Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Análisis forense de eventos en Infraestructuras críticas

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Muñiz Da Costa, Alejandro

Tutor: Oltra Gutiérrez, Juan Vicente

Curso 2020/2021

Resumen

El objetivo de este trabajo es presentar al lector una serie de herramientas que le pueda servir de utilidad de cara a realizar un análisis forense de los eventos en una Infraestructura Crítica. Para esto, el trabajo comienza con una introducción al contexto de estas infraestructuras indicando su marco legal, la situación de las Infraestructuras Críticas en España y comentando la principal amenaza de estas, las APTs. Tras ello, se explica el proceso de toma de evidencias, con la finalidad de entender qué tipo de herramientas necesita un investigador forense, y tras realizar una clasificación de estas según su objetivo, se pasa a exponer una serie de herramientas de cada clase. Para concluir, se añaden herramientas elaboradas por el CCN-CERT específicamente para el contexto de las Infraestructuras Críticas.

Este trabajo busca servir como guía de cara a la elaboración de un paquete de herramientas personalizado para el análisis forense de las incidencias producibles en Infraestructuras Críticas. El resultado obtenido de este trabajo es la presentación de una serie de herramientas clasificadas según su utilidad y resumidas al final en forma de una serie de tablas.

Palabras clave: Infraestructuras Críticas, Ciberincidencias, Intrusión, APT, Evidencias, Monitorización del sistema, análisis de red, malware, Reversing y Análisis Forense.

Abstract

The main goal of this work is present to the reader a list of tools useful in order to do forensics analysis of the events in a Critical Infrastructure. To archive this goal, this work starts introducing the context of this infrastructures, remarking its legal framework, the situation of Critical Infrastructures in Spain and pointing its main threat, the APTs. After this, it is explained the process of taking of evidence, with the purpose of doing a classification depending on its aims. This forensics tools will be also explained to let the reader know how they work and how they can be used for. To conclude, there are included some CCN-CERT's tools elaborated specifically to be used in Critical Infrastructures.

This academic work tries to serve as a guide to any reader who wants to elaborate a personal toolkit to realize forensics investigations of the cyberincidents that may occur in Critical Infrastructures. The result obtained in this work is the presentation of a list of tools classified by its utilities and resumed at the end in four tables.

Keywords: Critical Infrastructures, Cyber-incidents, Intrusion, APT, Evidences, System Monitoring, Net Analysis, Malware, Reversing and Forensics Analysis.

Tabla de contenidos

Índice de figuras

Índice de tablas

1. Introducción

Un ordenador te permite cometer más errores y más rápido
que cualquier otra invención en la historia de la humanidad,
con las posibles excepciones de las pistolas y el tequila.
Mitch Radcliffe.

Décadas atrás, cuando la informática aún estaba dando sus primeros pasos, lo último que podría preocupar a cualquier persona era la seguridad de esta, ya que no se concebía que se pudiese y quisiese atacar a esta nueva tecnología. Años más tarde, la entrada en escena de crackers[1], como Kevin Mitnick o Matthew Bevan y Richard Pryce, hizo que tanto el público general como las instituciones se diesen cuenta de lo potencialmente peligroso que puede ser un ordenador [1]. Un ejemplo de este potencial peligro lo podemos ver en Estonia, que en 2007 sufrió un hackeo que dejó sin actividad a una gran parte de las infraestructuras críticas de dicha nación, quedando inaccesible durante semanas las páginas gubernamentales o las de los bancos más importantes del país, entre otras [2].

Actualmente, la seguridad informática ha evolucionado en gran medida, habiendo multitud de sectores y expertos que se dedican a mejorarla lo máximo posible. Pero, aun así, para poder defender un sistema o infraestructura, el especialista en seguridad defensiva debe encontrar todos los vectores de ataque posible y prever su explotación, mientras que el atacante con encontrar una brecha ya ha ganado. Si esto de por sí ya no suena muy halagüeño, aún falta por incluir la pieza más peligrosa de este duelo: el ser humano. Errores tan frecuentes como pueden ser el dejarte una contraseña apuntada, utilizar pendrives que te encontraste por la calle o confiar en el correo que te acaba de llegar de un supuesto compañero pueden ser un baipás a todas las capas de protección puestas por la empresa o institución.

