurez y el nivel 5 (“Advanced / Progressive Cyber Higiene”) el de mayor madurez. En los niveles 1, 2 (“Intermediate Cyber Higiene”) y 3 (“Good Cyber Higiene”) no hay referencias a prácticas o procesos de Ciberinteligencia o Threat Hunting.

En el nivel 4 (“Proactive Cyber Higiene”) las siguientes prácticas destacan:

- Control “RM.4.150”: Emplear ciberinteligencia para informar en el

desarrollo de sistemas y arquitecturas de seguridad, selección de soluciones de seguridad, monitoreo, Threat Hunting y respuesta y recuperación de actividades.

- Control “SA.4.171”: Establecer y mantener capacidades de Cyber Threat Hunting para buscar Indicadores de Compromiso (IoC) en los sistemas y de detectar, rastrear e interrumpir amenazas que evaden los controles existentes.
- Control “SI.4.221”: Utilizar información de indicadores de amenaza que sea relevante a la información y los sistemas que están siendo protegidos y mitigaciones efectivas obtenidas a partir de organizaciones externas, para informar de detección de intrusiones y a equipos de Threat Hunting.
- Control “SC.4.199”: Utilizar la ciberinteligencia para proactivamente bloquear peticiones a sistema de nombres de dominio (DNS) que tengan como destino un dominio malicioso.

En el nivel 5 (“Advanced / Progressive Cyber Higiene”) se añade también:

- Control “RM.5.155”: Analizar la efectividad de las soluciones de seguridad al menos anualmente para afrontar de manera anticipada los riesgos en los sistemas y la organización, basándose en la inteligencia de amenazas existente y acumulada.

Pese a que sería poco aconsejable y es en sí poco usual, una organización podrá tener el requerimiento o la necesidad de implementar servicios de ciberinteligencia y/o Threat Hunting sin pretender implementar otros procesos y prácticas asociados a los niveles de madurez previos al nivel 4 o 5, y en estos casos lo más recomendable sería hacerlo mediante la contratación de un MSSP.

La escasez de personal de ciberseguridad a nivel mundial, genera que las organizaciones compitan entre ellas (y con los MSSP mismos) para disponer del personal calificado capaz de brindar este servicio y alcanzar el nivel de madurez pretendido. Por consiguiente, la capacidad de gestionar este servicio exclusivamente de manera interna (con contrataciones directas) estará fuertemente asociada a su capacidad de inversión en ciberseguridad, lo que en la mayoría de los casos da la ventaja a las organizaciones más grandes en facturación y valor en activos (o bien a los MSSP mismos cuya inversión es mayoritariamente en ciberseguridad). Sin embargo las diferentes ofertas de mercado establecidas por los MSSP para los servicios de ciberinteligencia y/o Threat Hunting, cubren (en mayor o menor medida) las necesidades de las organizaciones con todos los rangos de presupuesto, aunque el presupuesto orientado a ciberseguridad estará fuertemente ligado a la capacidad de la organización de alcanzar el nivel madurez pretendido. En este análisis se

omite intencionalmente el caso en que la organización sea el MSSP mismo, ya que se asume que para proveer el servicio, el MSSP deberá tener la capacidad de aplicarlo para sí.

La Ley 5/2015[34] de España, de fomento de la financiación empresarial, del 27 de abril de 2015 establece los siguientes parámetros para definir el tamaño de una empresa:

- Microempresa: Menos de 10 trabajadores y un volumen de facturación anual (o total de activos) inferior a 2 millones de euros.
- Pequeña empresa: Menos de 50 trabajadores y un volumen de facturación o total de activo inferior a 10 millones de euros.
- Mediana empresa: Menos de 250 trabajadores y un volumen de facturación inferior a 50 millones de euros (o total de activo inferior a 43 millones de euros).
- Grandes empresas: Todas aquellas que sobrepasen estos parámetros.

Esta norma coincide con el artículo “Enterprises by business size”[35] de la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Dado que todas las empresas son organizaciones pero no todas las organizaciones son empresas, y a falta de una definición formal en relación al tamaño de las organizaciones, se establecen los parámetros de la ley mencionada para definirlas también a estas.

Una organización con menos de 250 miembros (Microempresa, Pequeña empresa y Mediana empresa) no podrá asignar personal contratado de manera directa lo suficientemente especializado para cubrir los requerimientos que demanda la gestión de estos servicios de manera exclusiva debido a la limitación de miembros, incluso si su facturación anual o valoración en activos es considerada alta para su tamaño. Por consiguiente, si la organización pretende alcanzar el nivel de madurez, requerirá la tercerización parcial o total del servicio mediante un MSSP (seleccionandolo de acuerdo a su presupuesto disponible en ciberseguridad). En los casos en que la tercerización del servicio sea parcial, los miembros contratados directamente por la organización deberán trabajar colaborativamente con el MSSP, usualmente consumiendo y procesando la ciberinteligencia resultante de estos y retroalimentando al MSSP con valor agregado relacionado a la organización, para la ejecución conjunta de prácticas de Threat Hunting cuando sea posible.

Las organizaciones con 250 miembros o más (Empresas grandes) pueden ser muy disímiles entre sí, pero la cantidad de miembros no tiende a ser determinante en la posibilidad de gestionar el servicio de manera interna o tercerizada. La facturación anual o valor en activos tiende a mantener una relación directa con la inversión destinada en ciberseguridad. Las organizaciones con mayor inversión en ciberseguridad tendrán la posibilidad de elegir cómo gestionar el servicio. De optar por la gestión interna, podrán competir

para la contratación directa de profesionales incluso ante la escasez de profesionales del sector.

Resulta importante comprender que incluso las empresas más maduras en ciberseguridad utilizan en mayor o menor medida algún servicio de MSSPs, pero en general se restringe a consumir información provista por estos, por lo que no se requiere una relación de confianza inversa que ponga en riesgo información de la organización contratante. Sin embargo, aquellas organizaciones consideradas grandes que no pueden competir en la contratación directa para atraer profesionales calificados, deberán obligadamente subcontratar total o parcialmente los servicios de un MSSP otorgándoles confianza suficiente para acceder al menos parcialmente a su información y/o infraestructura. Esto representa un problema, ya que los MSSP son un objetivo muy atractivo para múltiples actores maliciosos, como las amenazas persistentes avanzadas (APT), los grupos organizados de ciberdelincuencia o los grupos organizados de ciberterrorismo. Este tipo de ataques en que se vulnera un MSP, CSP o MSSP para lograr vulnerar otras organizaciones se denominan “ataques a la cadena de suministro” (*Supply chain attacks* o *Island Hopping*) y de acuerdo al reporte “Global Incident Response Threat Report” de VM-Ware Carbon Black de 2019[36], el 50 % de todas las brechas de seguridad utilizan este vector. Se han visto diversos casos de empresas que brindan servicios de ciberseguridad vulneradas como SolarWinds[37], Malwarebytes[38], Kaspersky[39], LastPass[40], BitDefender[41], Cyberoam (Sophos)[42], FireEye (Mandiant)[43], Microsoft[44], OKTA[45], IBM y HPE[46] entre otros. En 2019, CISA advirtió que APTs estaban explotando activamente MSP[47], y en 2020 el Servicio Secreto de Estados Unidos emitió un comunicado advirtiendo sobre un incremento en brechas de seguridad sobre MSPs en general[48]. Si (o, cuando) estos atacantes logran vulnerar la infraestructura del MSSP, tendrán por esta relación de confianza entre ambos, acceso a información con clasificación no pública que la organización debe necesariamente haber compartido con el MSSP para que este provea sus servicios de ciberinteligencia y/o Threat Hunting. Este problema existe también para organizaciones de menor tamaño que contrataron al MSSP, pero afecta en mayor medida a las más grandes (o bien a las que administran información más sensible) ya que los actores maliciosos tendrán como objetivo principal a estas organizaciones y no al MSSP mismo (ni a organizaciones más pequeñas o con información menos sensible).

La solución ideal para una organización que afronta este inconveniente, sería poder mantener la relación de confianza con el MSSP ajustando al máximo sus controles de seguridad preventivos a fin de disminuir la información compartida y acceso otorgado entre las partes. Alcanzar este objetivo satisfactoriamente implica la implementación en toda la infraestructura de conceptos como defensa en profundidad (*Defense-in-depth*) y modelos de seguridad de confianza cero (*Zero Trust*) entre otros. Lograr estas características es complejo y alcanzado únicamente por las organizaciones más

maduras en ciberseguridad.

Alternativamente, las organizaciones pueden migrar a una gestión de servicio interna que les permita disminuir la dependencia del MSSP, logrando una relación de confianza en la que el MSSP no necesite acceso a información sensible ni a infraestructura de la organización, y a su vez esta pueda consumir información e inteligencia del MSSP. Teniendo en cuenta las restricciones presupuestarias para la contratación directa de personal ya calificado para estas prácticas, una opción viable es la de aumentar la inversión en la capacitación del personal interno (o bien contratar personal sin los conocimientos necesarios pero que busquen formarse en ellos). En los casos en que las organizaciones no dispongan de presupuesto suficiente para llevar adelante la capacitación (y/o adquisición de soluciones), los profesionales del equipo de ciberseguridad deberán recurrir a la formación en base a recursos gratuitos y a la implementación de herramientas gratuitas. De aquí surge una creciente necesidad por soluciones simples que incluyan herramientas gratuitas (parcial o totalmente), bien documentadas para su aprendizaje y efectivas para las prácticas de ciberinteligencia y Threat Hunting. Idealmente las organizaciones en esta situación necesitaran que las soluciones asistan a los profesionales de ciberseguridad en los procesos y metodologías más básicos de estas prácticas:

1. El proceso II de ciberinteligencia: Recolectar información e identificar IoCs sobre actores maliciosos emergentes y existentes.
2. El proceso V de ciberinteligencia: Identificar el nivel de exposición de información de la organización y sus miembros.
3. La metodología basada en inteligencia de Threat Hunting.
4. La metodología basada en datos de Threat Hunting.

3.2. Especificación de requisitos

A fin de analizar las soluciones existentes, se debe comprender que se requiere para implementar cada uno de los procesos y metodologías:

- El proceso II de ciberinteligencia requiere de fuentes abiertas que compartan IoCs confiables en un formato que pueda ser utilizado por la organización. La sección “Sources” del repositorio “Awesome-Threat-Intelligence”[49] de GitHub provee un extenso listado de fuentes gratuitas desde las cuales una organización podrá recolectar IoCs. La selección de qué fuentes se utilizará dependerá de cuánta confianza cada organización asigne a las diferentes fuentes y que el formato de compartición de IoCs de la fuente sean compatibles (o adaptables) al formato requerido por la organización. El formato que la organización va a requerir para los IoCs dependerá del nivel de automatización que desee implementar para esta tarea, y esto en gran medida dependerá de las soluciones de seguridad preexistentes que consuman estos IoCs. Preferentemente, y como se mencionó en la Sección 1.4.2, se debería automatizar este proceso para que los IoCs sean consumidos por las soluciones de seguridad preexistentes como cortafuegos (*Firewalls*), SIEMs, Sistemas de orquestación, automatización y respuesta de seguridad (SOAR), etc; ya sea con fines preventivos (bloqueo) o detectivos (alertas). No existe un conjunto de herramientas específicas para automatizar esta tarea, ya que dependerá de la solución misma y por lo tanto se deberá referir a la documentación de cada una para verificar cómo configurarlo y que formato de IoCs acepte. La sección “Formats” del repositorio de Github mencionado, lista algunos de los formatos más conocidos y utilizados para compartir y recolectar los IoCs, como STIX y TAXII.
- El proceso V de ciberinteligencia requiere por un lado de herramientas para la fase de recolección mediante footprinting y fingerprinting (pasivo y activo), que en base a un dato concreto (nombre de una organización, nombre completo de una persona, un dominio, un usuario, una Dirección IP, un email, etc.) puedan recolectar otros datos e información relacionada, y por otro lado de herramientas para la fase de procesamiento que permitan introducir contexto, correlacionar y visualizar los datos e información.
- La metodología basada en inteligencia de Threat Hunting requiere de un flujo de IoCs que se buscarán en los registros de eventos históricos para determinar si fueron vistos durante el periodo de tiempo previo a cuando fueron configurados para bloquear o alertar en los sistemas de seguridad. Las búsquedas de estos IoCs dependen de las soluciones de seguridad preexistentes donde estos registros se almacenan, sien-

do el soporte de YARA y reglas SIGMA preferentes para esta tarea. SOC Prime desarrollo Uncoder[50] que permite la conversión de reglas SIGMA a consultas de SIEM específicos de múltiples marcas y CTI Uncoder[51] que construye búsquedas en base a IoCs.

- La metodología basada en datos de Threat Hunting requiere indispensablemente de acceso a un almacén de datos (por ejemplo, un SIEM) que nos permita hacer consultas o bien de herramientas para recolectar estos datos, como “tcpdump” (para capturar comunicaciones de red, nativa en la mayoría de las distribuciones del sistema operativo Linux), y preferentemente de herramientas para detectar patrones como “Real Intelligence Threat Analytics” (RITA)[52].

Puede concluirse entonces que:

1. El proceso II de ciberinteligencia y la metodología basada en inteligencia de Threat Hunting pueden aprovechar las ventajas que proporcionan ciertas herramientas siempre y cuando sean soportados por las soluciones de seguridad preexistentes.
2. El proceso V de ciberinteligencia y la metodología basada en datos de Threat Hunting son muy disímiles entre sí y no comparten herramientas o requerimientos.

Dada la problemática observada y las conclusiones obtenidas, se considerarán **soluciones que cumplan las siguientes características:**

A Provean o asistan en:

- Las fases de recolección, procesamiento y/o análisis del ciclo de Ciberinteligencia para el proceso (V) mediante la disciplina OSINT. Se omite la fase de planificación ya que está predefinida por lo antepuesto.
- Técnicas estadísticas de la metodologías de Threat Hunting basadas en datos.

B Sean efectivas en las funciones que digan ejecutar.

C Gratuitas (en su totalidad o parcialmente).

D Actualizadas al menos una vez en los últimos 18 meses. Esto resulta imprescindible por la rápida evolución de las políticas de privacidad alrededor de la información disponible en internet, la dinámica de las tecnologías en general y de los diferentes espacios desde donde estas soluciones recopilan datos e información en particular.

E Tengan suficiente documentación para permitir su aprendizaje de manera autónoma.

F Provea resultados que puedan ser interpretados y comprendidos por un profesional de ciberseguridad que tenga los conocimientos teóricos en materia de ciberinteligencia y Threat Hunting, aunque no disponga de experiencia previa en estas prácticas.

Se omite del análisis de soluciones el siguiente requerimiento, ya que dependiendo del nivel de sensibilidad asociado a la información de la organización, podría resultar más o menos relevante:

- Las herramientas deberán indicar con claridad en sus términos y condiciones que no almacenan los datos recolectados para sí mismos.

Las soluciones se pueden definir como:

- **Soluciones individuales.** Es decir, herramientas online (ejecutadas mediante un navegador web) u offline (descarga de software que se ejecuta localmente).
- **Soluciones empaquetadas.** Es decir, Máquinas virtuales (VMs, por sus siglas en inglés *Virtual Machine*) o Contenedores que agrupan un conjunto de soluciones individuales preexistentes. En este apartado se incluyen las secuencias de comandos ejecutables (*Scripts*) que en base a un Sistema Operativo dado realizan la descarga, instalación y configuración de múltiples soluciones individuales.

Mayormente las soluciones empaquetadas orientadas a Ciberinteligencia y Threat Hunting se encuentran en máquinas virtuales, debido a que los contenedores tienen una naturaleza más efímera y es poco usual encontrar múltiples soluciones agrupadas en ellos.

Las soluciones individuales a considerar deberán cumplir con los requisitos antes mencionados, y las soluciones empaquetadas deberán cumplir con los requisitos antes mencionados en todas las soluciones individuales que contengan y para sí mismas.

3.3. Pruebas de concepto

3.3.1. Selección de sector

El panorama de amenazas para la industria educativa:

El sector de Servicios Educativos, o Industria Educativa, está comprendida por establecimientos que brindan instrucción y capacitación en una amplia variedad de temas, siendo los más reconocidos las escuelas, colegios, universidades, y centros de capacitación. En general también son incluidos dentro de este sector los organismos y centros de investigación y desarrollo, sean privados o públicos. De acuerdo al reporte “EdTech Market” de 2022[53], se estima que el valor de la industria en 2021 era de 254,8 mil millones de dólares y se estima que crecerá a 605,4 mil millones de dólares para 2027. Este rápido crecimiento está potenciado por las consecuencias de la pandemia del COVID-19, que llevó a la obligatoriedad de migrar rápidamente muchos de los servicios de estas organizaciones a una modalidad online o híbrida. Estadísticas que demuestran el incremento de amenazas hostiles contra el sector:

- El reporte de ciberseguridad de Check Point de 2021[54], muestra que la industria educativa lidera el ranking de incremento anual de ataques reportados, con un 75 % más que el año anterior.
- En la figura 8 del reporte “The state of Encrypted attacks” de ZScaler de 2021[55], se observa que la industria educativa recibió un 50 % más de ataques sobre protocolos cifrados que en el año anterior. Dada la dificultad de ejecución de estos ataques, es evidente que la industria está siendo objetivo de amenazas más avanzadas debido a la sensibilidad que tiene la información que gestionan.
- La sección “Threats to sectors and vectors” del reporte de amenazas de Trellix de junio 2021[56], destaca que el sector educativo recibió un 46 % más de malware que en cuatrimestres anteriores. En ese sentido se observa también cómo el sector educativo tuvo un 100 % más de incidentes de ciberseguridad que en el cuarto cuatrimestre de 2019.
- En la figura 13 del reporte del panorama global de amenazas de Fortinet del segundo semestre de 2021[57], se observa que la infección de sistemas generada a partir de la ejecución manual de malware por parte de usuarios es de 32 %, afectando a la industria educativa más que a cualquier otra.
- La sección “The Future of Ransomware” del reporte “Navigating cybersecurity in an uncertain world” de Sophos de 2021[58] remarca como el sector educativo se a vuelto el campo de batalla y objetivo de múltiples actores maliciosos que utilizan diferentes familias de Ransomware en sus ataques.

- Un reporte del World Economic Forum de 2021[59] demostró que el sistema educativo es la segunda industria más afectada por casos de Ransomware reportados, con un total de 35.
- El reporte “Threat Landscape Retrospective” de Tenable de 2021[60] observa que el 13% de las brechas de ciberseguridad corresponden a la industria educativa y el 52% de esas brechas se corresponde con ataques que utilizaron Ransomware.
- La figura 1 del reporte “Top New Attacks and Threats” de SANS de 2021[61] muestra que la industria educativa sufrió 24 brechas de seguridad con un total de 110000 individuos afectados durante 2020.
- El reporte “Cost of a Data Breach Report” de IBM de 2021[62] observa que el sector educativo sufrió pérdidas por 3,8 millones de dólares durante el año previo debido a brechas de seguridad.
- En la sección “Industry failure rates” del reporte “State of the Phish” de Proofpoint de 2022[63] se observa que en el sector educativo en promedio un 10% de las personas que reciben un correo de tipo Phishing son víctimas del ataque. El reporte resulta especialmente relevante teniendo en cuenta que España fue uno de los 7 países seleccionados para el análisis.

El panorama de amenazas para las Universidades:

Las universidades siempre han tenido un rol central como centros de desarrollo e investigación de nuevas tecnologías aplicadas a diferentes ámbitos e industrias. El ejemplo más evidente es la Internet misma, creada en 1969 y conocida como ARPANET (*Advanced Research Projects Agency Network*), conectaba a 4 computadoras de 4 universidades distintas de Estados Unidos. Debido a la información sensible relacionada a investigaciones y nuevas tecnologías que suelen gestionar las universidades, el reporte de ciberamenazas para la industria Educativa de Mandiant de 2016[64] resaltaba cómo las universidades son un objetivo cada vez más usual para APTs. Esto se vio reflejado el 15 de mayo de 2020 cuando la empresa Cado Security reportó que un Malware dirigido a supercomputadoras en Universidades fue observado en España, Alemania, Inglaterra y Suiza[65]. En la actualidad se suma la creciente dificultad para administrar y securizar sus redes y sistemas debido al rápido incremento de usuarios que causó la pandemia del COVID-19.

Las instituciones de educación superior siempre han mantenido infraestructuras más abiertas que otras organizaciones, con el fin de favorecer la cooperación y colaboración entre estudiantes e investigadores y proveer un libre flujo e intercambio de información con colegas alrededor del mundo. El informe “Working Remote: How Universities Secure Open Networks” de Cybereason de 2019[66] destaca cómo por esta razón son objetivos particularmente atractivos para los atacantes, recibiendo hasta 9 veces más ataques

informáticos que la organización promedio.

Estadísticas que demuestran el incremento de amenazas hostiles contra las universidades:

- El reporte “Digital Defense” de Microsoft de 2021[67] detalla que al menos 1 APT de origen Ruso y 3 APTs de origen Chino tienen como objetivo de sus ataques a instituciones universitarias.
- El reporte de protección de aplicaciones “Of Ransom and Redemption” de F5 de 2021[68] detalla que los servicios educacionales (ej: Plataformas educativas online) fueron la segunda industria más afectada por fugas de información, representando el 16,6 % del total (116 incidencias totales observadas). Se observa especialmente el caso donde al menos 201 universidades se vieron afectadas luego de un ataque contra la plataforma PrismRBS y otro caso (con un número indeterminado de víctimas) contra la plataforma educativa “Aeries Student Information System”.
- En la tabla 7 de la sección “E-Mail related threats” del reporte del panorama de amenazas de ENISA de 2021[69], se destacan ataques de adversarios avanzados a 25 Universidades distintas mediante campañas de Spear-phishing. Adicionalmente, en la subsección de recomendaciones (4.2) de la sección de Malware (4) se destaca la implementación de prácticas de Threat Hunting basada en inteligencia como mitigación.

El panorama de amenazas en España:

El estudio “Top 20 Countries Found to Have the Most Cybercrime”[70] muestra que España es el sexto país a nivel mundial (tercero en Europa) con mayor índice de ciberdelincuencia. Además, el reporte “Which EU Country Is Most Vulnerable To Cybercrime?”[71] indica que si bien España tiene una proporción alta de acceso a Internet de sus habitantes (76 %), es el cuarto país de Europa más vulnerable a ataques informáticos.

Estadísticas que demuestran el incremento de amenazas hostiles contra el país:

- El reporte de amenazas de Ransomware de Palo Alto Networks de 2021[72] reconoce durante 2020 un total de 3 organizaciones víctimas de Ransomware en España cuyos datos fueron publicados, 10 organizaciones víctimas en la industria Educativa a nivel mundial y 3 cepas distintas de Ransomware que estaban destinadas a la industria educativa específicamente.
- El análisis presentado en “España, en el punto de mira” durante la XV Jornadas STIC CCN-CERT por Miguel Ángel de Castro[73] detalla como España es objetivo de ataques de adversarios avanzados de distintos tipos (APTs, organizaciones cibercriminales, etc).

- La sección “Exploits” del reporte de amenazas de tercer trimestre de 2021 de ESET[74] muestra que España es el país que más intentos de adivinar contraseñas recibió globalmente, coincidiendo con el descubrimiento de la vulnerabilidad conocida como Log4Shell.

El panorama de amenazas para las Universidades de España:

El reporte “Estadísticas de Estudiantes Universitarios” del Sistema Integrado de Información Universitaria del Ministerio de Universidades del Gobierno de España[75] muestra un incremento interanual del número de estudiantes universitarios de grado y posgrado. Además, España es el país que más estudiantes recibe de Europa mediante el programa Erasmus, y el tercero que más estudiantes envía al exterior[76].

Estadísticas y eventos que demuestran el incremento de amenazas hostiles contra Universidades Españolas:

- El estudio de ciberseguridad sobre las principales universidades de España realizado por Deloitte en 2018[77] menciona 6 ataques sobre estas entidades ocurridos durante 2017 que han sido reportados a medios de comunicación. El cuestionario enviado a las universidades participantes refleja que las mismas tienen entre 0 y 5 recursos dedicados a la seguridad de la información y en ningún caso el presupuesto destinado a ciberseguridad supera el 10 % del presupuesto asignado a tecnología de la información. En general se calculó un nivel de madurez medio de 1,58 sobre 5 puntos.
- El 25 de febrero de 2022 la Universidad de Oviedo sufrió un ataque de denegación de servicio con direcciones IP de origen Ruso[78].
- El 11 de octubre de 2021 la Universidad Autónoma de Barcelona (UAB) sufrió un ataque de Ransomware que dejó sin servicio a la mayoría de sus sistemas[79].
- El 03 de enero de 2022 la Universidad Oberta de Catalunya (UOC) sufrió un ataque de Ransomware que dejó sin servicio a muchos de sus sistemas[80].
- El 18 de abril de 2021 la Universidad de Castilla-La Mancha (UCLM) sufrió un ataque de Ransomware que la obligó a cortar la conectividad externa[81].

3.3.2. Selección de organismo

La **Universidad de Granada (UGR)** es una universidad pública española con su sede principal ubicada en la provincia de Granada. Es la cuarta universidad de España por número de estudiantes y se ubica entre las 300 mejores universidades del mundo según la clasificación del Ranking Académico de las Universidades del Mundo (ARWU)[82]. La UGR tiene 5500 personas contratadas (docentes, administrativos, técnicos y personal de servicio), por lo que se considera una organización grande[83].

Basado en el presupuesto anual de 2022 publicado por la Dirección de Asuntos Económicos del equipo de Gerencia de la UGR[84], las siguientes previsiones presupuestarias son detalladas:

- El área de formación del PAS (Personal de Administración y Servicios, unidad encargada de la gestión administrativa del personal de la UGR), tiene un presupuesto de 140.441,00€ destinado a un conjunto de más de 30 actuaciones entre los que se observa “Seguridad de la información”, sin dar mayor detalle sobre ello. En ese sentido, se observan algunas iniciativas desde su sitio web orientadas a la formación de personal, pero no orientadas a la implementación de controles.
- El CSIRC cuenta con un presupuesto total de 2.866.740,32€ destinado a sus diferentes actuaciones, entre las cuales se destacan:
 - La actuación “Licencias software” con 775.353,54€ que podría englobar alguna inversión en software de ciberseguridad en determinados casos específicos.
 - La actuación “Servidores y almacenamiento (SisGes, SisInves, Micro, Plat. Educativas, Apoyo a la docencia, Telefonica, Seguridad Informatica)” con 271.000,00€, que parece englobar múltiples vectores de tecnología que no necesariamente incluyen aspectos de ciberseguridad, por lo que se podría estimar que solo un porcentaje de este número sería destinado a la Seguridad Informática.

Al ser previsiones presupuestarias, estos números podrían variar, pero muestran un panorama que permite estimar una inversión de ciberseguridad baja por parte de la entidad.

En la Figura 3.1 puede verse un ejemplo de servicio básico de ciberinteligencia provisto por un MSSP reconocido, específicamente para Universidades Públicas. Puede concluirse que el mismo sería casi inaccesible dada la inversión actual en ciberseguridad (El precio indicado es anual).

CYBERTHREATS UNIVERSIDADES

ROBO DE CREDENCIALES HASTA 5 DOMINIOS

Monitorizamos de forma continua **plataformas de posteo y mercados underground de la Deep Web** en busca de emails con contraseñas de alumnos y profesorado que se hayan visto expuestos públicamente y/o hayan sido comprometidos y recolectados por **bótnets**.

En colaboración con [Logo]

INFORME DE TENDENCIAS MENSUAL

Nuestro experto equipo de analistas elabora, con carácter mensual, **informes de tendencias** analizando la **evolución de las principales ciberamenazas y riesgos digitales** a los que se encuentra expuesto el sector Académico, tanto a nivel nacional como internacional.

BOLETÍN NOTICIAS SEGURIDAD SEMANAL

Se recopilan noticias de seguridad de carácter genérico (**fugas de información masivas, leyes y regulaciones, malware, vulnerabilidades...**), así como aquellas directamente relacionadas con el sector Académico y se entregan semanalmente a través de un boletín de noticias.

3 INVESTIGACIONES BAJO DEMANDA

Ponemos a disposición de la universidad nuestro equipo de analistas para realizar **investigaciones a medida bajo demanda** sobre cuestiones de especial interés, relacionadas con **riesgos digitales que puedan afectar al ámbito Académico** (operaciones **hacktivistas**, fugas de información, **phishing**, ataques dirigidos...).

P.V.P = 14.800 € / universidad

Figura 3.1: Folleto de servicios de Ciberinteligencia ofrecidos por MSSP a Universidades públicas.

Dentro del CSIRC, el personal del equipo de Seguridad Informática es de 2 individuos[85].

Existen otras áreas que probablemente tendrán asignadas actividades, tareas y controles de ciberseguridad vinculados a los activos que gestionan (Redes y Comunicaciones con 11 individuos, Servicios de Identidad Digital con 3 individuos, Administración y Gestión de Sistemas de Bases de Datos Corporativas con 4 individuos, Plataformas Web Corporativas con 3 individuos, Microinformática con 5 individuos, Servicios Telemáticos con 5 individuos, etc.), pero será poco probable que puedan asignar su tiempo en gran medida para la detección proactiva de amenazas.

El “Network Engineering & Security Group” (NESG)[86] es una agrupación de integrantes de múltiples departamentos de tecnología de la UGR con el objetivo de unificar esfuerzos y metas. Entre sus proyectos públicos relacionados a seguridad informática, se destaca el denominado “Information Leakage Detection in the Deep Web”[87] que tiene como objetivo el despliegue de un sistema de monitorización de información en la Deep web. Sin embargo, el proyecto iniciado en 2015 aún se encuentra en estado “en progreso”, por lo que se puede estimar que su despliegue aun no esta operativo (Posiblemente pausado o aun en fase de desarrollo).

Por fuera de la UGR, existen entidades que le proveen servicios de ciberseguridad:

- AndalucíaCERT[88] es el centro de gestión de la seguridad de las tecnologías de la información y la comunicaciones de la Junta de Andalucía. Si bien entre sus servicios ofrecidos se encuentra la “Alerta temprana de ciberamenazas”, el alcance del servicio parece ser limitado y no englobar ciberinteligencia. El sitio web indica que se puso en marcha en 2010-2013, pero no existe un sitio web específico del cual obtener infor-

mación adicional y por lo tanto se puede considerar como un servicio de ciberseguridad de madurez baja.

- IRIS-CERT[89] es el equipo de respuesta a incidentes de computacion de la RedIRIS (acronimo de “Red para la Interconexión de los Recursos InformáticoS”, red que provee servicios de conexión entre universidades y centros de investigación españoles) no ofrece servicios que se encuentren en las prácticas de ciberinteligencia o Threat Hunting.
- El INCIBE-CERT[90] (Instituto Nacional de Ciberseguridad - Computer Emergency Response Team) es el Centro de Respuesta a Incidentes de Seguridad de INCIBE, dependiente del Ministerio de Asuntos Económicos y Transformación Digital. En ese sentido, lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional. Provee un servicio de recolección de información para detección proactiva basado en OSINT denominado IGA[91] (*Information Gathering*) destinado a infraestructuras críticas. El catálogo de infraestructuras críticas es administrado por el CNPIC[92] (Centro Nacional de Protección de Infraestructuras y Ciberseguridad) y según el Real Decreto 704/2011[93] es clasificado como Secreto, por lo que no es posible determinar si este servicio puede ser consumido por Universidades.
- El CCN-CERT (Centro Criptológico Nacional - Computer Emergency Response Team) es el organismo estatal Español dependiente del CNI encargado de contribuir a la ciberseguridad de la administración pública, los organismos públicos y empresas estratégicas del país. Entre los servicios que provee, se encuentra un conjunto de soluciones de ciberseguridad que pueden ser implementadas por cualquier organismo público. Relacionadas a la ciberinteligencia y/o el Threat Hunting se destacan:
 - CARMEN[94] (Centro de Análisis de Registros y Minería de EveNTos): Solución para identificar el compromiso de la red de una organización por parte de amenazas persistentes avanzadas (APT).
 - IRIS (Indicadores Relacionados para Información de la Situación): Solución para conocer en tiempo real el estado de la ciberseguridad del sector público y la situación de la ciberamenaza a nivel nacional.
 - REYES[95]: Solución donde se comparte información de amenazas para organismos públicos. El Informe anual de 2021 del CCN-CERT[96] presentado en la XIV Jornada STIC CCN-CERT revela que algunas fuentes de información utilizadas por esta solución son las herramientas de BinaryEdge, SecurityTrails, WebArchive, Urlscan y Trillion.

- ELENA[97]: Simulador de cibervigilancia para promover la capacitación de profesionales en tácticas, técnicas y procedimientos de ciber investigación para la prevención y análisis de ciberamenazas.

El documento “Quién es quién en el sector de la Seguridad TIC en España”[98] detalla otras entidades oficiales, pero no se destaca ninguna por fuera de las ya mencionadas que provea servicios adicionales para asistir en la gestión de servicios de ciberinteligencia o Threat Hunting.

Existen otras entidades no oficiales como REN-ISAC y SAFER, que se definen como agrupaciones orientadas a coordinar esfuerzos para abordar los problemas de ciberseguridad que afronta la industria educativa en general, pero no proveen servicios específicos.

En lo que a ataques recibidos refiere, el único evento reportado públicamente[99] por la UGR ocurrió el 21/01/21 entre las 10:00 y las 14:00, cuando la Plataforma de Recursos de Apoyo a la Docencia (PRADO) sufrió un ataque distribuido de denegación de servicio (DDOS) que generó incidencias en 13 exámenes online programados para la jornada.

Basándose en la información presentada sobre la UGR (organización grande, bajo presupuesto de ciberseguridad, madurez media en ciberseguridad, historial de ataques públicos bajo y acceso a servicios de ciberinteligencia básicos mediante otros organismos), es posible concluir que sería un candidato idóneo para las pruebas de concepto de las soluciones existentes.

Las pruebas de concepto realizadas en el Sección 3.4 sobre la Universidad de Granada (UGR) de España fueron coordinadas y autorizadas por el jefe del equipo de Seguridad Informática del Centro de Servicios Informáticos y Redes de Comunicación (CSIRC) de la entidad, y tutor de este trabajo de fin de máster, Antonio Muñoz Ropa. El punto de inicio para las pruebas de concepto fue el dominio principal asociado a la entidad, “ugr.es”.

3.4. Análisis de soluciones existentes

3.4.1. Soluciones de Ciberinteligencia

Tanto en el campo de la Ciberinteligencia como en el de la Seguridad Ofensiva la recolección de información mediante disciplinas OSINT se encuentra sumamente desarrollado. Al observar colecciones de recursos OSINT como OSINTFramework.com[100], OSINTTechniques.com[101], Awesome-OSINT[102], Ciberpatrulla.com[103], cipher387.github.io[104] y hatless1der.com se[105] concluye que:

- A Las soluciones disponibles se cuentan por miles, por lo que relevan todas ellas resultaría una tarea ingente. Las soluciones son también muy dinámicas, muchas dejan de ser mantenidas o desaparecen, siendo reemplazadas por nuevas en la mayoría de los casos, por lo que la tarea también resultaría superflua. Además, las soluciones pueden ser muy específicas o muy generales, cumpliendo una función única o múltiples funciones, por lo que el relevamiento respecto a su eficacia, eficiencia o alcance será muy subjetivo respecto a las necesidades puntuales de la organización que les de uso. Se concluye entonces que se deberán priorizar las soluciones que sean multipropósito y multifunción, por sobre aquellas que cumplan funciones demasiado específicas o únicas.
- B A pesar de que existen soluciones multipropósito y multifunción ampliamente desarrolladas y avanzadas, no existe una única que sea capaz de abarcar todas las tareas de investigación y análisis que abarcan este proceso. Por lo tanto, es necesario priorizar soluciones empaquetadas. Agrupar suficientes soluciones individuales en una única solución que tenga valor al propósito de las diversas organizaciones, resultaría en una solución excesivamente grande en términos de espacio y abrumadora para un analista, por lo que la solución empaquetada deberá incluir las soluciones mencionadas en el punto anterior.
- C Existen ya soluciones que cumplen los puntos A y B, pero debido al solapamiento observado entre los procesos de la práctica de ciberinteligencia y el campo de la seguridad ofensiva, suelen incluir mayoritariamente recursos y herramientas para fases posteriores de Pentesting (es decir, por fuera de lo que se pretende o necesita en estos casos), resultando soluciones agobiantes o demasiado complejas para un analista de ciberinteligencia iniciando en esta práctica. Ejemplos de ello son las distribuciones Archstrike, Backbox, BlackArch, Kali, Parrot OS y Pentoo entre otras, razón por la cual se deben priorizar soluciones empaquetadas centradas en la ciberinteligencia o bien exclusivamente en la fase de reconocimiento de Pentesting.

Por otro lado, no se han contemplado soluciones empaquetadas que están orientadas a la anonimización como Tails o Whonix, ni soluciones empaquetadas orientadas a la endurecimiento (*hardening*) como Subgraph.

En resumen, idealmente se desea una solución empaquetada orientada a OSINT o la fase de Reconocimiento de Pentesting que contenga principalmente soluciones individuales multipropósito y multifunción. Tras un relevamiento se observa en la Tabla 3.1 las 13 soluciones encontradas que entran dentro de esta categoría:

Nombre	Actualizado	Documentación	Empaquetado	Notas
Buscador	19-01	Suficiente	VM	EOL. Originada en IntelTechniques
Huron	19-07	Suficiente	VM	-
Dora	20-02	Insuficiente	VM	Basada en IntelTechniques.
Osintux	20-08	Suficiente	VM	Proyecto de TFM (UCAM).
Trace Labs	22-01	Suficiente	VM	Orientada a la búsqueda de personas desaparecidas.
OffenOsint	21-08	Suficiente	VM	Orientada a la fase de reconocimiento de OffSec.
Argos	21-04	Suficiente	Script	Basada en IntelTechniques.
ns21osint	21-12	Suficiente	Script	Proyecto de TFM (ENIIT).
x0rzkov/docker-osint	19-08	N/A	Contenedor	-
fractalizers/osint	20-03	Insuficiente	Contenedor	-
vaultsecurity/osint	20-08	Suficiente	Contenedor	-
marcospr1974/Docker-OSINT	21-01	Suficiente	Contenedor	Múltiples contenedores agrupados.
kasmweb/tracelabs	21-12	No	Contenedor	Beta. Interfaz web. Basada en Trace Labs.

Tabla 3.1: Soluciones empaquetadas de Ciberinteligencia.

Solamente 4 de ellas (2 VMs y 2 Scripts) cumplen la características de ser gratuitas, haber sido actualizadas en los últimos 18 meses y estar suficientemente documentadas, que a continuacion se analizan individualmente. La mayoría de las soluciones empaquetadas se basan en Kali Linux o en alguna edición del libro “Open Source Intelligence Techniques” [106], que en la “Sección 1” provee instrucciones detalladas para la preparación y construcción de una máquina virtual para OSINT.

Trace Labs es una organización sin fines de lucro cuya misión es acelerar la reunificación familiar de personas desaparecidas al mismo tiempo que se provee capacitación en la inteligencia de fuente abierta (OSINT). Además del equipo principal que lo forma, Trace Labs es también una comunidad abierta en la cual se puede participar de iniciativas/operaciones de búsqueda. Para ello, han desarrollado la máquina virtual denominada Trace Labs OSINT VM (TL), basada en Kali Linux pero solamente con recursos y herramientas para asistir en una investigación OSINT. La Figura 3.2 muestra el escritorio del Sistema Operativo de la Máquina Virtual.

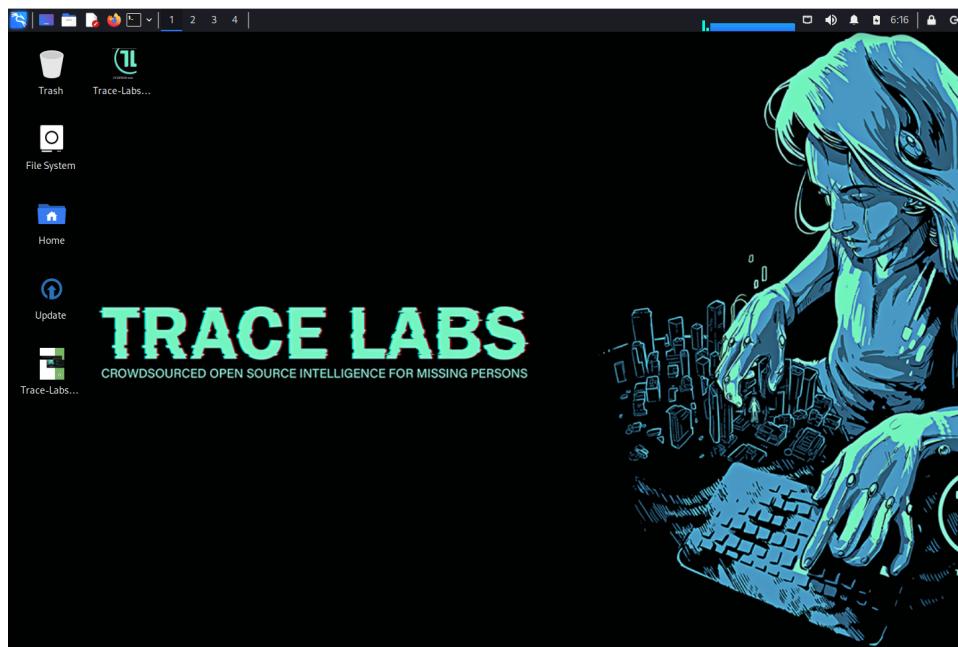
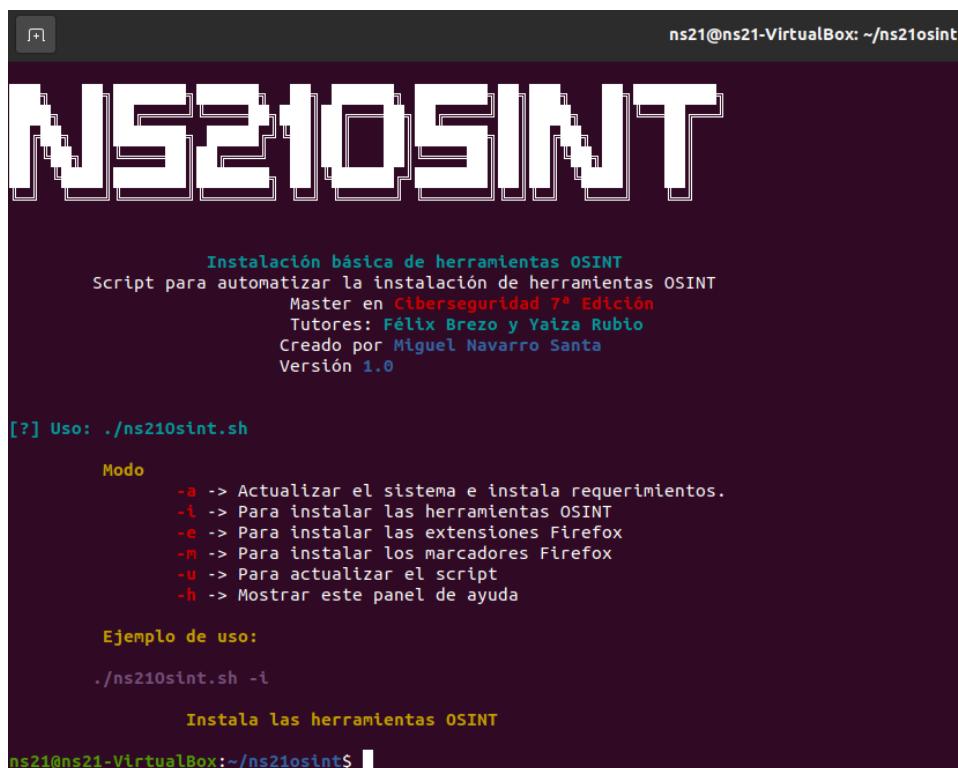


Figura 3.2: Captura de pantalla del escritorio del Sistema Operativo Trace Labs.

- Fortalezas: Mantenido por una organización con respaldo de una comunidad, incluye instrucciones para despliegue en contenedores. Al estar basado en Kali, las herramientas que pueden estar faltando suelen ser fácilmente instalables.
- Deficiencias: Contiene herramientas no actualizadas en los últimos 18 meses. La documentación es correcta, pero existen leves diferencias entre las herramientas que dice integrar según su repositorio de github, según la documentación del sitio web y lo que realmente existe en la máquina virtual. Faltan herramientas de fingerprinting y escaneo de vulnerabilidades debido a que está orientada a la búsqueda de personas.

ns21osint es un Script desarrollado por Miguel Navarro como parte de su Trabajo Final de Máster de Ciberseguridad, el cual en base a la distribución Ubuntu 20.02 LTS de Linux, instala un conjunto de recursos y herramientas OSINT. La Figura 3.3 muestra las opciones de ejecución del Script.



The screenshot shows a terminal window with the following content:

```
ns21@ns21-VirtualBox: ~/ns21osint
[?] Uso: ./ns21osint.sh

Modo
-a -> Actualizar el sistema e instala requerimientos.
-i -> Para instalar las herramientas OSINT
-e -> Para instalar las extensiones Firefox
-m -> Para instalar los marcadores Firefox
-u -> Para actualizar el script
-h -> Mostrar este panel de ayuda

Ejemplo de uso:
./ns21osint.sh -i

Instala las herramientas OSINT
ns21@ns21-VirtualBox:~/ns21osint$
```

Figura 3.3: Captura de pantalla del menú de ayuda del Script ns21Osint.sh.

- Fortalezas: Disponible en español. Instalacion facil y rapida. La mayoría de soluciones son multifunción y multipropósito, casi todas las herramientas contenidas se mantienen actualizadas.
- Deficiencias: Faltan herramientas de fingerprinting y escaneo de vulnerabilidades. Mantenido únicamente por su creador (falta una comunidad para respaldar el proyecto).

Argos es un Script desarrollado por Alessandro Rossetti en base a la 7ma edición del libro “Open Source Intelligence Techniques”, el cual en base a la distribución Ubuntu 20.04 LTS de Linux, instala un conjunto de recursos y herramientas OSINT. La Figura 3.4 muestra el escritorio del Sistema Operativo de la Máquina Virtual luego de ejecutar el Script.



Figura 3.4: Captura de pantalla del escritorio del Sistema Operativo luego de la ejecución del Script de Argos.

- Fortalezas: Instalación simple, el conjunto de soluciones incluidos es bastante amplio.
- Deficiencias: Contiene herramientas no actualizadas en los últimos 18 meses. El script falla silenciosamente al instalar herramientas importantes como Maltego y theHarvester. Faltan herramientas de finger-printing y escaneo de vulnerabilidades. Mantenido únicamente por su creador (falta una comunidad para respaldar el proyecto).

Offensint es una máquina virtual orientada a la fase de reconocimiento de seguridad ofensiva basada en Kali Linux. La Figura 3.5 muestra el escritorio del Sistema Operativo.

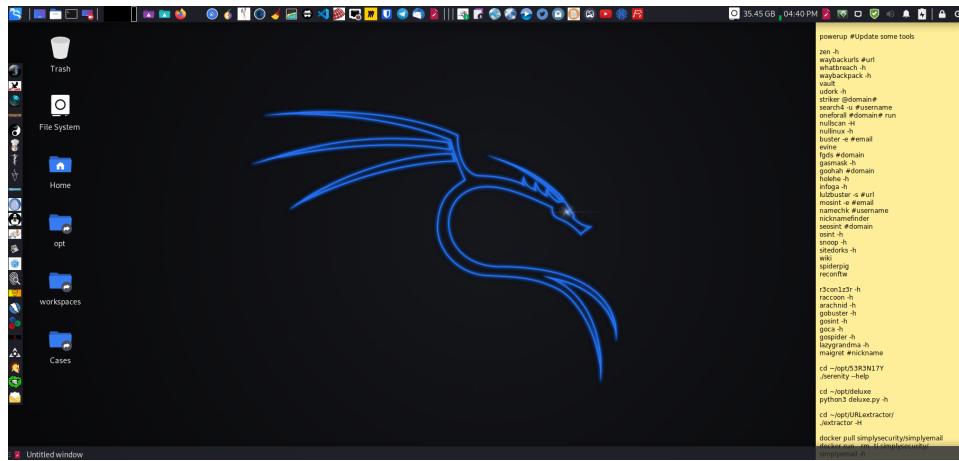


Figura 3.5: Captura de pantalla del escritorio del Sistema Operativo Offensint.

- Fortalezas: Muy completa. Al estar basado en Kali, las herramientas que pueden estar faltando suelen ser fácilmente instalables.
 - Deficiencias: Contiene herramientas no actualizadas en los últimos 18 meses. Mantenido únicamente por su creador (falta una comunidad para respaldar el proyecto). Utiliza el script de Argos por lo que hereda algunas de sus fortalezas y deficiencias. Está sobrecargada de herramientas e incluye muchas de explotación. Faltan herramientas para escaneo de vulnerabilidades.

Si bien cada una de las soluciones empaquetadas analizadas tienen una serie de fortalezas y deficiencias que las hacen adecuadas para ciertas organizaciones, ciertos contextos o bien situaciones específicas, se destaca la deficiencia común de que ninguna de ellas incluía un escáner de vulnerabilidades.

En líneas generales se puede observar que la bibliografía referenciada tiende a recomendar que el mejor camino posible es la construcción de una Máquina Virtual que se adecue a las necesidades específicas de cada organización. Sin embargo, esto requiere de un conocimiento previo tanto de las soluciones individuales existentes. En la Tabla 3.2 se listan las 157 soluciones individuales (todas gratuitas parcial o totalmente) que existen en las 13 soluciones empaquetadas relevadas.