Visto esto, la mejor estrategia de seguridad es en la que se trata de prevenir todos los problemas posibles, se educa lo mejor posible a los trabajadores para que no se equivoquen demasiado y se sobreentiende que aun así no se va a evitar la totalidad de los ataques, por lo que se trata de detectar desde dentro aquellos ataques que hayan podido evadir todas las trabas puestas. Es en este punto donde entra el análisis forense, cobrando incluso más importancia en el sector de las infraestructuras críticas. La protección de estas infraestructuras es vital en muchos aspectos, siendo considerado el ciberataque a estas como la mayor amenaza no ambiental para la humanidad [3].

Por esto mismo consideramos que este trabajo puede tener una utilidad real. Un doctor, por muy bueno que sea, no puede identificar con certeza el mal de un paciente si no cuenta con las herramientas necesarias (analíticas, máquinas de rayos X, TACs, etc.), esto mismo sucede con los informáticos forenses. Saber identificar correctamente los indicios de una anomalía en el funcionamiento del sistema o red es crucial para poder detectar y parar a tiempo un posible ataque, y este trabajo puede ayudar a aportar dichas herramientas. En una situación crítica, saber qué y dónde buscar y como interpretarlo puede ser clave en la resolución de un problema.

[1] **Cracker:** Es una persona interesada en saltarse la seguridad de un sistema informático.

1.1. Motivación

Dentro de la carrera de informática podemos encontrar una gran cantidad de ramas, desde el más bajo nivel en Hardware hasta la administración de sistemas en red, pasando por la programación, diseño de redes, creación de sistemas operativos, … Pero todas estas ramas tienen una cosa en común: necesitan que el resultado sea seguro.

A nivel personal, me ha costado decidirme por qué rama optar, dado que siempre he sentido atracción por temas tan diversos como la programación de sistemas en C o por la criptografía que se aplica a las comunicaciones en red, por lo que decidí optar por una vía donde pudiera estar en contacto con todos estos campos: el área de la ciberseguridad. Por eso, mi motivación para este trabajo es lograr aprender sobre la metodología de análisis de un sistema completo, siendo las Infraestructuras Críticas el caso más interesante en el que observar esto, ya que seguramente sea el sector en el que esta seguridad es más imprescindible y a su vez el principal foco de posibles ataques a gran escala.

1.2. Objetivos

Como objetivo principal tenemos el aportar una **guía con las herramientas** a nivel de sistemas y de redes que puedan ayudar a un ingeniero forense a **recopilar datos que le ayuden a detectar posibles casos de intrusiones** en su sistema o red.

Para lograr el objetivo antes comentado, también buscamos ayudar al lector a comprender la **excepcionalidad de las Infraestructuras Críticas** en cuestiones de ciberseguridad y la importancia de una **protección proactiva**, mostrando que la seguridad no termina en el cortafuegos o en una buena gestión de contraseñas, sino que esta va más allá, siendo imprescindible un **control constante** de todos aquellos factores que nos puedan dar una pista sobre el estado de nuestro sistema y de nuestra red, aún más cuando las posibles incidencias contra estas infraestructuras tienden a ser más avanzadas y personalizadas.

1.3. Estructura

Este trabajo estará dividido en cuatro partes diferenciadas por el aspecto principal donde ponen el foco. Comenzaremos por un listado de las **normativas vigentes** en este ámbito, continuando por un **análisis teórico** de lo que es una Infraestructura Crítica y de lo que nos podemos esperar a la hora de proteger una. Tras esto entraremos ya en una parte más aplicada, en la que veremos cuáles son los **puntos más interesantes para analizar** y qué **herramientas** nos pueden ser más útiles para realizar esta recopilación de datos forenses. Por último, haremos un resumen de las **conclusiones sacadas** en esos tres puntos previos y en el que analizaremos si hemos logrado cumplir con los objetivos antes marcados.

2. Estado del Arte

El ordenador nació para resolver problemas
que antes no existían.
Bill Gates.

La informática ya es una realidad en la vida de casi todas las personas, estados y organizaciones tecnológicamente avanzadas, haciendo que esta esté presente en casi todas partes. Por ello, las Infraestructuras críticas no iban a ser menos, pudiendo encontrar componentes informáticos desde las entrañas de los sistemas que regulan el correcto funcionamiento de estas, como en los sistemas auxiliares usados por los técnicos y operarios y probablemente también podemos encontrarnos con dispositivos electrónicos en los bolsillos de casi todos los trabajadores de estos centros. Por lo que no es de extrañar que los distintos países ya se hayan puesto manos a la obra creando la normativa correspondiente.