Nombre	Actualizado	Categoría	Trace Labs	ns2losint	Offensint	Argos
exifscan	18-08	Análisis de datos	Si			
Stegosuite	19-01	Análisis de datos	Si			
Elasticsearch-Crawler	20-10	Análisis de datos			Si	Si
exifprobe	20-12	Análisis de datos	Si			

Nombre	Actualizado	Categoría	Trace Labs	ns2losint	Offensint	Argos
DumpsterDiver	21-07	Análisis de datos	Si			
Ripgrep	22-03	Análisis de datos			Si	
MediaInfo	22-03	Análisis de datos			Si	
kali-anonsurf	17-7	Anonimizador				Si
waybackurls	20-04	Archivo Web			Si	
WikiLeaker	20-11	Archivo Web	Si	Si	Si	
waybackpack	20-11	Archivo Web			Si	
wayback-machine-downloader	21-09	Archivo Web			Si	
Cr3dOv3r	18-11	Brecha / Fuga				
karma	19-03	Brecha / Fuga				
WhatBreach	19-11	Brecha / Fuga			Si	
pwnedOrNot	22-03	Brecha / Fuga				
EyeWitness	22-03	Capturas de pantalla			Si	Si
CloudFail	22-03	CloudFlare Recon				
DNSTwist	22-03	Cybersquatting				
Deep Explorer	21-10	Deep web crawler				
OnionSearch	21-10	Deep web crawler	Si			
Amass	22-03	DNS Enumeration			Si	Si
dnsenum	15-02	DNS Enumeration			Si	
dnsmap	17-09	DNS Enumeration			Si	
OSIRA	19-04	DNS Enumeration			Si	
Sublist3r	20-07	DNS Enumeration	Si		Si	Si
DNSkron	20-12	DNS Enumeration			Si	
ip2domain	21-07	DNS Enumeration				
fierce	21-12	DNS Enumeration				
dnsscan	22-01	DNS Enumeration				
Knock	22-03	DNS Enumeration				
subfinder	22-03	DNS Enumeration				
dnsrecon	22-03	DNS Enumeration			Si	
WebHTTTrack	17-07	Downloader	Si		Si	Si
Website Copier						
Youtube-dl	22-03	Downloader	Si			
SimplyEmail	18-08	Email			Si	
Zen	19-05	Email			Si	
h8mail	21-02	Email	Si			
Infoga	21-04	Email	Si		Si	
Holehe	22-02	Email			Si	Si
iKy	22-03	Email			Si	
MOSINT	22-03	Email			Si	
badKarma	17-12	Escáner de red			Si	
arp-scan	18-11	Escáner de red				
nullscan	21-01	Escáner de red			Si	
masscan	21-09	Escáner de red				
fping	22-03	Escáner de red				
netdiscover	22-03	Escáner de red			Si	
nmap	22-03	Escáner de red			Si	
Nikto	22-03	Escáner de Servidor Web			Si	
Striker	19-06	Escáner de vulnerabilidades			Si	
nessus	22-03	Escáner de vulnerabilidades				
OpenVAS	22-03	Escáner de vulnerabilidades				
wafw00f	22-03	Escáner de WAF				
wig	16-10	Escáner de WebApp				
sslyze	22-03	Escáner SSL/TLS			Si	
Gitrob	18-07	Fugas (Github)				
GitGot	20-09	Fugas (Github)				
shhgit	21-02	Fugas (Github)				
Gitleaks	22-03	Fugas (Github)			Si	
GHunt	22-01	Fugas (Google)			Si	
Goohak	21-09	Fugas (Motor de búsqueda)			Si	
getrails-tool	21-10	Fugas (Motor de búsqueda)				
Fast-Google-Dorks-Scan	21-11	Fugas (Motor de búsqueda)			Si	
dorks-eye	22-01	Fugas (Motor de búsqueda)			Si	
uDork	22-03	Fugas (Motor de búsqueda)			Si	
sitedorks	22-03	Fugas (Motor de búsqueda)			Si	
ProtOSINT	21-11	Fugas (Proton)				
YaSeeker	21-12	Fugas (Yandex)			Si	
D4N155	22-01	Generador de wordlist				
creepy	19-05	Geolocalización				
trape	21-06	Ingeniería social				
Social-engineer-toolkit	22-01	Ingeniería social				
Spiderpig	16-08	Metadata	Si		Si	
Metaforge	19-03	Metadata			Si	
Goca	20-09	Metadata			Si	
FOCA	21-08	Metadata				

Nombre	Actualizado	Categoría	Trace Labs	ns2losint	Offensint	Argos
Goblyn	21-09	Metadata				
Metagoofil	21-11	Metadata	Si		Si	Si
exiftool	22-02	Metadata		Si		Si
DataSploit	18-08	Multi-función/propósito				
GOSINT	18-10	Multi-función/propósito			Si	
InfoSploit	18-10	Multi-función/propósito			Si	
InstaRecon	18-10	Multi-función/propósito				
Belati	18-12	Multi-función/propósito				
Gorecon	19-06	Multi-función/propósito			Si	
cignotrack	19-07	Multi-función/propósito			Si	
R3con1z3r	19-07	Multi-función/propósito			Si	
buster	19-08	Multi-función/propósito	Si		Si	
lazyGrandma	19-10	Multi-función/propósito			Si	
scriptnOsint	19-10	Multi-función/propósito			Si	
OSINT-SPY	20-04	Multi-función/propósito			Si	
Operative Framework	20-07	Multi-función/propósito				
DMitry	20-07	Multi-función/propósito	Si		Si	
RED_HAWK	20-09	Multi-función/propósito			Si	
LittleBrother	20-10	Multi-función/propósito	Si			
gasmask	21-05	Multi-función/propósito			Si	
OSINT Framework	21-06	Multi-función/propósito				
Recon-ng	21-08	Multi-función/propósito	Si	Si	Si	
SiteBroker	21-08	Multi-función/propósito			Si	
reconspider	21-08	Multi-función/propósito			Si	
Sarenka	21-10	Multi-función/propósito				
xray	21-10	Multi-función/propósito				
OSRFramework	21-11	Multi-función/propósito	Si	Si		
gobuster	21-11	Multi-función/propósito			Si	
metabigor	21-11	Multi-función/propósito				
Maltego	22-01	Multi-función/propósito	Si		Si	Si
FinalRecon	22-01	Multi-función/propósito	Si		Si	
Raccoon	22-01	Multi-función/propósito			Si	
Maryam	22-02	Multi-función/propósito			Si	
OSINT-SAN	22-02	Multi-función/propósito			Si	
Open Semantic Search	22-03	Multi-función/propósito			Si	
Reconftw	22-03	Multi-función/propósito			Si	
Spiderfoot	22-03	Multi-función/propósito	Si	Si	Si	Si
Photon	19-12	Multi-función/propósito	Si		Si	Si
GhostRecon	22-03	Multi-función/propósito			Si	
sn0int	22-03	Multi-función/propósito	Si	Si		
intrigue-core	22-03	Multi-función/propósito				
Dante OSINT	22-03	Multi-función/propósito		Si		
OneForAll	22-03	Multi-función/propósito			Si	
theHarvester	22-03	Multi-función/propósito	Si	Si	Si	Si
AutoRecon	22-03	Multi-función/propósito				
Namechk	18-07	Nombre de usuario			Si	
MagmaOsint	20-01	Nombre de usuario			Si	
Search4	21-02	Nombre de usuario			Si	
nexfil	22-01	Nombre de usuario		Si		
maigret	22-03	Nombre de usuario				Si
WhatsMyName	22-03	Nombre de usuario	Si		Si	
Moriarty-Project	22-02	Numeros de telefono				Si
phoneinfoga	22-03	Numeros de telefono	Si		Si	
TIDoS-Framework	21-02	OffSec Framework			Si	
sn1per	22-02	OffSec Framework			Si	
Legion	22-03	OffSec Framework			Si	
Metasploit-framework	22-03	OffSec Framework			Si	
tinfoleak	18-04	Redes sociales				
InstagramOSINT	20-03	Redes sociales				
Twint	21-03	Redes sociales	Si		Si	Si
InstaLooter	21-06	Redes sociales			Si	Si
Osintgram	21-10	Redes sociales		Si		
tiktok-scraprer	22-01	Redes sociales	Si			
Investigo	22-03	Redes sociales			Si	
social-analyzer	22-03	Redes sociales			Si	
instaloader	22-03	Redes sociales	Si		Si	Si
sherlock	22-03	Redes sociales	Si		Si	Si
nulllinux	22-03	SMB Enumeration			Si	
seosint	17-06	Web Crawler			Si	
aquatone	19-05	Web Crawler				
URLextractor	19-05	Web Crawler			Si	
lulzbuster	20-04	Web Crawler			Si	

Nombre	Actualizado	Categoría	Trace Labs	ns21osint	Offensint	Argos
BlackWidow	21-09	Web Crawler				
evine	21-10	Web Crawler			Si	
ParseHub	22-01	Web Crawler			Si	
arachnid	22-03	Web Crawler			Si	
Scrapy	22-03	Web crawler				
piderila	20-11	Web Crawler (Deep web)			Si	
torbot	21-12	Web Crawler (Deep web)				
getallurls	20-10	Web Crawler / Archivo Web			Si	

Tabla 3.2: Soluciones individuales existentes en las 13 soluciones empaquetadas relevadas.

Las categorías fueron asignadas de acuerdo a como fueron categorizadas por las diferentes soluciones empaquetadas combinado con los detalles que se indican en sus repositorios y/o sitios web origen. Puede observarse:

- 44 soluciones son consideradas Multi-función/propósito (28 %).
- 55 soluciones individuales no fueron actualizadas en los últimos 18 meses (35 %).
- Offensint cuenta con 90 soluciones con 36 no actualizadas en los últimos 18 meses (40 %).
- Trace Labs cuenta con 29 soluciones con 9 no actualizadas en los últimos 18 meses (31 %).
- Argos cuenta con 22 soluciones con 5 no actualizadas en los últimos 18 meses (22 %).
- ns21osint cuenta con 10 soluciones con 1 no actualizada en los últimos 18 meses (10 %).
- 45 soluciones no están incluidas en ninguna de las 4 soluciones empaquetadas preseleccionadas (de las 13 iniciales). De las 11 soluciones individuales consideradas Multi-función/propósito en este conjunto, solamente 4 no fueron actualizadas en los últimos 18 meses.
- Las herramientas Spiderfoot y theHarvester están incluidas en las 4 soluciones empaquetadas, son Multi-función/propósito y se mantienen actualizadas.
- Las herramientas Maltego y Recon-ng están incluidas en 3 de las 4 soluciones empaquetadas, son Multi-función/propósito y se mantienen actualizadas.
- Las herramientas OSRFramework, sn0int, FinalRecon están incluidas en 2 de las 4 soluciones empaquetadas, son Multi-función/propósito y se mantienen actualizadas.
- Las herramientas Metagoofil, sherlock, Twint e instaloader están incluidas en 3 de las 4 soluciones empaquetadas, pero no son tenidas en cuenta ya que son de propósito específico.

- Las herramientas nmap (Escáner de red), OpenVAS y Nessus (Escáneos de vulnerabilidades) no han sido apropiadamente contempladas por la mayoría de las soluciones empaquetadas.

Extendiendo el análisis con el conjunto de 139 soluciones descritas en “OSINTFramework.com” que se instalan y ejecutan localmente, detalladas en la Tabla 3.3, se observa:

- 32 soluciones ya fueron contempladas en el relevamiento previo.
- De las 107 soluciones restantes, 70 pueden excluirse por ser herramientas ya eliminadas o inexistentes, extensiones de navegador, herramientas de uso general no específicas para OSINT, herramientas de anonimización, soluciones individuales ya contempladas o soluciones empaquetadas ya relevadas.
- De las 37 soluciones restantes, solamente 9 fueron actualizadas en los últimos 18 meses y ninguna de ellas es Multi-función/propósito.

Nombre en OSINTFramework	Actualizado	Categoría
Pastebin OSINT Harvester	19-04	Brecha / Fuga
certgraph	21-05	CA Enumeration
URLCrazy	12-07	Cybersquatting
Catphish	17-11	Cybersquatting
dnspop	16-03	DNS Enumeration
AltDNS	21-09	DNS Enumeration
Hunting-New-Registered-Domains	21-10	DNS Enumeration
Orbit	19-07	Escaneo de Blockchain
CloudScraper	22-03	Escáner de Clouds
docker-onion-nmap	17-10	Escáner de red (Deep web)
Wappalyzer	22-03	Escáner de Web App
Inquisitor	17-07	Multi-función/propósito
Low Hanging Fruit (LHF)	17-08	Multi-función/propósito
AutoOSINT	17-11	Multi-función/propósito
IntRec-Pack	19-03	Multi-función/propósito
ReconDog	19-05	Multi-función/propósito
Bluto	20-05	Multi-función/propósito
SecLists	22-02	OffSec Framework
Burp	22-03	OffSec Framework
Hyperlapse	13-05	Redes sociales
TweetVacuum	16-09	Redes sociales
Birdwatcher	16-11	Redes sociales
fb-sleep-stats	18-04	Redes sociales
raven	18-09	Redes sociales
ExtractFace	19-09	Redes sociales
Treeverse	20-12	Redes sociales
DML-TCAT	22-03	Redes sociales
Ghidra	22-03	Reverse engineering Framework
IntelliTamper	06-05	Web Crawler

Tabla 3.3: Soluciones individuales de instalación local listadas en “OSINTFramework.com” no observadas previamente.

Las categorías fueron asignadas de acuerdo como fueron categorizadas por el sitio web “OSINTFramework.com” combinado con los detalles que se indican en sus repositorios y/o sitios web origen. De este listado, no se destaca ninguna herramienta.

Desde el punto de vista ofensivo, la bibliografía en general suele destacar soluciones ya relevadas, aunque existen excepciones como la herramienta

discover, mencionada en la sección “Before the snap - Red team recon” del libro “The Hacker Playbook 3” [107] que reutiliza muchas herramientas, agrega otra técnicas pero también se utiliza para explotación, razón por la cual es desestimada en este análisis.

En la mayoría de los casos las soluciones categorizadas como “Multi-función/propósito” utilizan parcialmente otras soluciones individuales con categorías más específicas para cumplir algunas de sus funciones o bien las realizan directamente utilizando los mismos métodos y técnicas, razón por la cual muchas de ellas se solapan. Además, muchas herramientas que proveen soluciones individuales de función o propósito único, tienden a ser más efectivas en su funcionamiento, por lo que en ningún caso debería descartarse la posibilidad de utilizarlas. En todo caso, luego de agotar los recursos y funciones posibles de las herramientas más generalistas, sería recomendable utilizar las herramientas de funciones más específicas para obtener mayor información sobre el activo en el que se quiere profundizar la investigación. Por otro lado es importante destacar que muchas tácticas o técnicas se encuentran en un espacio cruzado entre la ciberinteligencia, el Threat Hunting y la seguridad ofensiva, como ciertas herramientas de fingerprint (ike-scan, ssldump, sslh, sslscan, onesixtyone, snmp-check, swaks, enum4linux, nbtscan, smbmap, arping, thcping6, lbd, etc.), rastreadores y analizadores de paquetes (Wireshark, netsniff-ng, tcpdump, tshark, etc.), los escáneres de servicios o aplicaciones (wpscan, skipfish, wapiti, whatweb, etc.), los escáneres de vulnerabilidades más específicos (nikto, sqlmap, etc.), los Web crawlers (dirb, dirbuster, ffuf, wfuzz, etc.) o incluso ciertas herramientas multi-function/propósito (Burp, Metasploit), por lo que las necesidades de cada organización podrá variar considerablemente llevandolas a concluir que las soluciones empaquetadas previamente mencionadas cumplen sus expectativas específicas.

Por otro lado, si bien todas las soluciones relevadas requieren la instalación y ejecución local, en la gran mayoría de los casos utilizan o dependen de soluciones implementadas online para la recolección de la información, por lo que relevar las soluciones online de manera independiente resultaría redundante. En la Tabla 3.4 se listan algunos recursos y soluciones online que podrían resultar de especial interés en caso de que se deseé profundizar la investigación por estas vías directamente (aunque sería recomendable revisar los recursos presentados al inicio de esta Sección).

Nombre	Categoría
Internet Archive (Wayback Machine)	Archivo Web
PasteBin	Brecha / Fuga
HaveIBeenpwned	Brecha / Fuga
CrunchBase	Buscador específico
online-ide-search	Buscador específico
GrayhatWarfare Buckets	Buscador específico
GitHub Search	Buscador específico
Shodan	Buscador específico
Zoomeye	Buscador específico

Nombre	Categoría
Ask	Buscador global
Bing	Buscador global
Exalead	Buscador global
Google	Buscador global
Yahoo	Buscador global
LibreBorme	Buscador regional
Google scholar	Buscador regional
Lycos	Buscador regional
wikileaks	Denunciantes (whistleblowers)
globaleaks	Denunciantes (whistleblowers)
Cryptome	Denunciantes (whistleblowers)
DNSDumpster	DNS Enumeration
DNS-Trails	DNS Enumeration
DNSHistory	DNS Enumeration
Epieos	Email
BuiltWith	Escáner de tecnologías web
wappalyzer	Escáner de tecnologías web
crt.sh	Escaner SSL/TLS
certdb	Escaner SSL/TLS
UrlScan	Escaner web
psbdmp[.]jws	Fugas de información
eleaks[.]to	Fugas de información
nulled[.]to	Fugas de información
cracked[.]io	Fugas de información
sinister[.]ly	Fugas de información
crackiansleaks[.]com	Fugas de información
cracking[.]org	Fugas de información
leakzone[.]net	Fugas de información
sinfulsite[.]com	Fugas de información
weleakinfo[.]to	Fugas de información
dehashed[.]com	Fugas de información
snusbase[.]com	Fugas de información
leakcheck[.]io	Fugas de información
leak-lookup[.]com	Fugas de información
RaidForums (Derribado en 2022)	Fugas de información
WeLeakData (Hackeado en 2020)	Fugas de información
LeakBase (Hackeado en 2017)	Fugas de información
VirusTotal	Malware analysis
Hybrid-Analysis	Malware sandbox
Domain-Codex	Multi-función/propósito
Censys.io	Multi-función/propósito
BinaryEdge	Multi-función/propósito
Robtex	Multi-función/propósito
Hunter.io	Multi-función/propósito
ViewDNS	Multi-función/propósito
PulseDive	Multi-función/propósito
IntellX	Multi-función/propósito
NetCraft	Multi-función/propósito
domaindossier	Multi-función/propósito
namechk.com	Nombre de usuario
pipl.com	Nombre de usuario
PeekYou	Nombre de usuario
TInfoLeak.com	Redes sociales
TweetFeed.Live	Redes sociales
WhoIs (DomainTools)	WhoIs
WhoWas	WhoIs (histórico)

Tabla 3.4: Listado de recursos online que podrían proveer información adicional a las soluciones relevadas.

Las categorías fueron asignadas de acuerdo a como fueron categorizadas de acuerdo a lo observado tras su uso en la prueba de concepto.

Partiendo entonces de estas bases y el análisis realizado, las siguientes herramientas se investigan con el fin de cubrir las necesidades preestablecidas: Spiderfoot, theHarvester, Maltego, Recon-*ng*, OSRFramework, sn0int, FinalRecon, nmap, OpenVAS y Nessus.

SpiderFoot es una herramienta web de reconocimiento que realiza consultas en múltiples fuentes de datos públicos para recopilar información sobre

diferentes tipos de objetos y activos. El objetivo puede ser un nombre, un dominio o una dirección IP. Luego de especificar el objetivo a investigar, se deben seleccionar cómo se realiza la investigación (predeterminadamente permite seleccionar entre fuentes específicas, módulos que utilizan un conjunto de fuentes, casos de uso que utilizan un conjunto de módulos o bien todos los casos de uso). Las fuentes que utiliza son en algunos casos gratuitas y en otros pagas. En general, algunas fuentes gratuitas y todas las pagas requieren la preconfiguración de una clave de aplicación (*API Key*).

Se utilizó la versión gratuita de esta herramienta. Configurando todas las API Keys de fuentes gratuitas y omitiendo las fuentes pagas, se intentó ejecutar múltiples escaneos del dominio ugr.es utilizando todos los casos de uso, casos de uso específicos y distintos conjuntos de módulos, pero todos los escaneos llegan hasta un punto en que no detectan nuevos elementos durante horas y deben ser abortados manualmente, como se observa en la Figura 3.6

Name	Target	Started	Finished	Status	Elements	Action
UGR - Others	ugr.es	2022-04-14 15:19:51	Not yet	ABORT-REQUESTED	122081	●○○
UGR - Emails	ugr.es	2022-04-14 11:06:40	Not yet	ABORT-REQUESTED	80892	●○○
UGR - Ports	ugr.es	2022-04-12 21:32:03	Not yet	ABORT-REQUESTED	87061	●○○
UGR-Footprint	ugr.es	2022-04-12 08:24:08	Not yet	ABORT-REQUESTED	27633	●○○
UGR	ugr.es	2022-04-08 11:29:48	Not yet	ABORT-REQUESTED	41714	●○○
ugr	ugr.es	2022-04-07 17:55:48	Not yet	ABORT-REQUESTED	50418	●○○

Figura 3.6: Captura de pantalla de los escaneos (abortados manualmente) de Spiderfoot.

Todos los escaneos generaron múltiples errores, como se puede ver en la Figura 3.7, y estos tienen varios orígenes siendo mayoritariamente debido a inconvenientes con las APIs o a errores de configuración por parte del usuario.

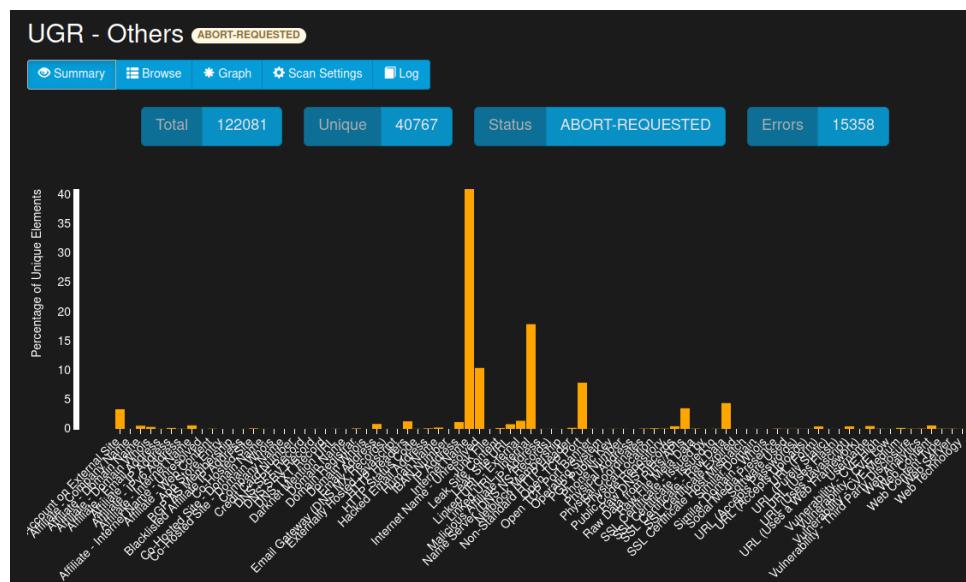
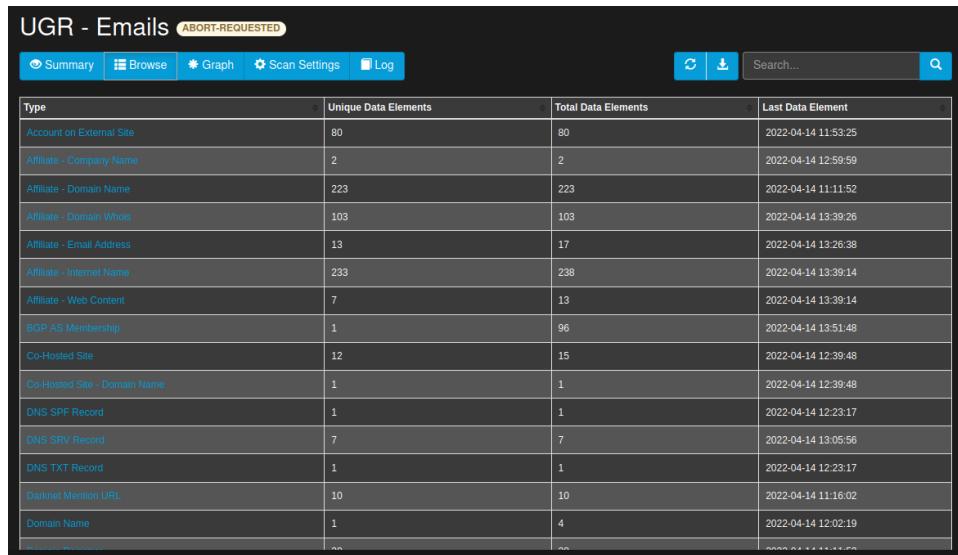


Figura 3.7: Captura de pantalla con detalles de un escaneo de Spiderfoot, en el que destaca la cantidad de errores generados.

Por otro lado puede observarse en la Figura 3.8 que incluso cuando el objetivo del escaneo es únicamente cuentas de correo, debido a las múltiples técnicas de colección utilizadas la herramienta provee resultados adicionales por fuera de lo esperado.



The screenshot shows a web-based interface for the Spiderfoot tool. At the top, there's a header bar with tabs for "Summary", "Browse", "Graph", "Scan Settings", and "Log". To the right of the tabs are icons for refresh, download, and search, along with a search input field. Below the header is a table with four columns: "Type", "Unique Data Elements", "Total Data Elements", and "Last Data Element". The table lists various types of data elements found during the scan, such as "Account on External Site", "Affiliate - Company Name", "Affiliate - Domain Name", etc. The "Unique Data Elements" column shows values like 80, 2, 223, etc., while the "Total Data Elements" column shows values like 80, 2, 223, etc. The "Last Data Element" column shows timestamps indicating when each type of element was last encountered.

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	80	80	2022-04-14 11:53:25
Affiliate - Company Name	2	2	2022-04-14 12:59:59
Affiliate - Domain Name	223	223	2022-04-14 11:11:52
Affiliate - Domain Whois	103	103	2022-04-14 13:39:26
Affiliate - Email Address	13	17	2022-04-14 13:26:38
Affiliate - Internet Name	233	238	2022-04-14 13:39:14
Affiliate - Web Content	7	13	2022-04-14 13:39:14
BGP AS Membership	1	96	2022-04-14 13:51:48
Co-Hosted Site	12	15	2022-04-14 12:39:48
Co-Hosted Site - Domain Name	1	1	2022-04-14 12:39:48
DNS SPF Record	1	1	2022-04-14 12:23:17
DNS SRV Record	7	7	2022-04-14 13:05:56
DNS TXT Record	1	1	2022-04-14 12:23:17
Darknet Mention URL	10	10	2022-04-14 11:16:02
Domain Name	1	4	2022-04-14 12:02:19
Domain Whois	20	20	2022-04-14 11:11:52

Figura 3.8: Captura de pantalla de los resultados de un escaneo de Spiderfoot para recolectar correos electrónicos.

A pesar de esto se puede observar que la cantidad de elementos obtenidos cuando se combinan los reportes, eliminan los elementos repetidos y los elementos que no resultan de especial relevancia, es de 18756, de los que destacan:

- 7 servidores DNS (3 de ugr.es, 2 de cica.es y 2 de rediris.es), 2 servidores de correo electrónico en el subdominio rediris.es, 7 registros DNS de tipo SPF, 7 registros DNS de tipo SRV, 8 registros DNS de tipo TXT.
- 16906 nombres de dominio que resuelven IP.
- 878 nombres de dominio a los que no pudo resolver IP.
- 120 dominios similares registrados.
- 20 dominios que se alojan en el mismo sistema que algún subdominio de ugr.es (potencialmente existen otros 32 que basados en una resolución inversa IP parecerían compartir alojamiento).
- 895 direcciones IP.
- 751 vulnerabilidades registradas por Shodan en IPs vinculadas a ugr.es. 2 detecciones de IPs en Shodan con Sistema Operativo Ubuntu específicamente.

- 5841 puertos abiertos en diferentes sistemas, de los cuales al menos 39 muestran Banners con versiones (OpenSSH_8.7, OpenSSH_7.9p1, OpenSSH_7.4, vsFTPD 3.0.3, vsFTPD 3.0.2, ProFTPD, etc.).
- 50 tecnologías detectadas (VMWare, Postfix, MySQL, OpenSSH, Apache Tomcat, Apache HTTPD, nginx, MS-SQL, etc.). 25 tecnologías web con versiones detectadas (Apache-Coyote/1.1, Apache/2.2.15 (CentOS), OpenCms/10.5.3, Microsoft-IIS/7.5, Apache/2.4.43 (Win32) OpenSSL/1.1.1g PHP/5.2.17, etc, Drupal 8.9.9, PHP/5.2.17, PHP/7.4.20, etc.).
- 41619 URLs. 198 posibles formularios, 2 posibles usos de tecnología Flash, 206 usos de Javascript, 12 formularios de login, 2 archivos Thumbs.db públicos, al menos 50 archivos PDF.
- 17 certificados SSL expirados, 4 certificados SSL cercanos a expirar y 48 usos de certificado incorrectos (utilizados en un subdominio para el que no es válido).
- 17 vulnerabilidades reportadas en programas de Bug Bounty.
- 35 detecciones de listas negras a subdominios.
- 1748 direcciones de correo.
- 1608 detecciones de una cuenta comprometida en alguna brecha / fuga de información.
- 10 menciones en sitios de la DarkNet.
- 97 menciones a ugr.es en Pastebin.
- 493 menciones a ugr.es en leaks de acuerdo a IntelligenceX.
- 329 nombres de usuarios.
- 98 nombres de personas.
- 9 números de teléfono.
- 27 cuentas en redes sociales con presencia de UGR.
- 71 repositorios públicos de Github.
- 92 versiones de aplicaciones de Android/iOS.
- 6 posibles números de tarjetas de crédito (baja fidelidad de detección).

theHarvester es una herramienta gratuita y simple, de código abierto y ejecución en línea de comandos, diseñada para ser utilizada en las primeras etapas del ciclo de seguridad ofensiva que recopila información en base a fuentes abiertas. Se centra en la recolección de correos electrónicos, nombres, nombres de dominio, IPs y URLs.

Las fuentes que utiliza son en algunos casos gratuitas y en otros pagos. En general, algunas fuentes gratuitas y todas las pagas requieren la preconfiguración de una API Key. Configurando todas las API Keys de fuentes gratuitos y omitiendo las fuentes pagas, se intento ejecutar multiples escaneos del dominio ugr.es utilizando todas las fuentes configuradas, pero en todos los casos se obtiene un error que finaliza el escaneo prematuramente, como se observa en la Figura 3.9.



```
git:(null) [~] 1 theharvester ugr.es | 500000 100 ... arubis,baidu,bing,bingapi,bufferoverun,censys,certspotter,crish,dnsdumpster,duckduckgo,fullhunt,github-code,google,hackertarget,hunter,intelx,linkedin,linkedin_links, ... t,omnisite,otx,ownct,rapiddns,rocketchat,securitytrails,sublist3r,threadcrowd,threadmining,trellix,twitter,uriwatch,vt,vttotal,whois,whoispy,commpy
```

```
THE HARVESTER
```

```
theharvester 4.0.3
Copyright (c) 2018, Martorells
Edge Security Research
Carturrell Lab Edge Security,com
```

```
[*] Target: ugr.es
[*] killed
```

Figura 3.9: Captura de pantalla de uno de los escaneo de theHarvester finalizando con errores.

Por esta razón, se ejecutaron múltiples escaneos utilizando fuentes en conjuntos más pequeños. Luego de combinarse los resultados, se destacan:

- 6573 direcciones de correo.
- 11720 direcciones IP, de las cuales 1 corresponde al rango 216.147.c.d, 1 al rango 51.254.c.d, 1 al rango 63.35.c.d y el resto al rango 150.214.c.d.
- 17968 nombres de dominio.

Maltego es un software para inteligencia de fuentes abiertas. Si bien la versión gratuita de Maltego (denominada “CE”, por sus siglas en inglés “Community Edition”) tiene una serie de restricciones cuya consecuencia es una recolección de información muy limitada, tiene un potencial de visualización de la información que destaca por sobre cualquier otra solución. Por esta razón y solamente en este caso específico, se dispuso de una licencia paga de Maltego para utilizar la versión denominada “One” que no tiene restricciones en la información que recolecta desde las fuentes configuradas. Se proporciona por defecto de una biblioteca de módulos (denominados transformaciones) que funcionan como fuentes para la recolección y los datos obtenidos son mostrados gráficamente en lo que se denomina entidades. De los 82 módulos disponibles, se seleccionaron e instalaron los 20 gratuitos más

relevantes. Algunos de estos módulos requieren la preconfiguración de una API Key. Partiendo del dominio ugr.es se ejecutaron todas las transformaciones. En la Figura 3.10 puede observarse cómo se visualizan los resultados luego de eliminar las entidades que no resultaban relevantes y agruparlas por tipo de entidad.

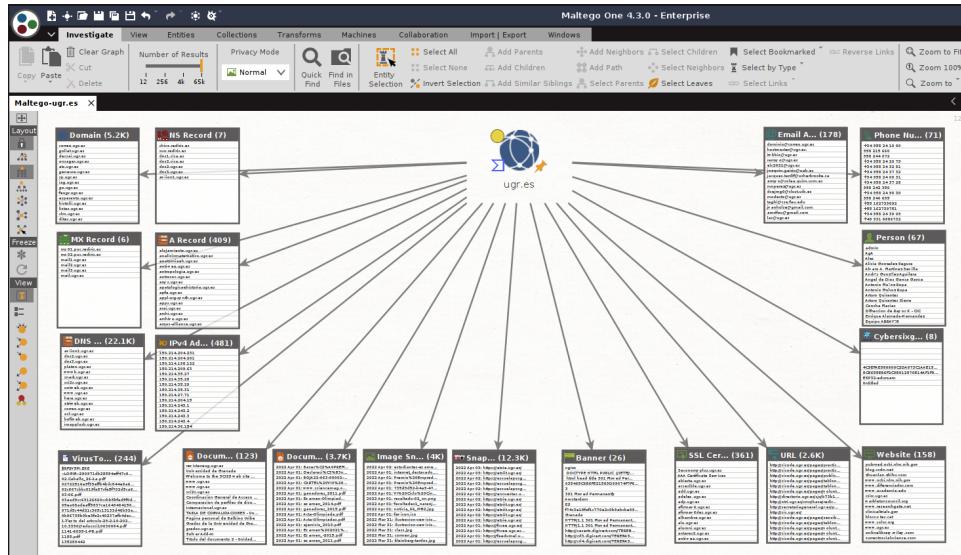


Figura 3.10: Captura de pantalla de Maltego con entidades agrupadas por tipo.

Se destacan:

- 5192 dominios: 98 dominios relacionados y 5094 subdominios de ugr.es.
 - 7 registros DNS de tipo NS, de los cuales 3 son subdominios de ugr.es.
 - 6 registros DNS de tipo MX, de los cuales 4 son subdominios de ugr.es.
 - 409 registros DNS de tipo A, siendo todos subdominios de ugr.es.
 - 481 direcciones IPs, de las cuales 2 son privadas (172.18.c.d), 1 del rango público 51.254.c.d y las demás del rango 150.214.c.d.
 - 178 direcciones de correo de las cuales 139 corresponden a ugr.es.
 - 67 personas.
 - 71 números de teléfono.
 - 22145 registros DNS históricos de ugr.es.

- 8 detecciones de menciones del dominio ugr.es por parte de actores maliciosos en mercados negros.
 - 158 sitios web.
 - 2597 URLs.
 - 261 certificados TLS/SSL, de los cuales 354 pertenecen a ugr.es.
 - 244 referencias en archivos a ugr.es en VirusTotal.
 - 12331 snapshots de sitios web de ugr.es (o alguno de sus subdominios) en WayBackMachine. Adicionalmente se detectaron 3976 snapshots de imágenes específicas, 3689 snapshots de documentos específicos y 123 documentos específicos que aún siguen presentes.
 - 26 Banners, de los cuales se destaca nginx por ser el motor de servidor web detrás del sitio web ugr.es.

En la Figura 3.11 se visualiza el gráfico de entidades luego de eliminar las de menor valor para el caso de uso, pivotando sobre entidades específicas y ejecutando transformaciones sobre ellas.

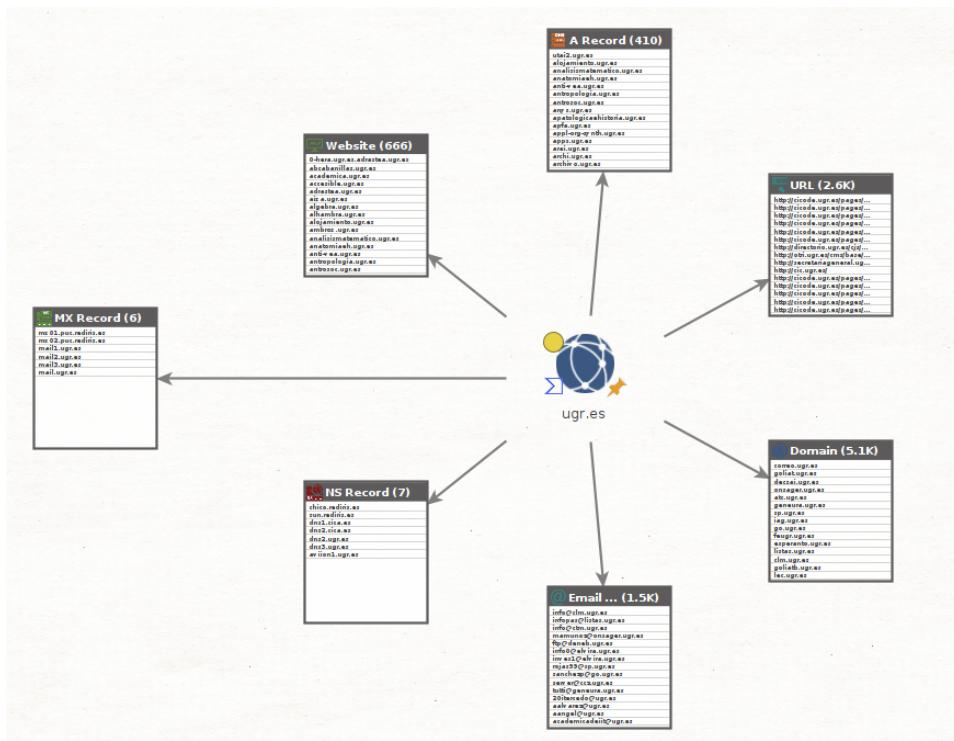


Figura 3.11: Captura de pantalla de Maltego con ejecución de transformaciones sobre algunas entidades descubiertas en la primera ejecución.

Se destacan también:

- 1470 direcciones de correo, de las cuales 656 fueron alguna vez comprometidos en base a HaveIBeenPwned (eliminado del gráfico para facilitar la visualización).
- 666 sitios web distintos.

Recon-*ng* es una herramienta de línea de comando y código abierto diseñada para proporcionar un entorno con el objetivo de realizar el reconocimiento en base a un dominio o URL y ejecutando consultas en múltiples fuentes de datos públicos. Las fuentes pueden descargarse como módulos desde un mercado utilizable desde el mismo entorno de la herramienta. Las fuentes que utiliza son en algunos casos gratuitas y en otros pagos. En general, algunas fuentes gratuitas y todas las pagas requieren la preconfiguración de una API Key. En la Figura 3.12 se observa el menú inicial de Recon-*ng* previo a la ejecución de sus módulos.

Figura 3.12: Captura de pantalla del menú de Recon-*ng* previo a la ejecución de sus módulos.

Instalando todos los módulos disponibles relacionados a Recon y Discovery que corresponden a fuentes gratuitas, configurando las API Keys y ejecutando en múltiples repeticiones (para que los resultados de la ejecución de unos módulos pueda nutrir a los siguientes al iterar la ejecución del conjunto), se observan:

- 352 subdominios.
 - 150 direcciones IP.
 - 10 direcciones de correo.
 - 37 dominios relacionados.

Los elementos obtenidos no resultan especialmente relevantes a comparación de las herramientas previamente observadas.

OSRFramework es una herramienta de línea de comandos y código abierto para realizar inteligencia de fuentes abiertas mediante una serie de módulos que buscan en base a un nombre de usuario, un correo electrónico, un teléfono u otros datos. En la Figura 3.13 se observa el módulo “mailfy” de OSRFramework en ejecución.

The screenshot shows a terminal window on a Kali Linux system. The command entered is \$ osrf mailfy -m "aropa@ugr.es". The output is a large grid of dots forming a watermark-like pattern with the text 'TRACE CROWDSOURCED SOURCE INTE'. Below this, the OSRFramework version 0.20.1 is displayed. At the bottom, credits to Yaiza Rubio & Félix Brezo are shown, along with copyright information for Mailfy (2014-2020).

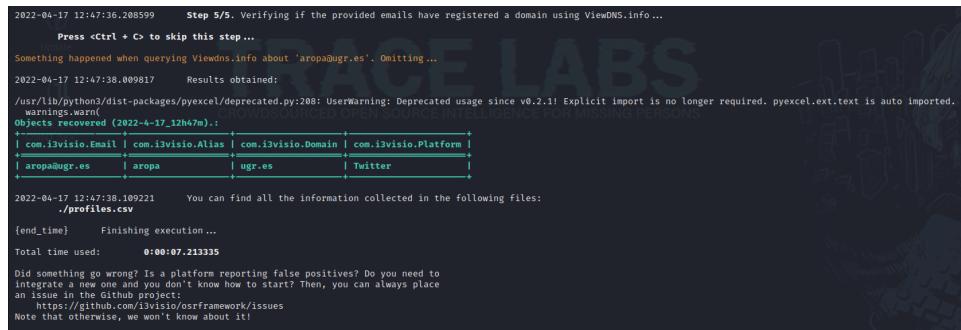
```
(osint㉿kali)-[~]
$ osrf mailfy -m "aropa@ugr.es"

File System
Home
Update
Trace OSINT
...
OSRFramework 0.20.1

Coded with ❤ by Yaiza Rubio & Félix Brezo
-- In OSRF CLI apps, you can set a different output folder with '-o'. --
Mailfy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2020
```

Figura 3.13: Captura de pantalla del módulo “mailfy” de OSRFramework en ejecución.

El análisis en este caso particular inició a partir del nombre del tutor del trabajo, Antonio Muñoz Ropa y su correo electrónico institucional, utilizando los diferentes módulos disponibles. La Figura 3.14 muestra el resultado final de hallazgos.



The screenshot shows a terminal window with the following text:

```
2022-04-17 12:47:36.208599 Step 5/5. Verifying if the provided emails have registered a domain using ViewDNS.info...
Press <Ctrl + C> to skip this step...
Something happened when querying Viewdns.info about 'aropadegr.es'. Omitting...
2022-04-17 12:47:38.009817 Results obtained:
/usr/lib/python3/dist-packages/pyexcel/deprecated.py:208: UserWarning: Deprecated usage since v0.2.1! Explicit import is no longer required. pyexcel.ext.text is auto imported.
warnings.warn("Viewdns.info is now a crowdsourced open source intelligence for missing persons")
Objects recovered (2022-4-17_12h47m):
+---+ com.i3visio.Email | com.i3visio.Alias | com.i3visio.Domain | com.i3visio.Platform +
| aropadegr.es | aropa | ugr.es | Twitter |
+---+
2022-04-17 12:47:38.109221 You can find all the information collected in the following files:
./profiles.csv
{end_time} Finishing execution...
Total time used: 0:00:07.213335
Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!
```

Figura 3.14: Captura de pantalla con hallazgos de OSRFramework.

Al no obtener datos relevantes más allá de la detección de una cuenta de Twitter registrada con esa dirección de correo, se repitieron las pruebas con el nombre del autor del trabajo, Fabián Olender y una de las cuentas de correo de las que dispone, pero de igual modo es muy escasa la información obtenida y no resulta relevante.

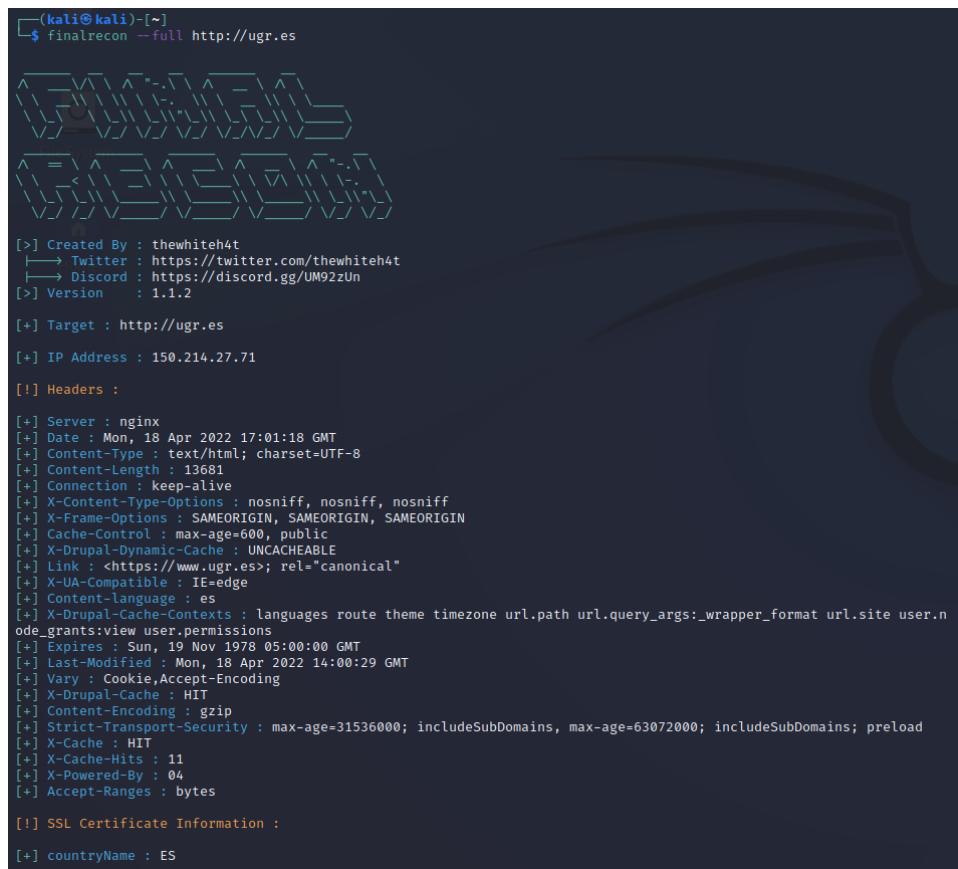
sn0int es una herramienta de línea de comandos y código abierto inspirada en recon-*ng* y Maltego que proporciona un entorno para investigaciones OSINT utilizando múltiples fuentes. Las fuentes pueden descargarse como módulos desde el entorno de la herramienta misma. Las fuentes que utiliza son en algunos casos gratuitas y en otros pagos. En general, algunas fuentes gratuitas y todas las pagas requieren la preconfiguración de una API Key. La configuración de las API Keys se basa en el uso de la funcionalidad “keyrings” de Amazon Web Services (AWS), por lo que esta configuración debió omitirse. Instalando todos los módulos recomendados por defecto y realizando múltiples ejecuciones sobre ugr.es, el resumen de hallazgos puede visualizarse en la Figura 3.15.

```
-active, -atempt, -cnt/fct, -name, -gabs  
-add, -value  
-IP/ and -n/-r/-o/.168[1-2]/4) sepa  
-asn, -value  
osint | recon | security (can be used  
-cidirc.hackint.org:6697/#sn0int  
CIDRs separated by commas (can be used  
[+] Connecting to database  
[+] Loaded 61 modules [!] configuration file.  
[sn0int][default] > workspace UGR  
[+] Connecting to database separated by commas (can  
[sn0int][UGR] > stats  
Censor output to make it suitable for  
domains value 14  
subdomains path to a file providing data 4,696  
ipaddrs string 316  
urls Path to the directory containing 1,059  
emails string 98  
phonenumbers path to a file providing data 0  
devices value 0  
networks data source names separated by commas 0  
accounts Show the program usage message 0  
breaches 0  
images Show the program usage message 0  
ports string 277  
netblocks path to a file providing data 13  
cryptoaddrs value 0  
activity data source names separated by commas 0  
blobs 0  
blobs (size) the IP addresses for discarding 0 B  
[sn0int][UGR] > █
```

Figura 3.15: Captura de pantalla con resumen de hallazgos de sn0int.

Los elementos obtenidos no resultan especialmente relevantes a comparación de las herramientas previamente observadas.

FinalRecon es una herramienta de línea de comandos y código abierto cuyo objetivo es proporcionar una visión general del objetivo en un período corto de tiempo manteniendo una alta tasa de precisión en los resultados. Utiliza pocas fuentes que requieren la configuración de API Keys, por lo que es relativamente sencilla de ejecutar. La Figura 3.16 muestra el inicio de la ejecución de FinalRecon.



```
(kali㉿kali)-[~]
$ finalrecon --full http://ugr.es

[>] Created By : thewhiteh4t
[→] Twitter : https://twitter.com/thewhiteh4t
[→] Discord : https://discord.gg/UM92zUn
[>] Version   : 1.1.2

[+] Target : http://ugr.es
[+] IP Address : 150.214.27.71

[!] Headers :

[+] Server : nginx
[+] Date : Mon, 18 Apr 2022 17:01:18 GMT
[+] Content-Type : text/html; charset=UTF-8
[+] Content-Length : 13681
[+] Connection : keep-alive
[+] X-Content-Type-Options : nosniff, nosniff, nosniff
[+] X-Frame-Options : SAMEORIGIN, SAMEORIGIN, SAMEORIGIN
[+] Cache-Control : max-age=600, public
[+] X-Dynamic-Cache : UNCACHEABLE
[+] Link : <https://www.ugr.es>; rel="canonical"
[+] X-UA-Compatible : IE=edge
[+] Content-Language : es
[+] X-Dynamic-Contexts : languages route theme timezone url.path url.query_args:_wrapper_format url.site user.n
ode_grants:view user.permissions
[+] Expires : Sun, 19 Nov 1978 05:00:00 GMT
[+] Last-Modified : Mon, 18 Apr 2022 14:00:29 GMT
[+] Vary : Cookie,Accept-Encoding
[+] X-Drupal-Cache : HIT
[+] Content-Encoding : gzip
[+] Strict-Transport-Security : max-age=31536000; includeSubDomains, max-age=63072000; includeSubDomains; preload
[+] X-Cache : HIT
[+] X-Cache-Hits : 11
[+] X-Powered-By : 04
[+] Accept-Ranges : bytes

[!] SSL Certificate Information :

[+] countryName : ES
```

Figura 3.16: Captura de pantalla con información inicial de hallazgos de FinalRecon.

En los resultados se observan:

- 17122 nombres de dominio.
- 4582 directorios en el sitio web
- 32955 directorios en el archivo de The Way Back Machine.

- 45212 URLs, de las cuales 40 son archivos robot.txt.

La rapidez de la herramienta se destaca, pero los elementos obtenidos no resultan relevantes a comparación de las herramientas previamente observadas.

nmap es una herramienta de línea de comandos y código abierto para el descubrimiento de redes mediante escaneos, que ofrece una versión gratuita para usuarios finales y licencias comerciales para organizaciones.

El análisis resulta más eficiente si se basa en IPs, por lo que basándose en los análisis previos se reconocen 1205 IPs del rango 150.214.c.d que podrían escanearse. Por precaución se restringe el escaneo a una IP seleccionada de manera aleatoria de cada subred de los rangos observados en “150.214.c”, resultando en un subconjunto de 63 IPs.

La Figura 3.17 muestra el inicio de un escaneo sobre el conjunto de IPs (Depositado en un archivo y cargado en la herramienta con el parámetro “-iL”) que evite la verificación mediante Ping (parámetro “-Pn”), aumente el nivel de verbosidad para imprima más información sobre el escaneo (parámetro “-v”) y realice el saludo de 3 vías (“Three-way handshake”) TCP de manera completa (parámetro “-sT”).

```
└─(kali㉿kali)-[~]
$ nmap -Pn -v -sT -iL UGR-IPsv2.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-26 06:50 EDT
Initiating Parallel DNS resolution of 63 hosts. at 06:50
Completed Parallel DNS resolution of 63 hosts. at 06:50, 0.11s elapsed
Initiating Connect Scan at 06:50
Scanning 63 hosts [1000 ports/host]
Discovered open port 113/tcp on 150.214.205.7
Discovered open port 113/tcp on 150.214.203.10
Discovered open port 113/tcp on 150.214.67.2
Discovered open port 113/tcp on 150.214.243.4
Discovered open port 113/tcp on 150.214.104.11
Discovered open port 113/tcp on 150.214.208.16
Discovered open port 113/tcp on 150.214.191.18
Discovered open port 113/tcp on 150.214.36.20
Discovered open port 113/tcp on 150.214.64.32
Discovered open port 113/tcp on 150.214.19.53
```

Figura 3.17: Captura de pantalla del inicio del escaneo de un conjunto de IPs mediante nmap.

Luego de unos minutos se pierde la conexión con cualquier IP o dominio de UGR, lo que nos permite suponer que existe un sistema que bloquea orígenes de conexiones cuando detecta comportamientos que podrían considerarse agresivos.

En la Figura 3.18 se observa el inicio de un escaneo sobre una IP específica,

y se destaca que todos los puertos escaneados se muestran abiertos, lo que resultaría inusual en un sistema.

```
└─(kali㉿kali)-[~]
└─$ nmap -Pn -v -sT 150.214.32.164
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-26 07:00 EDT
Initiating Parallel DNS resolution of 1 host. at 07:00
Completed Parallel DNS resolution of 1 host. at 07:00, 0.02s elapsed
Initiating Connect Scan at 07:00
Scanning gaia2.ugr.es (150.214.32.164) [1000 ports]
Discovered open port 3389/tcp on 150.214.32.164
Discovered open port 80/tcp on 150.214.32.164
Discovered open port 53/tcp on 150.214.32.164
Discovered open port 995/tcp on 150.214.32.164
Discovered open port 1723/tcp on 150.214.32.164
Discovered open port 8080/tcp on 150.214.32.164
Discovered open port 554/tcp on 150.214.32.164
Discovered open port 1720/tcp on 150.214.32.164
Discovered open port 143/tcp on 150.214.32.164
Discovered open port 113/tcp on 150.214.32.164
```

Figura 3.18: Captura de pantalla del inicio del escaneo de una IP específica mediante nmap.

Se observa también que si el escaneo sobre una IP específica incluye parámetros demasiado agresivos (por ejemplo “-A” que habilita la detección del sistema operativo, la detección de versiones y el escaneo con scripts) se genera un bloqueo del origen de las conexiones. Además, como se observa en la Figura 3.19, al intentar establecer conexiones manuales a los puertos la conexión es rechazada o bien se abre e inmediatamente cierra, lo que nos permite confirmar que no existe realmente un servicio abierto.

```
[└(kali㉿kali)-[~]
└$ telnet 150.214.32.164 1720
Trying 150.214.32.164 ...
Connected to 150.214.32.164.
Escape character is '^]'.
Connection closed by foreign host.

[└(kali㉿kali)-[~]
└$ nc 150.214.32.164 1720
```

Figura 3.19: Captura de pantalla con intentos de conexión manual a un puerto que nmap marcó como abierto.