En esta sección vamos a hacer un resumen de las **principales normas** que rigen el uso de la informática en las infraestructuras críticas. También realizaremos una mención a aquellos trabajos que hayan tratado en un pasado reciente esta temática.

2.1. Marco de Referencia

En cuanto a la regulación de la seguridad de las infraestructuras críticas, tomaremos en cuenta tanto las normas vigentes (normativa europea y española) como guías de recomendación, siendo el Esquema Nacional de Seguridad nuestra principal referencia entre estas. Cabe apuntar que esta normativa está en continua modificación y que en la actualidad la parte referente al Esquema Nacional de Seguridad está siendo revisada, pero a fecha de la realización de este trabajo no se han realizado más cambios de los aquí comentados.

Los ámbitos que tendremos más en cuenta a lo largo de este trabajo son los que están relacionados con la prevención de ciberamenazas[2] y, sobre todo, con la protección de las infraestructuras críticas. A continuación, indicaremos por orden cronológico el marco normativo que más se ajusta a estos ámbitos:

2.1.1. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Esta ley adapta la Directiva 2008/114 del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección. El objetivo buscado en esta ley pasa a ser el establecimiento de estrategias de protección (tanto físicas como cibernéticas) de las infraestructuras críticas logrando además una

[2] **Ciberamenaza:** En el contexto de la ciberseguridad, una circunstancia o evento que tiene el potencial de explotar las vulnerabilidades y de tener un potencial dañino (generar circunstancias adversas) en la organización, sus activos (incluyendo la información y los sistemas de información), sus miembros, otras organizaciones o la sociedad.

correcta coordinación entre los gestores de estas infraestructuras y las Administraciones Públicas.

Entrando en materia, se nos deja una definición formal de lo que se considerará como Infraestructura crítica de cara a la aplicación de dicha ley:

> **Artículo 2.e Infraestructuras críticas:** las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Establece también los siguientes **doce sectores** como aquellos **donde se aplicará esta catalogación**: Administración, Espacio, Industria nuclear, Industria química, Instalaciones de investigación, Agua, Energía, Salud, Tecnologías de la Información y las Comunicaciones (TIC), Transporte, Alimentación y el Sistema financiero y tributario.

Además, se realiza una parametrización de los **factores** que marcarán **cuan crítico es un sistema**, siendo estos los siguientes: número de personas afectadas, impacto económico, impacto medioambiental e impacto público y social.

Por último, en su Título III se especifican los **planes de actuación que deberán ser elaborados** por el personal competente en la materia además de otras consideraciones para mejorar la comunicación con el Sistema de Protección de Infraestructuras Críticas definido en su Título II.

2.1.2. *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.*

Este reglamento sirve como continuación a la Ley 8/2011 antes comentada, ya que es en el que se desarrolla el marco de medidas ya anunciado en dicha ley. También regula las obligaciones tanto del Estado como de los operadores de las infraestructuras críticas de cara a este nuevo marco normativo, delimitando el ámbito de actuación de cada uno de los miembros involucrados. Determina las funciones a llevar a cabo por el **Centro Nacional para la Protección de las Infraestructuras Críticas** (CNPIC) y la **Comisión Nacional para la Protección de las Infraestructuras Críticas** (referenciada como la Comisión), los cuales fueron creados en la Ley 8/2011.

En el Título III de este documento, se especifica el **Plan Nacional de Protección de las Infraestructuras Críticas**, siendo el documento en el cual se establecen los criterios y directrices para la coordinación de las Administraciones públicas con los operadores críticos. También establece una jerarquía de niveles de seguridad e intervención policial que dependen del Plan de Prevención y Protección Antiterrorista.

Al igual que en el documento anterior, en este Real Decreto no se entra en materia, sino que funciona como un **marco de definición de competencias** entre los distintos organismos y como punto de **definición de una serie de planes** que fueron desarrollados posteriormente por los profesionales especializados en dichas materias.

2.1.3. *Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.*

En esta resolución, el principal objetivo es el de establecer los contenidos mínimos que deberán incluirse a la hora de elaborar un **Plan de Seguridad del operador** (PSO) por parte de los operadores críticos. Establece que el PSO deberá ser presentado ante el Centro Nacional para la

Protección de las Infraestructuras Críticas y revisado cada dos años. Entre la materia incluida, el PSO siempre deberá incluir los siguientes cuatro puntos:

- Política general de seguridad del operador y marco de gobierno.
- Relación de Servicios Esenciales prestados por el operador crítico.
- Metodología de análisis de riesgo (amenazas físicas y de ciberseguridad).
- Criterios de aplicación de Medidas de Seguridad Integral.