Debido a que sería inusual que todos los puertos estén abiertos en un sistema y sumada la existencia de un bloqueo posiblemente automático ante escaneos agresivos, puede suponerse la presencia de un sistema de prevención de intrusiones (IPS), como por ejemplo Snort.

Agregando el parámetro “-sV” se hará un sondeo de los puertos abiertos para determinar la información de servicio y versión que responden, lo que permitirá diferenciar aquellos puertos que realmente se encuentran abiertos y con un servicio respondiendo. La Figura 3.20 y la Figura 3.21 muestran los resultados de nmap aplicando este parámetro en escaneos a IPs específicas para una serie de puertos específicos.

```
(kali㉿kali)-[~]
└─$ nmap -Pn -sT -sV -p21,22,25,53,80,110,139,389,443,8080 150.214.101.120
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-26 07:53 EDT
Nmap scan report for macdeproyectos.ugr.es (150.214.101.120)
Host is up (0.011s latency).

PORT      STATE     SERVICE      VERSION
21/tcp    open      ftp?
22/tcp    open      ssh?
25/tcp    filtered  smtp
53/tcp    open      domain?
80/tcp    open      http?
110/tcp   open      pop3?
139/tcp   filtered  netbios-ssn
389/tcp   filtered  ldap
443/tcp   open      https?
8080/tcp  open      http-proxy?
```

Figura 3.20: Captura de pantalla con escaneo de nmap sobre IP específica para reconocer servicios.

En los resultados de este escaneo pueden omitirse aquellos en los que responde un puerto abierto y el nombre del servicio incluye un signo de interrogacion (“?”) al final, ya que es una suposición de la herramienta basada en el número de puerto únicamente.

```
(kali㉿kali)-[~]
└─$ nmap -Pn -sT -sV -p21,22,25,53,80,110,139,389,443,8080 150.214.102.112
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-26 07:56 EDT
Nmap scan report for eppursimuvve.ugr.es (150.214.102.112)
Host is up (0.010s latency).

PORT      STATE     SERVICE      VERSION
21/tcp    open      tcpwrapped
22/tcp    open      ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered  smtp
53/tcp    open      tcpwrapped
80/tcp    open      http         Apache httpd 2.4.29 ((Ubuntu))
110/tcp   open      tcpwrapped
139/tcp   filtered  netbios-ssn
389/tcp   filtered  ldap
443/tcp   open      tcpwrapped
8080/tcp  open      tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figura 3.21: Captura de pantalla con escaneo de nmap sobre IP específica para reconocer servicios.

En los resultados de este escaneo, pueden omitirse aquellos en los que responde un puerto abierto con servicio “tcpwrapped” ya que corresponde a un sistema denominado “TCP Wrapper” que utiliza ACLs de red en sistemas para filtrar el acceso. Debido a las versiones de sistemas que responden en cada puerto, se presupone que el sistema operativo es Ubuntu, una distribución de Linux.

La Figura 3.22 muestra los resultados de extender el escaneo a todo el subconjunto de IPs nuevamente, pero centrandonos en el puerto 22 que por defecto utiliza SSH a fin de evitar generar una disrupcion en los servicios de la organizacion. A fin de evitar el bloqueo automático se debe ralentizar el escaneo utilizando el parámetro “-T” (preferentemente con el argumento “paranoid”, aunque “sneaky” sería suficiente para evitar el bloqueo a partir del umbral que por defecto utilizan por la mayoría de los IPS), reducir el número de sondas enviadas para para determinar la información de servicio y versión en cada puerto (parámetro “–version-intensity”) y almacenar los resultados en un archivo (parámetro “-oN”).

```

(kali㉿kali)-[~]
$ nmap -Pn -sT -sV --version-intensity 1 -T sneaky -p22,3389 -iU UGR-IPsv2.txt -oN UGR-IPsv2-Results.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-27 08:47 EDT
Stats: 0:01:37 elapsed; 0 hosts completed (63 up), 63 undergoing Service Scan
Service scan Timing: About 1.59% done; ETC: 09:56 (1:07:10 remaining)
Stats: 0:04:01 elapsed; 0 hosts completed (63 up), 63 undergoing Service Scan
Service scan Timing: About 5.56% done; ETC: 09:50 (0:59:30 remaining)
Stats: 0:09:59 elapsed; 0 hosts completed (63 up), 63 undergoing Service Scan
Service scan Timing: About 19.84% done; ETC: 09:35 (0:38:11 remaining)
Stats: 0:15:34 elapsed; 0 hosts completed (63 up), 63 undergoing Service Scan
Service scan Timing: About 31.75% done; ETC: 09:35 (0:32:21 remaining)
Stats: 0:26:19 elapsed; 0 hosts completed (63 up), 63 undergoing Service Scan
Service scan Timing: About 53.17% done; ETC: 09:36 (0:22:42 remaining)
Stats: 0:31:12 elapsed; 0 hosts completed (63 up), 63 undergoing Service Scan
Service scan Timing: About 63.49% done; ETC: 09:36 (0:17:39 remaining)
Nmap scan report for macdeproyectos.ugr.es (150.214.101.120)
Host is up (0.017s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh?
3389/tcp  open  ms-wbt-server?

Nmap scan report for eppursimuove.ugr.es (150.214.102.112)
Host is up (0.0100s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
3389/tcp  open  ms-wbt-server?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for atcmqtt.ugr.es (150.214.103.170)
Host is up (0.0095s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh?
3389/tcp  open  ms-wbt-server?

```

Figura 3.22: Captura de pantalla con escaneo de nmap sobre el conjunto de IPs y con una serie de parámetros para evitar la detección y bloqueo de los sistemas de seguridad.

Los hallazgos más relevantes que pueden observarse son en relación a la versión de SSH en los siguientes sistemas:

- eppursimuove.ugr.es (150.214.102.112): OpenSSH 7.6p1
- void.ugr.es (150.214.190.100): OpenSSH 7.6p1
- vcscontrol.ugr.es (150.214.194.249): OpenSSH 6.6
- ddred.ugr.es (150.214.199.63): OpenSSH 5.6

- varuiz.ugr.es (150.214.208.16): OpenSSH 6.5
- gis.ugr.es (150.214.21.198): OpenSSH 5.8
- granasat2.ugr.es (150.214.26.131): OpenSSH 8.4p1
- cmisabel.ugr.es (150.214.28.176): OpenSSH 7.4

OpenVAS es una herramienta web de código abierto para el escaneo de vulnerabilidades.

El análisis resulta más eficiente si se basa en IPs, por lo que basándose en los análisis previos se reconocen 1205 IPs del rango 150.214.c.d que podrían escanearse. Por precaución se restringe el escaneo al puerto SSH (22) de las 2 IPs seleccionadas provenientes de los resultados de los escaneos de Nmap que mostraron una versión de SSH antigua: vcscontrol.ugr.es (150.214.194.249) y ddred.ugr.es (150.214.199.63). La Figura 3.23 muestra el resultado de ambos escaneos.

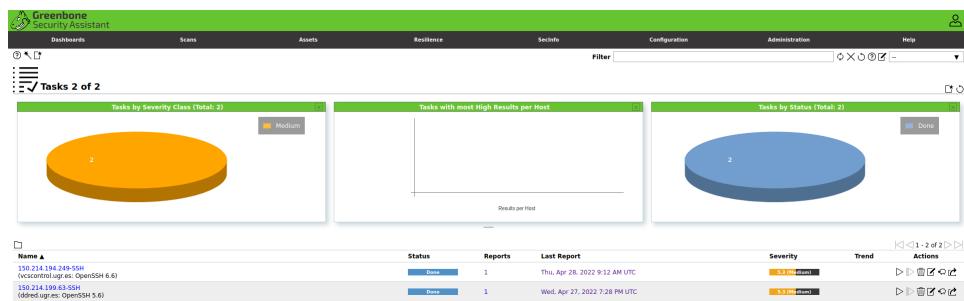


Figura 3.23: Captura de pantalla con resultados de escaneos de vulnerabilidades en el puerto SSH de OpenVAS.

El resultado de los escaneos de vulnerabilidades destaca una serie de vulnerabilidades de severidad baja y media observable en la Figura 3.24, así como el reconocimiento del sistema externo como una impresora de marca HP observable en la Figura 3.25.

Vulnerability	Severity	QoD	Host IP
Weak Host Key Algorithm(s) (SSH)	5.3 (Medium)	80 %	150.214.199.63
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)	80 %	150.214.199.63
Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)	95 %	150.214.199.63
Weak MAC Algorithm(s) Supported (SSH)	2.6 (Low)	95 %	150.214.199.63

Figura 3.24: Captura de pantalla con detalles de las vulnerabilidades detectadas por OpenVAS en un objetivo.

Operating System	CPE
HP JetDirect	cpe:/h:hp:jetdirect

Figura 3.25: Captura de pantalla con detalles del Sistema Operativo detectado por OpenVAS en un objetivo.

Nessus es un escáner de vulnerabilidades propietario desarrollado por Tenable. La versión gratuita permite el escaneo de hasta 16 IPs.

El análisis resulta más eficiente si se basa en IPs, por lo que basándose en los análisis previos se reconocen 1205 IPs del rango 150.214.c.d que podrían escanearse. Por precaución y a fin de poder comparar los resultados, se restringe el escaneo a al puerto SSH (22) de las IP observada en los escaneos de Nmap y OpenVAS que mostraron una versión de SSH antigua y un mayor número de vulnerabilidades.

La Figura 3.26 muestra como la cantidad de vulnerabilidades detectadas por Nessus es mayor a OpenVAS. Por otro lado Nessus también logra detectar detalles del ambiente en el que el sistema se encuentra, como la posible presencia de un Firewall de marca Check Point, observable en la Figura 3.27.

Vulnerabilities 17

Score ▾	Name ▾	Family ▾	Count ▾
7.5	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	1
6.5	SSL Certificate Cannot Be Trusted	General	1
6.4 *	SSL Self-Signed Certificate	General	1
LOW	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	1
INFO	SSL Certificate 'CommonName' Mismatch	General	1
INFO	SSL Certificate Information	General	1
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1
INFO	SSL Cipher Suites Supported	General	1

Figura 3.26: Captura de pantalla de Nessus con detalles de vulnerabilidades SSH en un objetivo.

3.27

ddred.ugr.es (150.214.199.63): OpenSSH 5.6

Severity	Critical	High	Medium	Low	Info
General	1	0	0	0	0
Service detection	1	0	0	0	0
Plugins	3	0	0	0	0
Misc.	6	0	0	0	0
Settings	2	0	0	0	0
FTP	1	0	0	0	0
General	1	0	0	0	0
Service detection	1	0	0	0	0
Service detection	1	0	0	0	0
Service detection	1	0	0	0	0
Service detection	1	0	0	0	0
Service detection	1	0	0	0	0
Service detection	1	0	0	0	0
Service detection	1	0	0	0	0
General	1	0	0	0	0
General	1	0	0	0	0
General	1	0	0	0	0
General	1	0	0	0	0

Figura 3.27: Captura de pantalla de Nessus con todas las vulnerabilidades detectadas y detalles del ambiente conseguidos durante el análisis de un objetivo centrado en SSH.

3.4.2. Soluciones de Threat Hunting

La práctica de Threat Hunting es considerada relativamente nueva, a pesar de que algunas organizaciones ejecutaban sus procesos incluso antes de que tenga este nombre, usualmente como una tarea adicional por parte de los CSIRT, los equipos de ciberinteligencia, los equipos de detección de amenazas y/o los equipos del SOC. Por esa razón muchas de las herramientas que se utilizan, como el SIEM, el UEBA o el EDR, están ya incorporadas por las organizaciones. Aunque en los últimos años han sido desarrolladas soluciones individuales específicas para asistir al Threat Hunter en las diferentes metodologías, aún pueden ser consideradas escasas y poco maduras en comparación a las soluciones existentes en otras prácticas, y no suelen ser multipropósito o multifunción. Respecto a las soluciones empaquetadas se observa:

- Debido a que el proceso para implementar metodologías de Threat Hunting basadas en inteligencia suele apoyarse por el proceso II de ciberinteligencia, las soluciones empaquetadas de ciberinteligencia que se relevaron previamente incluyen también soluciones individuales que facilitan esta esta metodología de Threat Hunting, pero en ningún caso incluyen también soluciones que asistan en el proceso para implementar metodologías de Threat Hunting basadas en datos. Por esta razón, será necesario considerar soluciones empaquetadas exclusivamente orientadas al Threat Hunting.
- Por el solapamiento observado entre las práctica de Threat Hunting y DFIR, muchas de las soluciones empaquetadas suelen incluir mayoritariamente recursos y herramientas orientados a la respuesta a incidentes y el análisis e ingeniería inversa de malware (es decir, por fuera de lo que se pretende o necesita en estos casos), resultando soluciones agobiantes o demasiado complejas para un Threat Hunter iniciando en esta práctica. Ejemplos de ello son las distribuciones Caine, CSI, Cuckoo, Flare, Remnux, SIFT, Slingshot y Tsurugi entre otras.
- Dado que uno de los posibles resultados que genera el Threat Hunting es la mejora de las detección existentes y el desarrollo de prototipos para nuevas detección, existe un solapamiento entre Threat Hunting y Threat Detection, por lo que soluciones empaquetadas como la distribución Security Onion incluyen más recursos y herramientas orientados al monitoreo y gestión de eventos de seguridad. El repositorio “awesome-threat-detection”[108] detalla múltiples herramientas y recursos usados en ambas prácticas.
- Otras soluciones empaquetadas orientadas al Threat Hunting se focalizan en herramientas que asistan en la metodología basada en hipótesis, esto resulta de que Threat Hunting es una práctica implementada en

su mayoría por organizaciones con maduración alta en ciberseguridad. Ejemplos de ello son ThreatPursuit y RedHunt. Por otro lado, si bien ambas cuentan con algunas soluciones para asistir en el proceso V de ciberinteligencia, no son suficientes, y las máquinas virtuales no han sido actualizadas en los últimos 18 meses. Alternativamente, los capítulos 7 a 14 del libro “Practical Threat Intelligence and Data-Driven Threat Hunting”[109] (Valentina Palacin) proveen instrucciones detalladas para la preparación y construcción de una máquina virtual de Threat Hunting similar a estas, y su implementación/uso en un ambiente de producción.

A fin de comprender las soluciones individuales deseadas para realizar Hunts que usen metodologías basadas en datos y no se focalicen en metodologías basadas en hipótesis, es importante comprender que las metodologías basadas en Hipótesis son categorizadas como estructuradas debido a que durante la fase de planificación se considera el contexto de la organización, los activos más importantes, los perfiles de adversarios reconocidos, las detecciones ya implementadas, los incidentes de seguridad ocurridos anteriormente así como muchos otros factores, y por el contrario la metodología basada en datos es categorizada como no estructurada debido a que durante la fase de planificación se consideran principalmente comportamientos maliciosos que han sido observados en distintas organizaciones (y en muchos casos son relativamente simples de buscar). A continuación se detallan algunos ejemplos de Hunts que podrían realizarse con metodología basada en datos:

- Combinación de eventos inusuales: Análisis de eventos ocurridos en períodos cortos de tiempo que por sí mismos no resultan relevantes pero combinados podrían ser indicativo de actividad inusual. Por ejemplo, un sistema en el que se detecte ejecuciones de comandos codificados y pocos segundos después manipulaciones de registros de eventos, o secretos (Contraseñas, Tokens, etc.) almacenados en los registros de eventos por ser utilizado como argumento en línea de comandos asociados a usuarios que este accediendo interactivamente a sistemas.
- Correlación de eventos de seguridad: Análisis de alertas o detecciones de baja prioridad provenientes de soluciones de seguridad en un período corto de tiempo que en base a algún dato específico acarrean una severidad mayor. Por ejemplo, dos detecciones de criticidad baja provenientes de un mismo sistema en un mismo día.
- Anomalías de acceso web: Peticiones HTTP repetitivas a dominios que no tengan una categoría asignada por el Web Proxy, valores inusuales en el parámetro “User-Agent” del encabezado HTTP, baja cantidad de parámetros presente en el encabezado HTTP de una petición (menos de 6 ya podría ser considerado fuera de lo normal), parámetro

“Content-length” del encabezado HTTP inexistente (por RFC es obligatorio).

- Irregularidades en el sistema: Librerías o ejecutables con nombre conocido cuyo Hash no ha sido visto antes o se encuentran en directorios inesperados, procesos homoglifos (por ejemplo, un proceso ejecutando como “svch0st.exe” para imitar a “svchost.exe”), código firmado con certificados falsificados, maliciosos o robados (ver el artículo “Tracking a stolen code-signing certificate with osquery”[110]), Drivers no firmados o expirados (ver el artículo “Tracking driver inventory to unearth rootkits”[111]), relaciones entre procesos padre e hijo poco comunes (por ejemplo, “cmd.exe” ejecutado por “winword.exe” o “svchost.exe” ejecutado por un proceso distinto a “services.exe”), comandos de Powershell con argumentos sospechosos (por ejemplo “-ExecutionPolicy Bypass” o “-EncodedCommand”), abuso de *Pipes* (ver artículo “Threat Hunting for PsExec, Open-Source Clones, and Other Lateral Movement Tools”[112]), abuso de “GetSystem” para escalar privilegios a usuario de sistema (ver el artículo “Hunting for GetSystem in offensive security tools”[113]), abuso de binarios preinstalados en Sistemas Operativos para evadir restricciones de seguridad (ver los proyectos LOLBAS[114] y GTFOBins[115]).
- Comunicaciones de red extrañas: Encapsulamiento de tráfico en peticiones DNS (por ejemplo, un alto volumen de peticiones de tipo NULL o TEXT podrían dar indicio sobre exfiltración de información mediante técnicas de *DNS Tunneling*), posible envío de balizas (*Beacons*) hacia sistemas de *Command & Control* (C&C) mediante servicios legítimos (ver el artículo “Rise of Legitimate Services for Backdoor Command and Control”[116]), accesos repetitivos desde un sistema subdominios en un sistema de nombres de dominio dinámicos (DDNS), peticiones DNS hacia dominios de la DarkNet provenientes de procesos distintos al de un navegador asociado a esa red (por ejemplo, una petición hacia un dominio “.onion” que no sea desde el navegador utilizado por TOR), alto volumen de tráfico hacia dominios que hayan sido registrados recientemente (ver el artículo “Tracking Newly Registered Domains”[117]), personificación de servicios cifrados existentes mediante técnicas de apropiación de nombres de dominio (*Cybersquatting*) combinado con certificados digitales falsificados o robados (ver detalles sobre cómo monitorear dominios similares en el “Certificate Transparency” (CT) log en el artículo “Proactive Malicious Domain Search”[118]), peticiones DNS a dominios generados por algoritmos (DGAs) (por ejemplo, mediante técnicas de Entropía[119] o mediante técnicas de procesamiento de lenguaje natural [NLP][120]), búsquedas pasivas mediante JA3[121] o activas mediante JARM[122] (ambas

desarrolladas por Salesforce) de Fingerprint TLS inusuales.

Es sencillo observar cómo estos Hunts dependen en gran medida de los sistemas y soluciones de seguridad que estén implementados, tal que si se dispone de un SIEM Splunk sería conveniente implementar la aplicación “ThreatHunting”[123] que genera tableros y reportes basados en MITRE ATT&CK para guiar los Hunts fácilmente, y por otro lado si se dispone del SIEM Elastic Stack convendría desplegar Flare[124] para realizar prototipos y análisis de comportamiento basado en comunicaciones de red a fin de identificar artefactos maliciosos.

La Tabla 3.5 lista las soluciones individuales que podrían asistir en el Threat Hunting con metodologías basadas en datos y no dependen ni se apoyan en un proveedor específico:

Nombre	Actualizado	Descripción
RITA	22-04	Análisis de patrones en comunicaciones de red para detectar conexiones maliciosas.
APT-Hunter	22-02	Análisis de eventos de Windows para detectar actividad maliciosa.
DeepBlueCLI	22-02	Análisis de eventos de Windows para detectar actividad maliciosa.
dnstwist	22-04	Generador de dominios similares que un adversario podría utilizar para personificar.
Oriana	19-09	Análisis de eventos de Windows para detectar actividad maliciosa.
Revoke-Obfuscation	20-02	Análisis de eventos de Windows para comandos ofuscados.

Tabla 3.5: Soluciones individuales para asistir en el Threat Hunting con metodología basada en datos.

RITA es un analizador del tráfico de red que se basa en logs con formato Zeek para detectar balizas de C&C, túneles DNS, conexiones inusualmente largas, comunicaciones con dominios o IPs en listas negras y otras anomalías de red. La Figura 3.28 muestra el primer paso, importar los logs en formato Zeek en la base de datos.

```
root@zeek:~/zeeksample$ rita Import * Sampletest
[+] Importing [capture_loss.log.gz conn.log.gz dce_rpc.log.gz dns.log.gz dpd.log.gz files.log.gz ftp.log.gz http.log.gz kerberos.log.gz modbus.log.gz notice.log.gz ntlm.log.gz ntp.log.gz pe.log.gz rdp.log.gz rfc3618.log.gz ssh_mapping.log.gz smtp.log.gz snmp.log.gz ssl.log.gz stats.log.gz syslog.log.gz weird.log.gz x509.log.gz zed-sample-data];
[+] Verifying log files ... (1 log file(s) have been previously parsed into the target dataset ...
[.] Processing batch 1 of 1
[.] UConn SampleTest ...
[.] Parsing http.log.gz -> SampleTest
[.] Parsing ssl.log.gz -> SampleTest
[.] Parsing dns.log.gz -> SampleTest
[.] Parsing dns.log.gz -> SampleTest
[.] Finished parsing logs in 2.484s
[.] Total log entries: 1242 [=====]
[.] UConn Analysis: 2428 / 2428 [=====] 100 %
[.] UConn Proxy Analysis: 7 / 5 [=====] 100 %
[.] UConn Port Analysis: 1650 / 1650 [=====] 100 %
[.] Hostname Analysis: 1650 / 1650 [=====] 100 %
[.] Beacon Analysis: 9428 / 9428 [=====] 100 %
[.] Other analysis for Beacon analysis: [=====]
[.] FQDN Beacon Analysis: 802 / 802 [=====] 100 %
[.] Invalid Beacon Analysis: 0 / 0 [=====] 100 %
[.] UserAgent Analysis: 39 / 39 [=====] 100 %
[.] Invalid Cert Analysis: 12 / 12 [=====] 100 %
[.] Invalid Certificate Headers ...
[.] Indexing log entries ...
[.] Updating metadatabase ...
[.] Done!
```

Figura 3.28: Captura de pantalla con importación de logs en formato Zeek a RITA.

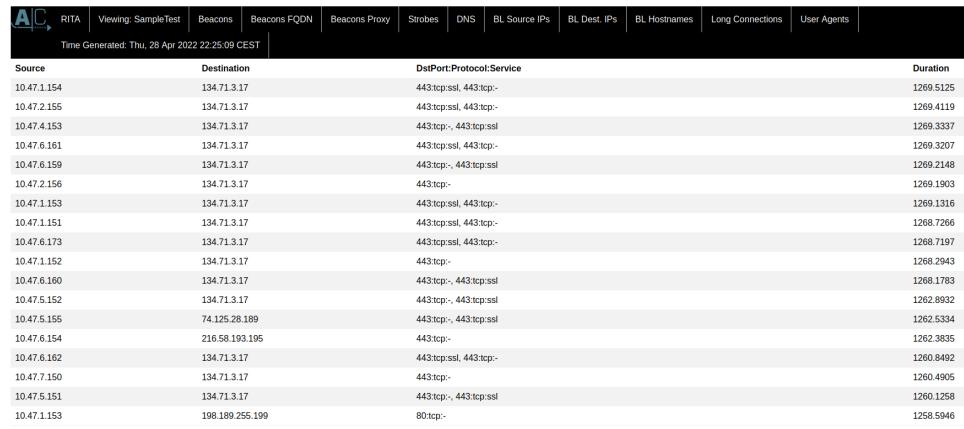
Las Figuras 3.29, 3.30, 3.31 muestran los resultados obtenidos luego de que la herramienta genera un reporte HTML en base al análisis que realizó.

RITA															RITA on Q
Viewing: SampleTest															
	Beacons	Beacons FQDN	Beacons Proxy	Strobes	DNS	BL Source IPs	BL Dest. IPs	BL Hostnames	Long Connections	User Agents					
Score	Source	Destination	Connections	Avg. Bytes	Intvl. Range	Size Range	Intvl. Mode	Size Mode	Intvl. Mode Count	Size Mode Count	Intvl. Skew	Size Skew	Intvl. Dispersion	Size Dispersion	Total Bytes
0.920	10.47.2.155	192.229.211.36	68	10777.000	6	80	1	1042	2	47	0.000	0.000	0	0	732889
0.897	10.47.7.154	134.71.3.16	88	10382.000	12	3218	12	3068	19	73	0.200	0.000	2	0	913684
0.891	10.47.2.155	104.16.18.96	50	11193.000	6	6718	1	1068	2	29	0.000	0.000	1	0	559662
0.887	10.47.7.150	134.71.3.16	130	10698.000	11	3226	12	3076	53	116	-0.600	0.000	1	0	1390766
0.882	10.47.6.160	134.71.3.16	43	10956.000	23	3226	30	3076	36	38	0.000	0.000	0	0	471110
0.881	10.47.8.10	198.199.95.203	41	3680.000	31	400	30	2424	27	23	0.000	0.000	0	0	150897
0.874	10.47.2.155	23.73.187.161	33	13437.000	6	1474	1	1082	3	21	0.000	0.000	0	0	443424
0.861	10.47.2.155	74.126.28.189	102	3830.000	635	49674	1	304	9	97	0.600	0.000	1	0	390754
0.860	10.47.3.156	151.101.65.69	24	30888.000	599	13894	2	0	7	20	0.000	0.000	1	0	741324
0.858	10.47.6.162	134.71.3.16	24	11443.000	218	1528	30	3076	16	20	0.000	0.000	0	0	274642
0.854	192.168.204.57	159.99.66.200	24	76.000	1	0	150	76	22	24	0.000	0.000	0	0	1824
0.853	10.47.7.154	216.50.193.193	25	1794.000	403	3570	7	0	3	15	0.000	0.000	6	0	44864
0.824	10.47.4.153	134.71.3.16	252	27599.000	35	33198	30	1782	29	17	0.000	0.031	0	0	6955050
0.822	10.47.2.100	151.101.196.133	297	12227.000	447	23852	1	0	30	125	0.000	0.069	0	2102	3631602
0.817	10.47.2.155	134.71.3.16	155	27352.000	496	31992	30	2242	11	9	0.000	-0.034	1	3580	4239580
0.817	10.47.4.151	134.71.3.16	244	29265.000	30	27148	30	1782	35	16	0.000	0.073	0	2686	7140790
0.816	10.47.5.156	134.71.3.16	258	28951.000	30	47168	30	1776	32	27	0.000	-0.082	0	1564	7376568
0.814	10.47.4.100	134.71.3.16	206	28095.000	50	35744	30	2046	23	17	0.000	0.052	1	2500	5787572

Figura 3.29: Captura de pantalla con estadísticas de posibles detecciones de balizas de RITA.

RITA															RITA on Q
Viewing: SampleTest															
	Beacons	Beacons FQDN	Beacons Proxy	Strobes	DNS	BL Source IPs	BL Dest. IPs	BL Hostnames	Long Connections	User Agents					
IP	Connections			Unique Connections			Total Bytes			Sources					
59.148.253.194	10			1			560707			172.16.0.170					
104.131.62.48	5			1			460			172.16.0.170					
144.217.88.125	5			1			1152674			172.16.0.149					
180.250.21.2	4			1			567419			172.16.0.170					
139.196.72.155	3			1			453279			172.16.0.170					
198.199.98.78	1			1			776570			172.16.0.170					
54.37.106.167	1			1			3701			172.16.0.170					
128.199.93.156	1			1			535620			172.16.0.170					
185.184.25.78	1			1			1137083			172.16.0.170					
128.199.192.135	1			1			244319			172.16.0.170					

Figura 3.30: Captura de pantalla con estadísticas de conexiones entre IPs de RITA a fin de detectar posible exfiltración de información.



The screenshot shows a table of network connection statistics from the RITA tool. The columns are: Source, Destination, DstPort:Protocol:Service, and Duration. The data includes various IP addresses and port numbers, with some entries showing extended duration times like 1269.5125 seconds.

Source	Destination	DstPort:Protocol:Service	Duration
10.47.1.154	134.71.3.17	443/tcp:ssl, 443/tcp:-	1269.5125
10.47.2.155	134.71.3.17	443/tcp:ssl, 443/tcp:-	1269.4119
10.47.4.153	134.71.3.17	443/tcp:-, 443/tcp:ssl	1269.3337
10.47.6.161	134.71.3.17	443/tcp:ssl, 443/tcp:-	1269.3207
10.47.6.159	134.71.3.17	443/tcp:-, 443/tcp:ssl	1269.2148
10.47.2.156	134.71.3.17	443/tcp:-	1269.1903
10.47.1.153	134.71.3.17	443/tcp:ssl, 443/tcp:-	1269.1316
10.47.1.151	134.71.3.17	443/tcp:ssl, 443/tcp:-	1268.7266
10.47.6.173	134.71.3.17	443/tcp:ssl, 443/tcp:-	1268.7197
10.47.1.152	134.71.3.17	443/tcp:-	1268.2943
10.47.6.160	134.71.3.17	443/tcp:-, 443/tcp:ssl	1268.1783
10.47.5.152	134.71.3.17	443/tcp:-, 443/tcp:ssl	1262.8932
10.47.5.155	74.125.29.189	443/tcp:-, 443/tcp:ssl	1262.5334
10.47.6.154	216.58.193.195	443/tcp:-	1262.3835
10.47.6.162	134.71.3.17	443/tcp:ssl, 443/tcp:-	1260.8492
10.47.7.150	134.71.3.17	443/tcp:-	1260.4905
10.47.5.151	134.71.3.17	443/tcp:-, 443/tcp:ssl	1260.1258
10.47.1.153	198.189.255.199	80/tcp:-	1258.5946

Figura 3.31: Captura de pantalla con estadísticas de conexiones de IPs de RITA a fin de detectar conexiones inusualmente extendidas.

Los resultados que corresponden al escenario observado en estas imágenes se basan en una combinación de muestras de comunicaciones de red, algunas de las cuales incluyen específicamente tráfico de red maliciosa conocido.

APT-Hunter es una herramienta desarrollada en Python que analiza eventos de Windows con el fin de detectar actividad maliciosa.

Al ejecutarse puede leer una serie de archivos en formato EVTX y genera un reporte en formato XLSX que incluye todos los eventos detectados, un reporte en formato CSV para ser utilizado en Timesketch y otro reporte en formato CSV que incluye todos los inicios de sesión y su correspondiente información (también puede ser utilizado con Timesketch). La Figura 3.32 muestra APT-Hunter analizando una serie de archivos con formato EVTX y la Figura 3.33 muestra el reporte generado en formato XLSX.

Figura 3.32: Captura de pantalla de APT-Hunter analizando un conjunto de archivos con formato EVTX.

Figura 3.33: Captura de pantalla del reporte en formato XLSX generado por APT-Hunter.

Los resultados que corresponden al escenario observado en estas imágenes se basan en una serie de muestras de eventos de Windows obtenidas del repositorio de Github la herramienta DeepBlueCLI.

DeepBlueCLI es una herramienta desarrollada en Powershell que analiza eventos de Windows con el fin de detectar actividad maliciosa. Una versión en Python funcional se encuentra disponible, y si bien no parece estar siendo actualizada, podría resultar suficiente en caso de requerir la ejecución de esta solución en un sistema Linux.

Al ejecutarse puede leer un archivo en formato EVTX a la vez. Mediante Pipes y otros comandos de Powershell (por ejemplo “—Format-Table” o “—ConvertTo-Csv”) pueden visualizarse los resultados con mayor facilidad. La Figura 3.34 muestra una serie de ejecuciones de DeepBlueCLI en base a una muestra de eventos de Windows obtenidas del propio repositorio de Github de la herramienta.

Figura 3.34: Captura de pantalla de múltiples análisis realizados por DeepBlueCLI en base a múltiples archivos con formato EVTX.

dnstwist utiliza diferentes técnicas de *Cybersquatting* sobre un dominio para detectar dominios similares que hayan sido registrados, proveyendo información respecto a la geolocalización, los registros DNS de tipo NS y MX, la IP y la tasa de similaridad (porcentual) del sitio web en relación al dominio original. En la Figura 3.35 se observan los resultados obtenidos por la herramienta sobre el dominio ugr.es.

```
(kali㉿kali)-[~/dnstwist]
$ dnstwist -t 2 --registered -w -p --ssdeep --mxcheck -g ugr.es
[...]
{20220131}

Fetching content from: http://ugr.es > https://www.ugr.es/ [84.5 KB]
Rendering web page: http://ugr.es
Permutations: 100.00% of 662, Found: 26, ETA: 00:00 [ 5 qps]
WHOIS: 100.00% of 26

+original      ugr.es    150.214.27.71/Spain NS:avion1.ugr.es MX:mx01.puc.rediris.es PHASH:100%
bitsquatting   egr.es    212.83.163.35/France NS:ns1.srv-acens.com MX:mx.egr.es PHASH:12%
bitsquatting   tgr.es    185.53.178.52/Germany NS:ns1.parkingcrew.net MX:mail.h-email.net
bitsquatting   ucr.es    99.83.248.67/UnitedStates NS:ns1.parkingcrew.net MX:mail.h-email.net PHASH:27%
bitsquatting   uer.es    64.190.63.111/UnitedStates NS:ns1.sedoparking.com MX:localhost PHASH:9%
bitsquatting   ugb.es    52.58.78.16/Germany 2001:1d0:801:2000:515 NS:ns.doomey.de MX:mx2.hostmailer.xyz PHASH:9%
bitsquatting   ugs.es    64.190.63.111/UnitedStates NS:ns1.sedoparking.com MX:localhost PHASH:9%
bitsquatting   ugv.es    99.83.248.67/UnitedStates NS:ns1.parkingcrew.net MX:mail.h-email.net PHASH:27%
bitsquatting   uor.es    64.190.63.111/UnitedStates NS:ns1.sedoparking.com MX:localhost PHASH:12%
homoglyph      uqr.es    67.214.175.75/UnitedStates NS:ns1.dnsexit.com PHASH:3%
replacement    hgr.es    46.29.49.11/Spain NS:ns1.hospedajeydominios.com MX:mail.hgr.es
replacement    igr.es    64.190.63.111/UnitedStates NS:ns1.sedoparking.com MX:localhost
replacement    ubr.es    213.186.33.5/France NS:ns1.ovh.net MX:mx3.mail.ovh.net PHASH:23%
replacement    ugd.es    13.37.74.225/UnitedStates NS:ns1.eurodns.com PHASH:12%
replacement    uegs.es  64.190.63.111/UnitedStates NS:ns1.sedoparking.com MX:localhost
replacement    ugf.es    185.53.178.54/Germany NS:ns1.parkingcrew.net MX:mail.h-email.net PHASH:27%
replacement    ugt.es    213.149.245.114/Spain NS:ns1.telefonica-data.com MX:mailugt.ugt.org
replacement    uhrs.es  45.87.158.7/Switzerland NS:ns.inwx.de
replacement    utres.es  134.0.11.42/Spain NS:ns1.cdmom.net MX:alt1.aspxmx.l.google.com
replacement    uvr.es    31.214.178.54/Spain NS:ns1.dondominio.com PHASH:3%
replacement    ygr.es    64.190.63.111/UnitedStates NS:ns1.sedoparking.com MX:localhost PHASH:9%
replacement    zgr.es    217.76.128.34/Spanish NS:ns1.dnservidoresds.net
transposition   gur.es    217.116.0.144/Spanish NS:ns1.srv-hostalia.com MX:mx.gur.es
transposition   urg.es    199.59.243.200/UnitedStates NS:ns1.bodis.com
vowel-swap     agr.es    91.134.184.208/Spanish NS:ns1.dnsxperta.com MX:agr-es.mail.protection.outlook.com
vowel-swap     ogr.es    64.190.63.111/UnitedStates NS:ns1.sedoparking.com MX:localhost PHASH:9%
```

Figura 3.35: Captura de pantalla con resultados de dnstwist.

Capítulo 4

Diseño

A partir del análisis realizado en las Secciones 3.4.1 y 3.4.2 se observa que existe una tendencia a recomendar que las organizaciones armen sus propias soluciones empaquetadas en base a Sistemas Operativos reconocidos y agregando el conjunto de soluciones que se adapten a sus requisitos específicos. Se destaca de ambas secciones también que:

- En cuanto a las soluciones de ciberinteligencia puede concluirse que de las 9 soluciones individuales preseleccionadas debería ser suficiente con **Spiderfoot**, **theHarvester**, **Maltego**, **nmap** y **Nessus**.
- En cuanto a las soluciones de Threat Hunting puede concluirse que resultan particularmente beneficiosas las herramientas **RITA**, **APT-Hunter** y **dnstwist** (aunque será imprescindible disponer de herramientas y recursos que se adapten a las soluciones de seguridad ya existentes para nutrir los análisis).

Las soluciones empaquetadas pre-armadas en forma de Máquinas Virtuales o Scripts tienen como desventaja que suelen quedar desactualizadas o dejar de ser mantenidas y/o contienen herramientas que no se utilizaran, en algunos casos siendo abrumadora la cantidad incluida. Teniendo en cuenta el desafío que el armado de una soluciones empaquetada propia representa en términos de cantidad de tiempo a invertir y profundidad de conocimientos necesaria, es usual que se recurra a las soluciones empaquetadas prearmadas.

No se han encontrado soluciones prearmadas que abarquen herramientas de ambas prácticas en el relevamiento, en parte por ser usualmente prácticas ejecutadas por especialistas de ciberseguridad diferentes. Sin embargo, como se ha visto en la Sección 3.1, las organizaciones que comienzan a desarrollarse en estas prácticas no suelen disponer de suficiente personal y/o recursos para desplegar equipos en cada una.

Un Script que instala todas las herramientas en un sistema operativo reconocido provee más garantías a los usuarios que una máquina virtual ya

empaquetada, debido a que el Script es más fácil de auditar y verificar. Como ventajas adicionales, resulta más fácil de actualizar (o bien modificar) por futuros desarrolladores y puede implementarse en Máquinas Virtuales o físicas.

Por las razones mencionadas, se optara por el desarrollo de un **Script** en **Bash** que en base a un Sistema Operativo **Ubuntu 20.04 LTS** instale las herramientas Spiderfoot, theHarvester, Maltego, nmap, Nessus, RITA, APT-Hunter y dnstwist. El Script instalará todos los prerequisitos que estas herramientas necesiten y dará la posibilidad de instalar las herramientas de Ciberinteligencia y/o las herramientas de Threat Hunting. El Script podrá ser ejecutado por cualquier usuario, pero debido a que descargara e instalará/actualizara paquetes, se deberá escalar privilegios mediante el uso del comando “sudo”.

Capítulo 5

Implementación

El primer paso sera descargar e instalar la versión de Ubuntu deseada siguiendo los pasos indicados en el sitio web oficial[125]. Al seleccionar el modo de instalación, el script funcionará apropiadamente tanto con el modo “Minimal” como “Normal”.

Luego de haber finalizado la instalación e iniciado el Sistema Operativo, se recomienda obtener el Script desde su repositorio de Github denominado “**HunTnisO**”[126], donde se mantendrá actualizado a su última versión disponible, o en su defecto copiando manualmente desde Listado de código 5.1 hacia un archivo.

```
1 #!/bin/bash
2
3 # Colors
4 g="\e[0;32m\033[1m" # Good
5 b="\e[0;31m\033[1m" # Bad
6 n="\033[0m\e[0m" # Normal
7 # Variables
8 pwd=$(pwd)
9
10 # Banner
11 function banner() {
12     echo -e ' _ _ '
13     echo -e '| | | | - - - - - | - - - - - | - - - - - | - - - - - | - - - - - | - - - - - | - - - - - | - - - - - | '
14     echo -e '| | | | | | | / - \ | | | | | | | / - \ | | | | | | | / - \ | | | | | | | / - \ | | | | | | | / - \ | '
15     echo -e '| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | '
16     echo -e '| | | | | | | . - / | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | '
17     echo -e
18     echo -e "Usage:"
19     echo -e " --osint: Install OSINT tools."
20     echo -e " --hunt: Install Hunting tools."
21     echo -e ""
22 }
23
24 # Check requirements and install them where needed.
25 function requirements() {
26     # Verify apt Packet Manager.
27     apt -v > /dev/null 2>&1
28     if [ $? -ne 0 ]; then
29         echo -e "${b}apt Packet Manager is not installed.${n}"
30         exit 1;
31 }
```

```
31 else
32     # Verify git.
33     git --version > /dev/null 2>&1
34     if [ $? -ne 0 ]; then
35         echo -e "${g}Installing git...${n}"
36         sudo apt -y install git > /dev/null 2>&1
37         if [ $? -ne 0 ]; then
38             echo -e "${b}git installation failed.${n}"
39             exit 1
40         fi
41     fi
42     # Verify python3.
43     python3 -V > /dev/null 2>&1
44     if [ $? -ne 0 ]; then
45         echo -e "${g}Installing python3...${n}"
46         sudo apt -y install python3 > /dev/null 2>&1
47         if [ $? -ne 0 ]; then
48             echo -e "${b}python3 installation failed.${n}"
49             exit 1
50         fi
51     fi
52     # Verify pip.
53     pip -v > /dev/null 2>&1
54     if [ $? -ne 0 ]; then
55         echo -e "${g}Installing pip...${n}"
56         sudo apt -y install pip > /dev/null 2>&1
57         if [ $? -ne 0 ]; then
58             echo -e "${b}pip installation failed.${n}"
59             exit 1
60         fi
61     fi
62     # Verify java.
63     java --version > /dev/null 2>&1
64     if [ $? -ne 0 ]; then
65         echo -e "${g}Installing java...${n}"
66         sudo apt -y install default-jre > /dev/null 2>&1
67         if [ $? -ne 0 ]; then
68             echo -e "${b}java installation failed.${n}"
69             exit 1
70         fi
71     fi
72 fi
73 }
74
75 # Spiderfoot.
76 function spiderfoot() {
77     cd $pwd
78     echo -e "${g}=-Spiderfoot=-${n}"
79     which spiderfoot > /dev/null 2>&1
80     if [ $? -eq 0 ]; then echo -e "${n}Spiderfoot already installed,
81     skipping...${n}" && return; fi
82     if [ -d "spiderfoot/" ]; then echo -e "${n}Directory 'spiderfoot/'"
83     already exists, skipping...${n}" && return; fi
84     git clone "https://github.com/smicallef/spiderfoot" > /dev/null 2>&1
85     if [ $? -ne 0 ]; then echo -e "${b}Spiderfoot download failed.${n}" &&
86     return; fi
87     cd spiderfoot
88     pip3 install -r requirements.txt > /dev/null 2>&1
89     if [ $? -ne 0 ]; then echo -e "${b}Spiderfoot requirements failed to
90     install.${n}" && return; fi
91     echo -e "${g}Spiderfoot usage: cd $pwd/spiderfoot/ && python3 sf.py -l
92     127.0.0.1:5001 (Web access: https://127.0.0.1:5001)${n}"
```

```
88 }
89
90 # nmap.
91 function NMap() {
92     echo -e "${g}=-nmap--${n}"
93     nmap -V > /dev/null 2>&1
94     if [[ $? -eq 0 ]]; then echo -e "${n}nmap already installed, skipping...${n}" && return; fi
95     sudo apt -y install nmap > /dev/null 2>&1
96     if [[ $? -ne 0 ]]; then echo -e "${b}nmap download/install failed.${n}" && return; fi
97     echo -e "${g}nmap usage: nmap -h${n}"
98 }
99
100 # theHarvester.
101 function theharvester() {
102     cd $pwd
103     echo -e "${g}=-theHarvester--${n}"
104     which theHarvester > /dev/null 2>&1
105     if [ $? -eq 0 ]; then echo -e "${n}theHarvester already installed, skipping...${n}" && return; fi
106     if [ -d "theHarvester/" ]; then echo -e "${n}Directory 'theHarvester/' already exists, skipping...${n}" && return; fi
107     git clone "https://github.com/laramies/theHarvester" > /dev/null 2>&1
108     if [ $? -ne 0 ]; then echo -e "${b}theHarvester download failed.${n}" && return; fi
109     cd theHarvester
110     pip3 install -r requirements.txt > /dev/null 2>&1
111     if [ $? -ne 0 ]; then echo -e "${b}theHarvester requirements failed to install.${n}" && return; fi
112     echo -e "${g}theHarvester usage: cd '$pwd/theHarvester/' && python3 theHarvester.py -h${n}"
113 }
114
115 # Maltego.
116 function maltego() {
117     echo -e "${g}=-Maltego--${n}"
118     which maltego > /dev/null 2>&1
119     if [ $? -eq 0 ]; then echo -e "${n}Maltego already installed, skipping...${n}" && return; fi
120     sudo dpkg -l maltego > /dev/null 2>&1
121     if [ $? -eq 0 ]; then echo -e "${b}Maltego already installed, skipping...${n}" && return; fi
122     wget -nc "https://maltego-downloads.s3.us-east-2.amazonaws.com/linux/Maltego.v4.3.0.deb" > /dev/null 2>&1
123     if [ $? -ne 0 ]; then echo -e "${b}Maltego download failed.${n}" && return; fi
124     sudo dpkg -i "Maltego.v4.3.0.deb" > /dev/null 2>&1
125     if [ $? -ne 0 ]; then echo -e "${b}Maltego installation failed.${n}" && return; fi
126     echo -e "${g}Maltego usage: maltego${n}"
127 }
128
129 # Nessus.
130 function Nessus() {
131     echo -e "${g}=-Nessus--${n}"
132     sudo dpkg -l nessus > /dev/null 2>&1
133     if [ $? -eq 0 ]; then echo -e "${n}Nessus is already installed, skipping...${n}" && return; fi
134     wget -nc "https://www.tenable.com/downloads/api/v1/public/pages/nessus/downloads/16125/download?i_agree_to_tenable_license_agreement=true" -O "Nessus-10.1.2-ubuntu110_amd64.deb" > /dev/null 2>&1
```

```
135 if [ $? -ne 0 ]; then echo -e "${b}Nessus installer already exists in
136     $pwd.${n}" && return; fi
137 sudo dpkg -i "Nessus-10.1.2-ubuntu1110_amd64.deb" > /dev/null 2>&1
138 if [ $? -ne 0 ]; then echo -e "${b}Nessus installation failed.${n}" &&
139     return; fi
140 sudo /bin/systemctl start nessusd.service > /dev/null 2>&1
141 if [ $? -ne 0 ]; then echo -e "${b}Nessus initialization failed.${n}" &&
142     return; fi
143 echo -e "${g}Nessus web access (Registration will be requested during
144     setup to get an activation code and user/pass): https
145     ://127.0.0.1:8834/${n}"
146 }
147
148 # RITA.
149 function Rita() {
150     cd $pwd
151     echo -e "${g}=-RITA=-${n}"
152     which rita > /dev/null 2>&1
153     if [ $? -eq 0 ]; then echo -e "${n}RITA already installed, skipping...${
154         n}" && return; fi
155     if [[ -d "rita/" ]]; then echo -e "${n}Directory 'rita/' already exists,
156         skipping...${n}" && return; fi
157     git clone "https://github.com/activecm/rita" > /dev/null 2>&1
158     if [ $? -ne 0 ]; then echo -e "${b}RITA download failed.${n}" && return;
159     fi
160     cd rita/
161     sudo ./install.sh --disable-zeek -r > /dev/null 2>&1
162     #if [ $? -ne 0 ]; then echo -e "${b}RITA installation failed.${n}" &&
163         return; fi
164     echo -e "${g}RITA usage: rita -h${n}"
165 }
166
167 # APT-Hunter.
168 function apt-hunter() {
169     cd $pwd
170     echo -e "${g}=-APT-Hunter=-${n}"
171     if [[ -d "APT-Hunter/" ]]; then echo -e "${n}Directory 'APT-Hunter/'"
172         already exists, skipping...${n}" && return; fi
173     git clone "https://github.com/ahmedkhlief/APT-Hunter" > /dev/null 2>&1
174     if [ $? -ne 0 ]; then echo -e "${b}APT-Hunter download failed.${n}" &&
175         return; fi
176     cd APT-Hunter
177     python3 -m pip install -r requirements.txt > /dev/null 2>&1
178     if [ $? -ne 0 ]; then echo -e "${b}APT-Hunter requirements failed to
179         install.${n}" && return; fi
180     echo -e "${g}APT-Hunter usage: python3 $pwd/APT-Hunter/APT-Hunter.py -h${
181         n}"
182 }
183
184 # dnstwist.
185 function dnstwist() {
186     cd $pwd
187     echo -e "${g}=-DNSTwist=-${n}"
188     if [[ -d "dnstwist/" ]]; then echo -e "${n}Directory 'dnstwist/' already
189         exists, skipping...${n}" && return; fi
190     git clone "https://github.com/elceef/dnstwist" > /dev/null 2>&1
191     if [ $? -ne 0 ]; then echo -e "${b}DNSTwist download failed.${n}" &&
192         return; fi
193     cd dnstwist
194     pip install . > /dev/null 2>&1
195     if [ $? -ne 0 ]; then echo -e "${b}DNSTwist installation failed.${n}" &&
196         return; fi
```

```
181     echo -e "${g}DNSTwist usage: python3 $pwd/dnstwist/dnstwist.py -h${n}"  
182 }  
183  
184 # Clean the screen.  
185 clear  
186 # Show the banner.  
187 banner  
188 if [[ $1 == "--osint" ]] || [[ $1 == "--hunt" ]]; then  
189     # Install requirements  
190     requirements  
191 fi  
192 if [[ $1 == "--osint" ]] || [[ $2 == "--osint" ]]; then  
193     # Install OSINT tools.  
194     echo -e "${n}+++ Threat Intelligence tools for OSINT +++${n}"  
195     spiderfoot  
196     NMap  
197     theharvester  
198     maltego  
199     Nessus  
200 fi  
201 if [[ $1 == "--hunt" ]] || [[ $2 == "--hunt" ]]; then  
202     # Install Hunt tools.  
203     echo -e "${n}+++ Threat Hunting tools +++${n}"  
204     Rita  
205     apt-hunter  
206     dnstwist  
207 fi  
208 # The End.  
209 echo -e "${n}+++ Game Over +++${n}"  
210 exit 0
```

Listado de código 5.1: Script en Bash para automatizar instalación de herramientas de OSINT y Threat Hunting no estructurado

Luego se deberá cambiar los permisos del archivo para permitir que sea ejecutado por el usuario en uso, mediante el comando “chmod +x”. Al ejecutar el script sin incluir ningún parámetro mostrará una ayuda con los parámetros que puede utilizarse, como se observa en la Figura 5.1.

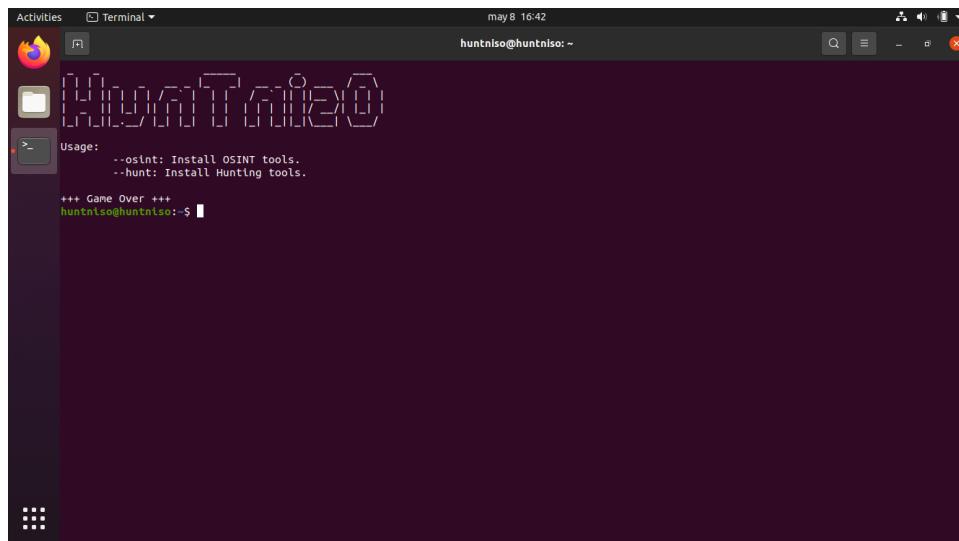


Figura 5.1: Captura de pantalla de ejecución de HunTnisO sin parámetros.

A fin de instalar las herramientas deseadas el Script puede ejecutarse con los parámetros “–osint” y “–hunt” por separado o bien juntos como se muestra en la Figura 5.2.

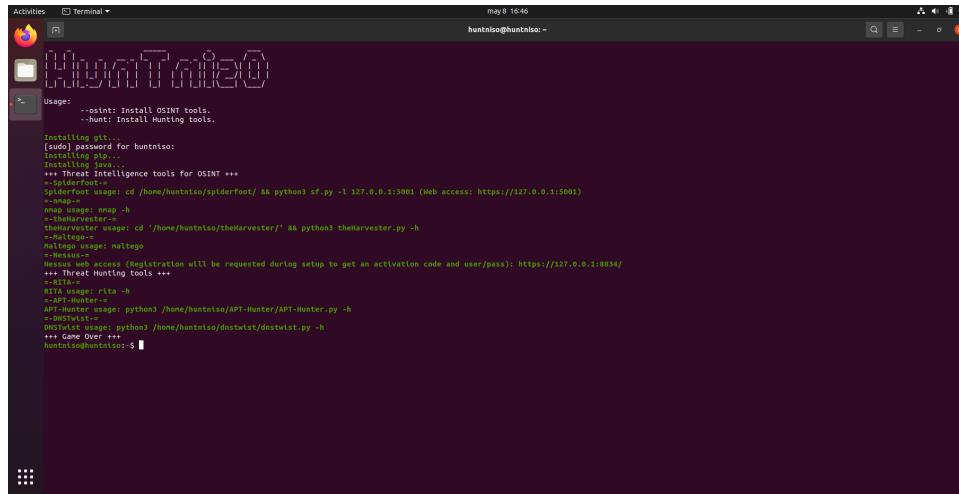
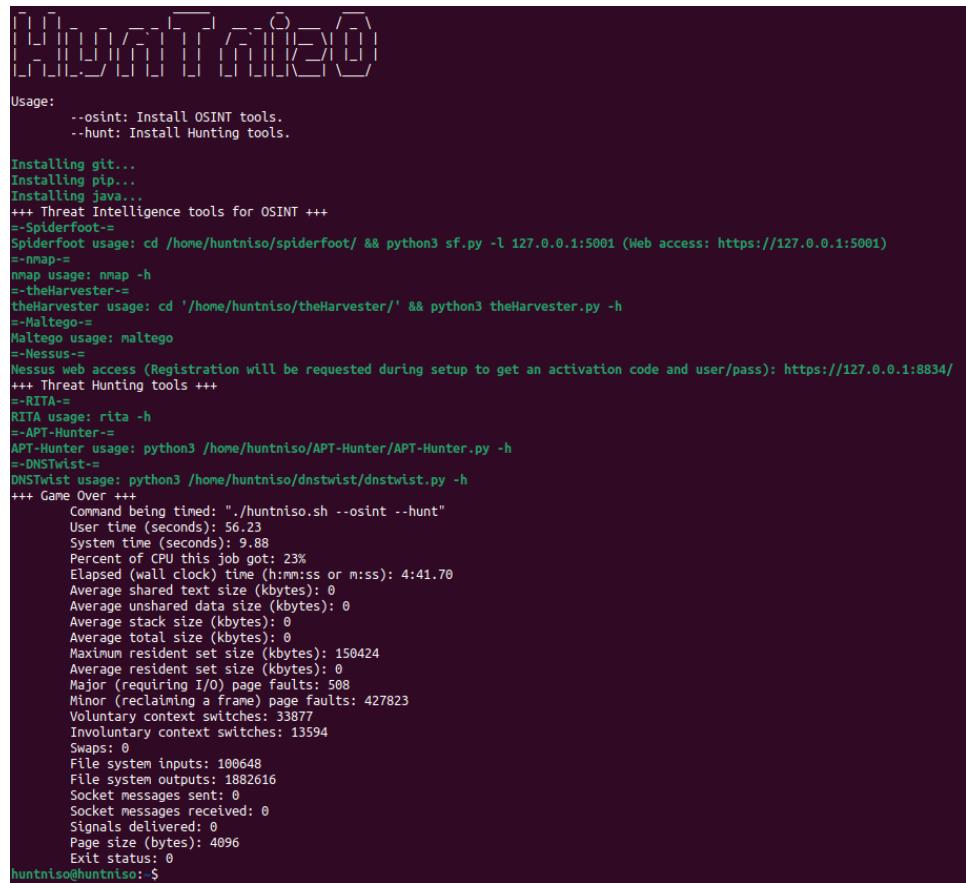


Figura 5.2: Captura de pantalla de ejecución de HunTnisO con ambos parámetros en Ubuntu 20.04 LTS.

Capítulo 6

Evaluación y pruebas

En la Figura 6.1 puede observarse que anteponiendo el uso del comando “time” a la ejecución del Script en una máquina virtual con Sistema Operativo Ubuntu 20.04 con 4 procesadores, 2048 MBs de RAM y conexión de fibra óptica de 1GBps, todas las dependencias y herramientas se descargan e instalan en menos de 5 minutos, sin un consumo significativo de CPU, Memoria o descarga de datos.

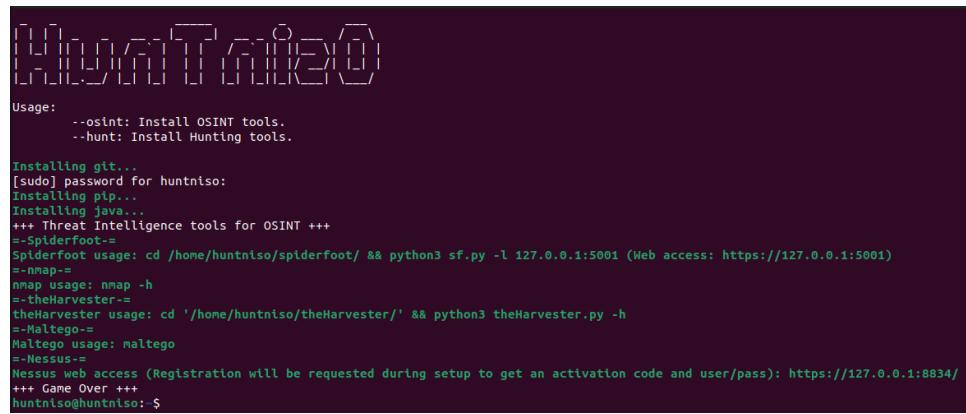


```
[...]
Usage: --osint: Install OSINT tools.
--hunt: Install Hunting tools.

Installing git...
Installing pip...
Installing java...
+++ Threat Intelligence tools for OSINT ===
--SpiderFoot=
SpiderFoot usage: cd /home/huntniso/spiderFoot/ && python3 sf.py -l 127.0.0.1:5001 (Web access: https://127.0.0.1:5001)
--nmap=
nmap usage: nmap -h
--theHarvester=
theHarvester usage: cd '/home/huntniso/theHarvester/' && python3 theHarvester.py -h
--Metago=
Metago usage: metago
--Nessus=
Nessus web access (Registration will be requested during setup to get an activation code and user/pass): https://127.0.0.1:8834/
+++ Threat Hunting tools ===
--RITA=
RITA usage: rita -h
--APT-Hunter=
APT-Hunter usage: python3 /home/huntniso/APT-Hunter/APT-Hunter.py -h
--DNSTwist=
DNSTwist usage: python3 /home/huntniso/dnstwist/dnstwist.py -h
+++ Game Over ===
Command being timed: "./huntniso.sh --osint --hunt"
User time (seconds): 56.23
System time (seconds): 9.88
Percent of CPU this job got: 23%
Elapsed (wall clock) time (hh:mm:ss or m:ss): 4:41.70
Average shared text size (kbytes): 0
Average unshared data size (kbytes): 0
Average stack size (kbytes): 0
Average total size (kbytes): 0
Maximum resident set size (kbytes): 150424
Average resident set size (kbytes): 0
Major (requiring I/O) page faults: 508
Minor (reclaiming a frame) page faults: 427823
Voluntary context switches: 33877
Involuntary context switches: 13594
Swaps: 0
File system inputs: 100648
File system outputs: 1882616
Socket messages sent: 0
Socket messages received: 0
Signals delivered: 0
Page size (bytes): 4096
Exit status: 0
huntniso@huntniso:~$
```

Figura 6.1: Captura de pantalla de estadísticas de ejecución del Script HunTnisO.

La ejecución del Script utilizando el parámetro “–osint” únicamente instalará las dependencias y herramientas Spiderfoot, nmap, theHarvester y Nessus, como se observa en la Figura 6.2.



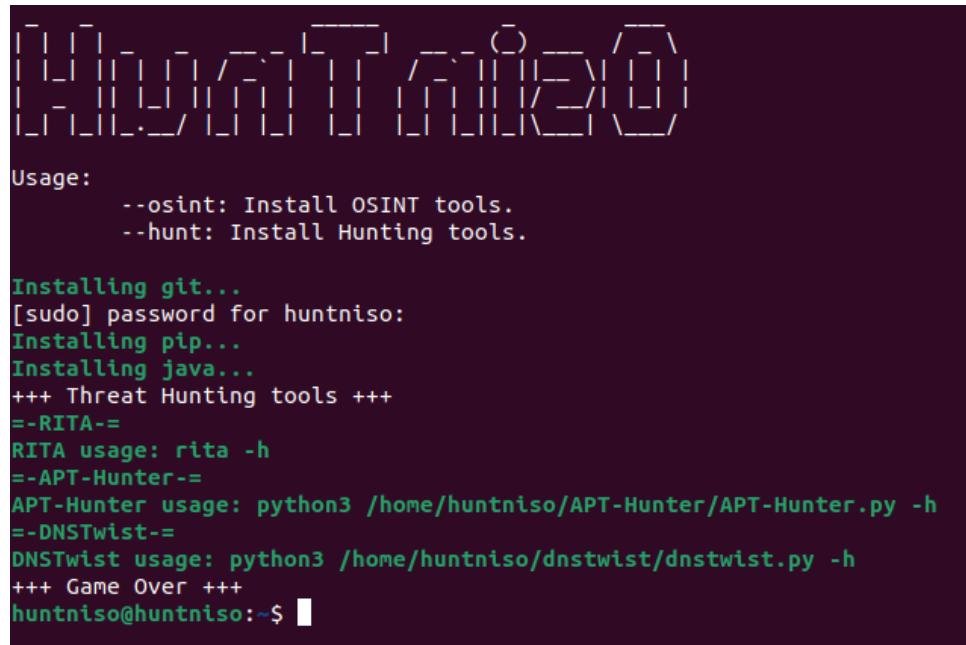
```
HunTnisO()

Usage:  --osint: Install OSINT tools.
        --hunt: Install Hunting tools.

Installing git...
[sudo] password for huntniso:
Installing pip...
Installing java...
+++ Threat Intelligence tools for OSINT ===
--SpiderFoot--
SpiderFoot usage: cd /home/huntniso/SpiderFoot/ && python3 sf.py -l 127.0.0.1:5001 (Web access: https://127.0.0.1:5001)
--nmap--
nmap usage: nmap -h
--theHarvester--
theHarvester usage: cd '/home/huntniso/theHarvester/' && python3 theHarvester.py -h
--Maltego--
Maltego usage: maltego
--Nessus--
Nessus web access (Registration will be requested during setup to get an activation code and user/pass): https://127.0.0.1:8834/
+++ Game Over ===
huntniso@huntniso:~$
```

Figura 6.2: Captura de pantalla de ejecución del Script HunTnisO con parámetro “–osint”.

La ejecución del Script utilizando el parámetro “–hunt” únicamente instalará las dependencias y herramientas RITA, APT-Hunter y DNSTwist, como se observa en la Figura 6.3.



```
HunTnisO()

Usage:  --osint: Install OSINT tools.
        --hunt: Install Hunting tools.

Installing git...
[sudo] password for huntniso:
Installing pip...
Installing java...
+++ Threat Hunting tools ===
--RITA--
RITA usage: rita -h
--APT-Hunter--
APT-Hunter usage: python3 /home/huntniso/APT-Hunter/APT-Hunter.py -h
--DNSTwist--
DNSTwist usage: python3 /home/huntniso/dnstwist/dnstwist.py -h
+++ Game Over ===
huntniso@huntniso:~$
```

Figura 6.3: Captura de pantalla de ejecución del Script HunTnisO con parámetro “–hunt”.

Teniendo en cuenta que la versión del sistema operativo Ubuntu 22.04

LTS se encuentra en etapa Beta se ha verificado, como se observa en la Figura 6.4, que la instalación funciona correctamente.

```
Usage:
  --osint: Install OSINT tools.
  --hunt: Install Hunting tools.

Installing git...
[sudo] password for huntniso:
Installing pip...
Installing java...
+++ Threat Intelligence tools for OSINT ===
--Spiderfoot=
Spiderfoot usage: cd /home/huntniso/spiderfoot/ && python3 sf.py -l 127.0.0.1:5001 (Web access: https://127.0.0.1:5001)
--nmap=
nmap usage: nmap -h
--theHarvester=
theHarvester usage: cd '/home/huntniso/theHarvester/' && python3 theHarvester.py -h
--Maltego=
Maltego usage: maltego
--Nessus=
Nessus web access (Registration will be requested during setup to get an activation code and user/pass): https://127.0.0.1:8834/
+++ Threat Hunting tools ===
--RITA=
RITA usage: rita -h
--APT-Hunter=
APT-Hunter usage: python3 /home/huntniso/APT-Hunter/APT-Hunter.py -h
--DNSTwist=
dnstwist usage: python3 /home/huntniso/dnstwist/dnstwist.py -h
+++ Game Over ===
huntniso@huntniso:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04 (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
```

Figura 6.4: Captura de pantalla de ejecución de HunTnisO en Ubuntu 22.04 LTS.

Debido a que el Sistema Operativo Kali es muy utilizado en estas prácticas, se verificó que el Script se ejecuta satisfactoriamente en la versión 2022.01, como se observa en la Figura 6.5.

Figura 6.5: Captura de pantalla de ejecución del Script HunTnisO en Kali 2022.01.

Finalmente, el Script realiza múltiples verificaciones para detectar si las dependencias y las herramientas ya se encuentran preinstaladas para evitar sobrescribir las mismas, como se observa en la Figura 6.6.

```
[██████████] [██████████] [██████████] [██████████] [██████████] [██████████]
[██████████] [██████████] [██████████] [██████████] [██████████] [██████████]
[██████████] [██████████] [██████████] [██████████] [██████████] [██████████]
[██████████] [██████████] [██████████] [██████████] [██████████] [██████████]

Usage:
    --osint: Install OSINT tools.
    --hunt: Install Hunting tools.

    +++ Threat Intelligence tools for OSINT +++
--Spiderfoot--
Directory 'spiderfoot/' already exists, skipping...
--nmap--
nmap already installed, skipping...
--theHarvester--
Directory 'theHarvester/' already exists, skipping...
--Maltego--
Maltego already installed, skipping...
--Nessus--
Nessus is already installed, skipping...
    +++ Threat Hunting tools +++
--RITA--
RITA already installed, skipping...
--APT-Hunter--
Directory 'APT-Hunter/' already exists, skipping...
--DNSTwist--
Directory 'dnstwist/' already exists, skipping...
    +++ Game Over +++
huntniso@huntniso:~$
```

Figura 6.6: Captura de pantalla de ejecución del Script HunTnisO en un Sistema Ubuntu con todas las dependencias y herramientas ya instaladas.

Capítulo 7

Conclusiones

Se ha presentado en este trabajo una introducción teórica de los conceptos básicos de ciberseguridad defensiva y ofensiva que permiten comprender la problemática actual que afrontan organizaciones grandes con una madurez en ciberseguridad media o alta, cuyas capacidades les permiten introducirse en las prácticas de Ciberinteligencia y Threat Hunting de un modo que va más allá de la recolección, bloqueo y detección de Indicadores de Compromiso reconocidos. Resulta relevante destacar que el problema no es único de este tipo de organización, a pesar de que es donde más claramente se presenta, ni tampoco es el único problema ni necesariamente el más importante que afrontan, ya que eso siempre estará asociado a las características y ámbito de la organización. La selección del sector y organismo para la prueba de concepto ha tenido un amplio desarrollo en este trabajo, que incluye múltiples fuentes asociadas a empresas de ciberseguridad, con el fin de situar al lector con una explicación clara de en qué contexto el organismo seleccionado existe.

El trabajo ha concentrado gran parte de los esfuerzos en relevar y probar las soluciones existentes para seleccionar aquellas que cumplían los requisitos predefinidos para resolver la problemática observada. Se han revisado múltiples fuentes bibliográficas para determinar el mejor modelo posible para el despliegue de las soluciones elegidas. Se ha desarrollado un Script que facilita el despliegue de soluciones con doble finalidad:

1. En términos de Ciberinteligencia, ayuda a un analista a identificar en base a fuentes OSINT el nivel de exposición de información de la organización de la que forma parte y de sus miembros.
2. En términos de Threat Hunting, asistan al analista en las investigaciones y Hunts no estructurados, con técnicas estadísticas de la metodología basada en datos.

La selección de herramientas ha tenido en cuenta múltiples factores, pero

mantener un bajo número para simplificar la decisión y tarea de los analistas fue el parámetro principal que guió la construcción de la solución. Esto conlleva que a la solución puedan estar faltandole herramientas que ciertas organizaciones considerarian importantes, pero desarrollar una herramienta que tenga en cuenta todas las posibles variedades de cada organización o sector sería inabarcable, por lo que sería recomendable que las organizaciones adapten el Script a sus necesidades o bien instalen otras herramientas adicionales cuando lo consideren conveniente.

Bibliografía

- [1] D. R.-J. G.-J. Rydning *et al.*, “The digitization of the world from edge to core,” *Framingham: International Data Corporation*, vol. 16, 2018, <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>.
- [2] J. H. Anna Zeiter, Scott Snyder, “Articulating value from data,” https://www3.weforum.org/docs/WEF_Articulating_Value_from_Data_2021.pdf, Tech. Rep., 2021.
- [3] “Iso/iec 27001:2013,” <https://www.iso.org/standard/54534.html>, Tech. Rep., 2013.
- [4] D. McCandless, T. Evans, M. Quick, E. Hollowood, C. Miles, and D. Hampson, “World’s biggest data breaches & hacks—information is beautiful,” <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>, Tech. Rep.
- [5] “2022 global threat report,” <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf>, Tech. Rep., 2022.
- [6] “Security outcomes study volume 2,” <https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-study-vol-2-report.pdf?ccid=cc000160&oid=rptsc027923&dtdid=odicdc001478>, Tech. Rep., 2021.
- [7] “2020: Q2 threat report,” <https://www.rapid7.com/research/report/2020Q2-threat-report/>, Tech. Rep., 2020.
- [8] A. Breakspear, *A new definition of intelligence*. Taylor & Francis, 2013, vol. 28, no. 5.
- [9] R. McMillan, “Definition: Threat intelligence,” <https://www.gartner.com/en/documents/2487216>, Tech. Rep., 2013.
- [10] K. Nickels, “The cycle of cyber threat intelligence,” <https://www.youtube.com/watch?v=J7e74QLVxCk>, Tech. Rep., 2019.

- [11] C. N. de Inteligencia, “El ciclo de inteligencia,” <https://www.cni.es/la-inteligencia>.
- [12] C. I. Agency, “How intelligence works,” <https://www.intelligencecareers.gov/icintelligence.html>.
- [13] “Exploring the opportunities and limitations of current threat intelligence platforms,” <https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms>, Tech. Rep., 2017.
- [14] “Cyber threat intelligence maturity assessment tool,” <https://www.crest-approved.org/2022/02/18/cyber-threat-intelligence-maturity-assessment-tool/index.html>, Tech. Rep., 2018.
- [15] “Maturing a threat intelligence program,” <https://www.crest-approved.org/2022/02/18/cyber-threat-intelligence-maturity-assessment-tool/index.html>, Tech. Rep., 2017.
- [16] C. D. Mark Luchs, “Measuring your cyber threat intelligence maturity,” <https://www.ctim.eu/static/downloads/pdf/ctim-whitepaper.pdf>, Tech. Rep.
- [17] C. Press, “The intelligence handbook,” <https://go.recordedfuture.com/hubfs/ebooks/intelligence-handbook-fourth-edition.pdf>, Tech. Rep., 2022.
- [18] P. S. Rebekah Brown, “Sans 2022 cyber threat intelligence survey,” <https://www.sans.org/white-papers/sans-2022-cyber-threat-intelligence-survey/>, Tech. Rep., 2022.
- [19] R. Bejtlich, “Become a hunter,” 2011, http://docs.media.bitpipe.com/24x/24618/item_370437/informationsecurity_july_aug2011_final.pdf.
- [20] M. Bromiley, “Sans 2022 att&ck and d3fend report: Incorporating frameworks into your analysis and intelligence,” <https://www.sans.org/white-papers/sans-2022-att-ck-and-d3fend-report-incorporating-frameworks-into-your-analysis-and-intelligence/>, Tech. Rep., 2022.
- [21] MITRE, “Adversary emulation plans,” <https://attack.mitre.org/resources/adversary-emulation-plans/>.
- [22] ——, “Cyber analytics repository,” <https://car.mitre.org/>.
- [23] ——, “Att&ck navigator,” <https://mitre-attack.github.io/attack-navigator/>.

- [24] R. Rodriguez, “Threat hunter playbook,” <https://threathunterplaybook.com/introduction.html>.
- [25] “Threathuntingproject/threathunting,” <https://github.com/ThreatHuntingProject/ThreatHunting/tree/master/hunts>.
- [26] Sqrrl, “Hunt evil: Your practical guide to threat hunting,” <https://www.threathunting.net/files/hunt-evil-practical-guide-threat-hunting.pdf>.
- [27] ——, “Huntpedia,” <https://www.threathunting.net/files/huntpedia.pdf>.
- [28] d. V. Rob van Os, “Tahiti,” <https://www.betaalvereniging.nl/wp-content/uploads/TaHiTI-Threat-Hunting-Methodology-whitepaper.pdf>.
- [29] Sqrrl, “The hunting loop,” <https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf>.
- [30] D. Gunter and M. Seitz, “A practical model for conducting cyber threat hunting,” *SANS*, 2019.
- [31] D. Bianco, “The hunting maturity model,” <http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html>.
- [32] J. L. Mathias Fuchs, “The hunting maturity model,” <https://www.sans.org/white-papers/sans-2021-survey-threat-hunting-uncertain-times/>.
- [33] D. of Defense (USA), “Cybersecurity maturity model certification,” <https://www.acq.osd.mil/cmmc/>.
- [34] J. de Estado (España), “Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial,” <https://www.boe.es/buscar/pdf/2015/BOE-A-2015-4607-consolidado.pdf>.
- [35] O. para la Cooperación y el Desarrollo Económicos, “Enterprises by business size,” <https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm>.
- [36] V. C. Black, “Global incident response threat report,” <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-the-ominous-rise-of-island-hopping-and-counter-incident-response-continues.pdf>.
- [37] D. Temple-Raston, “A ‘worst nightmare’ cyberattack: The untold story of the solarwinds hack,” *National Public Radio*, 2021.

- [38] Xataka, “Malwarebytes, la popular empresa de ciberseguridad, dice haber sido hackeada por los mismos que atacaron solarwinds,” <https://www.xataka.com/seguridad/malwarebytes-popular-empresa-ciberseguridad-dice-haber-sido-hackeada-mismos-que-atacaron-solarwinds>.
- [39] B. UK, “Kaspersky lab cybersecurity firm is hacked,” <https://www.bbc.co.uk/news/technology-33083050>.
- [40] BleepingComputer, “Lastpass users warned their master passwords are compromised,” <https://www.bleepingcomputer.com/news/security/lastpass-users-warned-their-master-passwords-are-compromised/>.
- [41] Knowbe4, “Av firm bitdefender hacked; did not encrypt customer passwords,” <https://blog.knowbe4.com/av-firm-bitdefender-hacked-did-not-encrypt-customer-passwords>.
- [42] DataBreaches, “Sophos acquisition cyberoam victim of cyber attack,” <https://www.databreaches.net/sophos-acquisition-cyberoam-victim-of-cyber-attack/>.
- [43] D. E. Sanger and N. Perlroth, “Fireeye, a top cybersecurity firm, says it was hacked by a nation-state,” *The New York Times*, vol. 8, 2020.
- [44] BleepingComputer, “Lapsus\$ hackers leak 37gb of microsoft’s alleged source code,” <https://www.bleepingcomputer.com/news/microsoft/lapsus-hackers-leak-37gb-of-microsofts-alleged-source-code/>.
- [45] Reuters, “Hackers hit authentication firm okta, customers ‘may have been impacted’,” <https://www.reuters.com/technology/authentication-services-firm-okta-says-it-is-investigating-report-breach-2022-03-22/>.
- [46] MSSPAlert, “Justice department: Chinese hackers hits msps,” <https://www.msspalert.com/cybersecurity-breaches-and-attacks/chinese-hackers-hit-msps-ibm-hpe/>.
- [47] CISA, “Apts targeting it service provider customers,” <https://www.cisa.gov/uscert/APTs-Targeting-IT-Service-Provider-Customers>.
- [48] S. S. (USA), “Information only alert - gioc reference #20-032-1,” <https://www.documentcloud.org/documents/6980788-US-Secret-Service-PIN-on-MSP-attacks.html>.
- [49] Github, “Awesome threat intelligence,” <https://github.com/hslatman/awesome-threat-intelligence>.
- [50] S. Prime, “Information only alert - gioc reference #20-032-1,” <https://uncoder.io/>.

- [51] ——, “Information only alert - gioc reference #20-032-1,” <https://cti.uncoder.io/>.
- [52] A. Countermeasures, “Information only alert - gioc reference #20-032-1,” <https://github.com/activecm/rita>.
- [53] “Edtech market - global outlook & forecast 2022-2027,” https://www.reportlinker.com/p06221889/EdTech-Market-Global-Outlook-Forecast.html?utm_source=GNW, Tech. Rep., 2022.
- [54] “Cyber security report 2021,” <https://www.checkpoint.com/pages/cyber-security-report-2021/>, Tech. Rep., 2021.
- [55] “The state of encrypted attacks,” <https://www.zscaler.com/resources/industry-reports/state-of-encrypted-attacks-2021.pdf>, Tech. Rep., 2021.
- [56] “Trellix advanced threat research reports,” <https://www.trellix.com/en-us/threat-center/threat-reports.html>, Tech. Rep., 2022.
- [57] “Global threat landscape report,” <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-q1-2022-threat-landscape.pdf>, Tech. Rep., 2022.
- [58] “Sophos 2021 threat report: Navigating cybersecurity in an uncertain world,” <https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf>, Tech. Rep., 2021.
- [59] “Ransomware attacks are on the rise. these are the industries most a risk.” <https://www.weforum.org/agenda/2021/11/industries-affected-ransomware-cybersecurity-cybercrime>, Tech. Rep., 2021.
- [60] “Tenable’s 2021 threat landscape retrospective,” https://static.tenable.com/marketing/research-reports/Research-Report-2021_Threat_Landscape_Retrospective.pdf, Tech. Rep., 2021.
- [61] “Sans 2021 report: Top new attacks and threat report,” <https://www.sans.org/blog/sans-2021-threat-report/>, Tech. Rep., 2021.
- [62] “Cost of a data breach report,” <https://www.ibm.com/downloads/cas/OJDVQGRY>, Tech. Rep., 2021.
- [63] “2022 state of the phish,” <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2022.pdf>, Tech. Rep., 2022.
- [64] “Cyber threats to the education industry,” <https://www.fireeye.com/current-threats/reports-by-industry/education-threat-intelligence.html>, Tech. Rep., 2016.

- [65] “Recent attacks against supercomputers,” <https://www.cadosecurity.com/recent-attacks-against-supercomputers/>, Tech. Rep., 2020.
- [66] “Working remote: How universities secure open networks,” <https://www.cybereason.com/blog/the-higher-ed-security-challenge>, Tech. Rep., 2019.
- [67] “Microsoft digital defense report,” <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi>, Tech. Rep., 2021.
- [68] “2021 application protection report: Of ransom and redemption,” <https://www.f5.com/labs/articles/threat-intelligence/2021-application-protection-report-of-ransom-and-redemption>, Tech. Rep., 2021.
- [69] “Enisa threat landscape 2021,” <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>, Tech. Rep., 2021.
- [70] “Top 20 countries found to have the most cybercrime,” <https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>, Tech. Rep.
- [71] “Which eu country is most vulnerable to cybercrime?” <https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/>, Tech. Rep., 2018.
- [72] “2022 unit 42 ransomware threat report,” <https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html>, Tech. Rep., 2022.
- [73] “España, en el punto de mira,” <https://www.youtube.com/watch?v=nRY3QapA6Hg>, Tech. Rep., 2021.
- [74] “Threat report t3 2021,” https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf, Tech. Rep., 2021.
- [75] “Estadística de estudiantes universitarios (eeu),” <https://www.universidades.gob.es/stfls/universidades/Estadisticas/ficheros/PpalesResulEEU.pdf>, Tech. Rep., 2021.
- [76] “España se mantiene como el tercer país que más universitarios erasmus envía al exterior y el que más recibe en la ue,” <https://www.europapress.es/sociedad/educacion-00468/noticia-espana-mantiene-tercer-pais-mas-universitarios-erasmus-envia-exterior-mas-recibe-ue-20190124113944.html>, Tech. Rep., 2019.

- [77] “Las ciberamenazas ponen en alerta a las universidades,” <https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/ciberamenazas-alertan-universidades.html>, Tech. Rep., 2018.
- [78] “La universidad de oviedo, afectada por un ciberataque procedente de rusia,” <https://www.lavozdeasturias.es/noticia/asturias/2022/02/26/universidad-oviedo-afectada-ciberataque-procedente-rusia/00031645877244831842414.htm>, Tech. Rep., 2022.
- [79] “El ciberataque a la uab afectará hasta finales de año: la difícil gestión de una universidad sin acceso a su sistema informático durante meses,” <https://www.xataka.com/seguridad/ciberataque-a-uab-afectara-finales-ano-dificil-gestion-universidad-acceso-a-su-sistema-informatico-durante-meses>, Tech. Rep., 2021.
- [80] “La uoc sufre un ransomware que afecta a su campus virtual: así es el último ciberataque que golpea a una universidad española,” <https://www.xataka.com/seguridad/uoc-sufre-ransomware-que-afecta-a-su-campus-virtual-asi-ultimo-ciberataque-que-golpea-a-universidad-espanola>, Tech. Rep., 2022.
- [81] “La universidad de castilla-la mancha sufre un ataque informático similar al del servicio público de empleo estatal,” <https://periodicoclm.publico.es/2021/04/19/universidad-castilla-la-mancha-afectada-ataque-informatico-similar-sufrido-sepe/>, Tech. Rep., 2021.
- [82] S. Ranking, “2021 academic ranking of world universities,” <https://www.shanghairanking.com/rankings/arwu/2021>.
- [83] U. de Granada, “Granada y la universidad,” <https://www.ugr.es/universidad/organizacion/granada-y-la-universidad>.
- [84] ——, “Universidad de granada: Presupuesto ejercicio 2022,” https://gerencia.ugr.es/pages/vger_eco/presupuestos/presupuesto2022/#page=110.
- [85] ——, “Csirc-seguridad informática,” <https://csirc.ugr.es/informacion/directorio-personal/entidades/csirc-seguridad-informatica>.
- [86] ——, “Network engineering & security group,” <https://nesg.ugr.es/>.
- [87] N. E. . S. Group, “Information leakage detection in the deep web,” <https://nesg.ugr.es/index.php/en/projects-contracts-2?view=project&task=show&id=26>.

- [88] J. de Andalucía, “Andalucía cert,” <https://www.juntadeandalucia.es/organismos/presidenciaadministracionpublicaeinterior/areas/tecnologias-informacion/seguridadyconfianzadigital/paginas/andaluciacer-jda.html>.
- [89] R. IRIS, “Iris cert,” <https://www.rediris.es/cert/>.
- [90] INCIBE, “Incibe cert,” <https://www.incibe-cert.es/>.
- [91] I. CERT, “Iga,” <https://www.incibe-cert.es/servicios-operadores/information-gathering>.
- [92] M. del Interior (España), “Cnpic,” <https://cetse.ses.mir.es/publico/cetse>.
- [93] J. de Estado (España), “Real decreto 704/2011, de 20 de mayo, por el que se aprueba el reglamento de protección de las infraestructuras críticas.” <https://www.boe.es/buscar/doc.php?id=BOE-A-2011-8849>.
- [94] CCN-CERT, “Carmen,” <https://www.ccn-cert.cni.es/soluciones-seguridad/carmen.html>.
- [95] ——, “Reyes,” <https://www.ccn-cert.cni.es/soluciones-seguridad/reyes.html>.
- [96] ——, “Centro criptológico nacional: Informe anual. retos 2021,” <https://www.ccn-cert.cni.es/pdf/documentos-publicos/xiv-jornadas-stic-ccn-cert/ponencias-1/5641-s19-d30-01-informe-anual-retos-2021/file.html>, 2021.
- [97] ——, “Elena,” <https://www.ccn-cert.cni.es/soluciones-seguridad/elena.html>.
- [98] INCIBE, “Quién es quién en el sector de la seguridad tic en España,” <https://www.incibe.es/extfrontinteco/img/File/intecocert/Actualidad/Notas/quienseguridadtic.pdf>.
- [99] “La universidad de granada sufre un ‘ataque organizado’ en sus sistemas informáticos que afecta a la realización de exámenes online,” https://www.granadahoy.com/granada/Universidad-Granada-ataque-informatico-examenes-online_0.1541846028.html, Tech. Rep., 2021.
- [100] “Osintframework,” <https://osintframework.com/>.
- [101] “Osinttechniques,” <https://www.osinttechniques.com/osint-tools.html>.
- [102] “Awesome-osint,” <https://github.com/jivoi/awesome-osint>.

- [103] “Ciberpatrulla,” <https://ciberpatrulla.com/links/>.
- [104] “Cipher387,” https://cipher387.github.io/osint_stuff_tool_collection/.
- [105] “Hatless1der,” <https://start.me/p/DPYPMz/the-ultimate-osint-collection>.
- [106] M. Bazzell, *Open Source Intelligence Techniques*. inteltechniques.com, 2022.
- [107] P. Kim and J. Faircloth, “The hacker playbook 3,” *Secure Planet LLC*, 2018.
- [108] 0x4D31, “Awesome threat detection,” <https://github.com/0x4D31/awesome-threat-detection>.
- [109] V. Palacin, *Practical Threat Intelligence and Data-Driven Threat Hunting*. Packt Publishing, 2021.
- [110] T. of Bits, “Tracking a stolen code-signing certificate with osquery,” <https://blog.trailofbits.com/2017/10/10/tracking-a-stolen-code-signing-certificate-with-osquery/>.
- [111] R. Canary, “Tracking driver inventory to unearth rootkits,” <https://redcanary.com/blog/tracking-driver-inventory-to-expose-rootkits/>.
- [112] ——, “Threat hunting for psexec, open-source clones, and other lateral movement tools,” <https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/>.
- [113] ——, “Hunting for getsystem in offensive security tools,” <https://redcanary.com/blog/getsystem-offsec/>.
- [114] “Lolbas,” <https://lolbas-project.github.io/>.
- [115] “Gtfobins,” <https://gtfobins.github.io/>.
- [116] Anomali, “Rise of legitimate services for backdoor command and control,” <https://www.anomali.com/resources/anomali-labs-report/rise-of-legitimate-services-for-backdoor-command-and-control>.
- [117] SANS, “Tracking newly registered domains,” <https://isc.sans.edu/diary/Tracking+Newly+Registered+Domains/23127>.
- [118] ——, “Proactive malicious domain search,” <https://isc.sans.edu/forums/diary/Proactive+Malicious+Domain+Search/23065/>.
- [119] R. Canary, “Using entropy in threat hunting: a mathematical search for the unknown,” <https://redcanary.com/blog/threat-hunting-entropy/>.

- [120] SANS, “Freq.py to detect randomness using nlp techniques,” <https://github.com/sans-blue-team/freq.py>.
- [121] Salesforce, “Ja3,” <https://github.com/salesforce/ja3>.
- [122] ———, “Jarm,” <https://github.com/salesforce/jarm>.
- [123] olafhartong, “Threathunting,” <https://github.com/olafhartong/ThreatHunting>.
- [124] A. Taylor, “Flare,” <https://github.com/austin-taylor/flare>.
- [125] Ubuntu, “Ubuntu installation manual,” <https://ubuntu.com/tutorials/install-ubuntu-desktop#1-overview>.
- [126] F. Olander, “Huntniso repository,” <https://github.com/FOlander/huntniso.git>.

Glosario

- Amazon Web Services (AWS): Empresa estadounidense subsidiaria de Amazon focalizada en computación en la nube (*Cloud Computing*).
- API Key: acrónimo del inglés, *application programming interface key*. Es una clave utilizada para identificar y autenticar una aplicación o un usuario. En general, cuando se identifica a un usuario se lo denomina “Token”.
- APT: por sus siglas en inglés, *Advanced Persistent Threat*. Una amenaza persistente avanzada es un actor que suele caracterizarse por sus intenciones maliciosas, sus métodos sigilosos, sus capacidades y habilidades, su motivación, organización y financiamiento. Diferentes denominaciones y numeraciones existen, ejemplos de ello pueden observarse en MITRE Groups y Mandiant APT Groups.
- Bash: por sus siglas en inglés, *Born-Again Shell*. Es una interfaz de usuario de línea de comandos, así como un lenguaje de scripting para sistemas basados en Unix.
- Beta: Proviene de la segunda letra del alfabeto Griego y en términos informáticos representa la primera versión completa de un Software que si bien podría presentar inestabilidades que deben aún ser corregidas, es considerada como una versión preliminar para uso general.
- C&C: por sus siglas en inglés, *Command & Control* (también abreviados “C2”). Refiere al origen desde el cual se controlan equipos remotamente, usualmente para control masivo de una red de bots (*Botnet*).
- Cado Security: empresa inglesa de ciberseguridad focalizada en la nube.
- Certificate Transparency (CT): Estándar abierto utilizado para la monitorización y auditado de certificados digitales emitidos por autoridades certificadoras.
- Check Point: Empresa israelí de ciberseguridad focalizada en la seguridad de las comunicaciones.

- CIA: por sus siglas en inglés, *Central Intelligence Agency*. Agencia de inteligencia estadounidense.
- CISA: por sus siglas en Inglés, *Cybersecurity and Infrastructure Security Agency*. Es una agencia federal de los Estados Unidos.
- Cisco: Empresa estadounidense de tecnología focalizada en las comunicaciones.
- CNI: por sus siglas en español, Centro Nacional de Inteligencia. Es la agencia de inteligencia española.
- CREST: Empresa inglesa de ciberseguridad focalizada en la educación.
- Crowdstrike: Empresa estadounidense de ciberseguridad focalizada en la seguridad de sistemas.
- CSIRT: por sus siglas en inglés, *Computer Security Incident Response Team* o *Cyber Security Incident Response Team*. Se refiere al equipo de respuesta a incidentes de seguridad informática.
- Cybereason: Empresa estadounidense de ciberseguridad focalizada en la seguridad de sistemas.
- Cybersquatting: Consiste en registrar nombres de dominio que simulan a uno legítimo, por ejemplo registrando los dominios “ugr.edu” o “vgr.es” para imitar a “ugr.es”.
- Data Science: Campo interdisciplinario que utiliza múltiples métodos (científicos, procesos, algoritmos y sistemas) para la colección, análisis y extracción de conocimientos a partir de grandes volúmenes de datos. Se denomina *Big Data* a las colecciones de datos considerados demasiado grandes o complejos (Originalmente asociado al concepto de las tres “V”: volumen, variedad y velocidad) para ser tratados por los métodos tradicionales de procesamiento de datos. Se denomina análisis de datos (*Data Analysis* o *Data Analytics*) a las técnicas utilizadas para inspeccionar y modelar los datos. Se denomina minería de datos (*Data Mining*) al proceso de descubrimiento de patrones y extracción de conocimiento a partir de los datos.
- DDNS: por sus siglas en inglés, *Dynamic DNS*. Método para actualizar la asociación entre nombre de dominio e IP automáticamente en un sistema de nombres de dominio (DNS).
- DDOS: por sus siglas en inglés, *Distributed Denial-of-service*. Es un ataque distribuido de denegación de servicio a sistemas informáticos que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

- Deloitte: empresa Inglesa de servicios profesionales que provee servicios en torno a consultoría, impuestos, asesoría jurídica, asesoría financiera y auditoría.
- DFIR: por sus siglas en inglés, *Digital Forensics and Incident Response*. Refiere a las practicas relacionadas al análisis forense digital y de respuesta a incidentes de seguridad.
- DGA: por sus siglas en inglés, *Domain Generation Algorithms*. Algoritmos que generan automáticamente nombres de dominio, usualmente utilizado por múltiples familias de malware.
- DIKW: por sus siglas en inglés, *Data, Information, Knowledge, Wisdom*, que se traduce como Datos, Información, Conocimiento, Sabiduría.
- Dirección IP: etiqueta numérica que identifica de manera lógica a una interfaz de red en un dispositivo que utiliza el protocolo de internet (IP).
- DLP: por sus siglas en inglés, *Data Loss Prevention* o *Data Leak Prevention*. Sistema que se encarga de controlar la información a fin de prevenir o controlar que datos están siendo enviados a lugares indeeados.
- DNS: por sus siglas en inglés, *Domain Name System*. Sistema de nombres jerárquico y descentralizado utilizado para identificar sistemas en redes.
- EC-Council: Empresa estadounidense de ciberseguridad focalizada en la educación.
- EDR: por sus siglas en inglés, *Endpoint Detection Response*. Sistema de detección de amenazas de seguridad con capacidad de mitigarlos. Son considerados una evolución del sistema antivirus tradicional.
- Elastic Stack: SIEM que combina una serie de soluciones con 3 proyectos Open Source conocidos como Elasticsearch, Logstash y Kibana.
- EOL: por sus siglas en inglés, *End of life*. Es una etiqueta utilizada para describir un producto que ha llegado al final de su vida útil.
- ENISA: por sus siglas en inglés, *European Network and Information Security Agency*. Agencia de la Unión Europea con el objetivo de mejorar las redes y la seguridad de la información.
- ESET: Empresa eslovaca de ciberseguridad focalizada en la seguridad de sistemas.

- F5: Empresa estadounidense de ciberseguridad focalizada en la seguridad de aplicaciones.
- Firewall: Sistema de seguridad que supervisa las comunicaciones de red entrantes y salientes en base a reglas predefinidas.
- Fortinet: Empresa estadounidense de ciberseguridad focalizada en la seguridad de sistemas y comunicaciones.
- Gartner: empresa estadounidense que provee servicios de consultoría e investigaciones de tecnologías de la información.
- GIAC: Empresa estadounidense de ciberseguridad focalizada en la educación, provee servicios profesionales de certificación para la empresa SANS.
- Github: Empresa estadounidense subsidiaria de Microsoft que provee servicios de alojamiento de código con control de versiones para desarrolladores.
- HPE: Empresa estadounidense de tecnología enparentada con “HP”.
- I2P: acrónimo del Inglés, *Invisible Internet Project*. Referencia tanto al proyecto que lo desarrolla como a la red misma (superpuesta sobre Internet), cuyo objetivo principal es la comunicaciones distribuida ocultando la dirección IP origen (anonimato a nivel de red) manteniendo la integridad y la confidencialidad de la información.
- IBM: Empresa estadounidense de tecnología.
- IoA: por sus siglas en inglés, *Indicator of Attack*. Similar a TTP pero mas amplio. A diferencia del IoC que se centra en artefactos, este se focaliza en detectar comportamiento o intención de un atacante.
- IoC: por sus siglas en inglés *Indicator of Compromise*. Es un artefacto observado en una red o en un sistema que indica una intrusión informática. Ejemplos de ello son Dominios, Direcciones IPs y Hash's.
- IP: por sus siglas en inglés, *Internet Protocol*. Es un protocolo de comunicación digital.
- IPS: por sus siglas en inglés, *Intrusion Prevention System*. Sistema que controla las comunicaciones de red para proteger a otros sistemas de ataques y abusos mediante la inspección de paquetes.
- ISO/IEC: por sus siglas en Inglés, *International Organization for Standardization / International Electrotechnical Commission*. Comité conjunto entre las organizaciones ISO e IEC para el desarrollo de estándares en el área de tecnología eléctrica y electrónica.

- JA3: Método desarrollado por Salesforce para calcular fingerprints de manera pasiva en sistemas utilizando SSL/TLS.
- JARM: Método desarrollado por Salesforce para calcular fingerprints de manera activa en sistemas utilizando SSL/TLS.
- Kaspersky: Empresa rusa de ciberseguridad.
- LastPass: Empresa estadounidense de ciberseguridad focalizada en almacenamiento seguro de contraseñas.
- Linux: Familia de sistemas operativos de código abierto proveniente de Unix.
- Lockheed Martin: empresa estadounidense de la industria aeroespacial y militar.
- Log4Shell: Vulnerabilidad de día 0 en un componente de Java que generaba una condición de ejecución de código remoto (RCE, por sus siglas del inglés *Remote Code Execution*).
- Mandiant: Empresa estadounidense de ciberseguridad, también conocida como FireEye.
- Malware: acrónimo del inglés, *Malicious Software*. Refiere a software intencionalmente diseñado para causar un comportamiento inesperado.
- Malwarebytes: Empresa rumana de ciberseguridad.
- Microsoft: Empresa estadounidense de tecnología focalizada en el desarrollo de software y computación en la nube.
- MITRE: Organización estadounidense sin fines de lucro que administra centros de investigación y desarrollo financiados con fondos federales para respaldar múltiples agencias gubernamentales.
- OCDE: por sus siglas en español, Organización para la Cooperación y el Desarrollo Económicos. Organismo Internacional de carácter intergubernamental fundado para estimular el progreso económico y el comercio mundial.
- Palo Alto Networks: Empresa estadounidense de ciberseguridad focalizada en la seguridad de las comunicaciones.
- Phishing: Ataque informático de ingeniería social utilizado para engañar a una víctima.

- Ping: herramienta para comprobar la accesibilidad a un sistema en una red IP mediante envío y respuesta de paquetes del Protocolo de Mensajes de Control de Internet (ICMP).
- Pipe: Concepto proveniente de sistemas Unix. Es un método de comunicación entre procesos con funcionamiento de primero en llegar primero en salir (FIFO).
- Proofpoint: Empresa estadounidense de ciberseguridad focalizada en la seguridad de correos electrónicos y otros protocolos de comunicación.
- Ransomware: Malware que cifra información para que sea inaccesible y utiliza la extorsión para compelir al objetivo a cumplir las demandas de quien realizó el cifrado.
- Rapid7: Empresa estadounidense de ciberseguridad creadora del Metasploit Framework.
- REN-ISAC: por sus siglas en inglés, *Research & Education Networks Information Sharing & Analysis Center*. Los ISAC son organizaciones sin fines de lucro que brindan recursos centralizadamente para recopilar información sobre amenazas cibernéticas. El REN se centra específicamente en la industria educativa y de investigación.
- Researchgate: Red social orientada a la colaboración y cooperación entre científicos e investigadores.
- SAFER: por sus siglas en inglés, *Security Assistance For Education & Research Trust Group*. Es un grupo operacional focalizado en la lucha contra el uso indebido de computadoras en el ámbito académico, educativo y de investigación.
- Salesforce: Empresa estadounidense focalizada en el desarrollo de soluciones en la nube.
- SANS: Empresa estadounidense de ciberseguridad focalizada en la educación.
- Seagate: Empresa estadounidense de almacenamiento de datos.
- SIEM: por sus siglas en inglés, *Security Information and Event Management*. Sistema que centraliza el almacenamiento y gestión de eventos de seguridad.
- SIGMA: Formato abierto y genérico que permite describir logs de manera sencilla.

- SOAR: por sus siglas en inglés, *Security Orchestration Automation and Response*. Sistema que genera flujos de trabajo y automatiza procedimientos de respuesta a eventos de seguridad.
- SOC: por sus siglas en inglés, *Security Operation Center*. Los centros de operaciones de seguridad monitorea y controlan la seguridad en las redes y sistemas.
- SOC Prime: Empresa estadounidense de ciberseguridad focalizada en la detección de amenazas.
- SOCRadar: Empresa estadounidense de ciberseguridad.
- Software: Conjunto de instrucciones computacionales para realizar tareas.
- SolarWinds: Empresa rumana de ciberseguridad.
- Sophos: Empresa británica de ciberseguridad focalizada en la seguridad de sistemas y comunicaciones.
- Spear-phishing: Ataque similar al Phishing, donde el adversario dirige el ataque a una entidad específica. El ataque de phishing suele referir a un ataque no dirigido, donde el adversario ataca con por igual a múltiples objetivos.
- Splunk: Empresa estadounidense focalizada en el desarrollo de soluciones de ciberseguridad.
- Sqrrl: Empresa estadounidense subsidiaria de Amazon focalizada en el Threat Hunting.
- STIX: por sus siglas en inglés, *Structured Threat Information Expression*. Es un lenguaje estructurado para la información de ciberinteligencia.
- TAXII: acrónimo del inglés, *Trusted Automated eXchange of Intelligence Information*. Es un lenguaje estructurado para compartir información de ciberinteligencia.
- TCP: por sus siglas del inglés, *Transmission Control Protocol*. Es un protocolo de redes IP orientado a la conexión, por lo que se debe establecer una conexión entre el cliente y el servidor previo a que los datos puedan ser enviados.
- Tenable: Empresa estadounidense de ciberseguridad focalizada en la detección y escaneo de vulnerabilidades.

- Timesketch: Herramienta de código abierto para el análisis colaborativo de datos visualizados en una línea de tiempo.
- TOR: por sus siglas del Inglés, *The Onion Router*. Referencia tanto al proyecto que lo desarrolla como a la red misma (superpuesta sobre Internet), cuyo objetivo principal es la comunicaciones distribuida ocultando la dirección IP origen (anonimato a nivel de red) manteniendo la integridad y la confidencialidad de la información.
- Three-way handshake: Metodología que utiliza el protocolo TCP para establecer una conexión IP fiable.
- ThreatConnect: Empresa estadounidense de ciberseguridad focalizada en ciberinteligencia.
- Trellix: Empresa estadounidense de ciberseguridad focalizada en la seguridad de sistemas creada a partir de la unión de McAfee y FireEye.
- TTP: por sus siglas en inglés, *Tactics, Techniques and Procedures*. Método para detectar amenazas focalizado en observaciones sobre las tácticas, técnicas o procedimientos que podrían indicar la presencia de un atacante..
- UEBA: por sus siglas en inglés *User and Entity Behavior Analytics*. Utiliza técnicas de aprendizaje automático (*Machine Learning*) para modelar el comportamiento de usuarios y dispositivos para identificar comportamientos anormales.
- Ubuntu: Distribución de Linux basada en Debian y compuesta principalmente por software libre y de código abierto.
- VMWare: Empresa estadounidense de tecnología focalizada en la virtualización de sistemas.
- VMware Carbon Black: Empresa estadounidense de ciberseguridad perteneciente a la empresa VMware.
- Windows: Sistema operativo propietario de la empresa Microsoft.
- World Economic Forum: Organización internacional no gubernamental localizada en Suiza.
- YARA: Herramienta para ayudar a los investigadores de malware a identificar y clasificar muestras de malware.
- Zeek: Anteriormente conocido como Bro, es un software (y también un formato) gratuito y de código abierto para el análisis de comunicación de red.

- Zettabytes: Un Zetabyte equivale a 1000 Exabytes, equivalente a 1000000 Petabytes, equivalente a $1.e+9$ Terabytes, equivalente a $1.e+12$ Gigabytes, equivalente a $1.e+15$ Megabytes, equivalente a $1.e+18$ Kilobytes, equivalente $1.e+21$ bytes.
- ZScaler: Empresa estadounidense de ciberseguridad focalizada en la seguridad de las comunicaciones.