Se define una Política General de Seguridad del Operador y Marco de seguridad, en la que, entre otras cosas, se incluye los organismos a los que hay que comunicar las incidencias, los campos sobre los que hay que formar y concienciar al personal de estas infraestructuras, la información mínima a aportar cuando se realice un análisis de riesgos, los riesgos valorados a la hora de realizar el PSO y los criterios de aplicación de medidas de seguridad.

Por último, también define el **Plan de Protección Específico** (PPE) que el operador crítico debe redactar para cada una de las Infraestructuras críticas que posea o gestione. Este PPE debe indicar como mínimo los siguientes puntos:

- Organización de la seguridad.
- Descripción de la infraestructura.
- Resultado del análisis de riesgos.

Al igual que en el caso del PSO, en esta resolución también se definen aspectos básicos de este plan. Algunos de estos aspectos son: el organigrama de seguridad y cómo designar al Delegado de Seguridad, los mecanismos de coordinación con otras infraestructuras críticas, autoridades o terceros; cómo se ha de realizar la descripción de una infraestructura crítica, incluyendo las instalaciones físicas, los sistemas informáticos, la arquitectura de red o los miembros del personal como puntos a destacar. También se establece que en el PPE se deben indicar las amenazas y los riesgos considerados al realizarlo y todas las medidas de seguridad integral existentes.

2.1.4. *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.*

El Real Decreto-Ley 12/2018 adapta la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (conocida como la Directiva NIS). En él se presenta el marco estratégico e institucional a través del cual se regulan las funciones de las autoridades competentes, matizando también en qué casos la responsabilidad de la respuesta a los incidentes será del CNI-CERT, en cuales será del INCIBE-CERT y en los que será del ESPDEF-CERT, siendo además el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) el que servirá como coordinador entre estos centros de respuesta de incidentes y el Ministerio de Interior. También se regula cómo se realizará la notificación de incidencias entre estos organismos.

El resto del Real Decreto-Ley se ve desarrollado a través del Real Decreto 43/2021, en el cual se realiza una supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y digitales y de la gestión de incidentes de seguridad.

Al igual que en la Ley 8/2011, en este documento se especifican las autoridades competentes de cada uno de los doce sectores catalogados como críticos junto al procedimiento de cooperación y coordinación entre ellas. Además incluye en sus anexos una **clasificación de los ciberdelitos** y una **división** de estos **por su nivel de peligrosidad**, por lo que lo resumiremos más adelante, haciendo énfasis sobre todo en esta última parte.

2.1.5. *Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.*

En esta orden, se indica el objetivo nacional de establecer un ciberespacio abierto, plural y seguro, mediante la **participación activa con instituciones de ciberseguridad y empresas privadas** y la adopción de un **modelo de ciberdefensa más proactiva** que esté basada en la investigación y en la disuasión.

También, en su Capítulo II se nombran las principales amenazas y desafíos en el ciberespacio, siendo estas el **ciberespionaje**, las **amenazas híbridas**, la **cibercriminalidad**, el **uso de criptomonedas para financiar o contratar servicios ilícitos** o la realización de delitos de carácter económico o el **uso malintencionado de datos personales**. A estas amenazas también le añaden las del **ciberterrorismo**, el **hacktivismo** y las **campañas de desinformación**.

En su Capitulo III se indican los propósitos, principios y objetivos para la ciberseguridad a nivel nacional. El principal propósito indicado para este documento es fijar las directrices generales en ciberseguridad para poder cumplir los objetivos que aparecen en la Estrategia de Seguridad Nacional. **La unidad de acción, anticipación, eficiencia y resiliencia** están señalados a su vez como los principios rectores de esta estrategia nacional. Como parte final de este capítulo se nos listan los siguientes objetivos generales:

1. Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.
2. Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso.
3. Protección del ecosistema empresarial y social y de los ciudadanos.
4. Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.
5. Seguridad del ciberespacio en el ámbito internacional.

A su vez, en el Capítulo IV se nos listan las líneas de acción, y las medidas dentro de estas, que se seguirán para lograr alcanzar los objetivos establecidos en los puntos previos. Estas **líneas de acción** son: Reforzar las capacidades ante amenazas del ciberespacio, garantizar la seguridad y resiliencia de activos estratégicos, reforzar la capacidad de investigación y persecución de la cibercriminalidad, impulsar la ciberseguridad de ciudadanos y empresas, potenciar la industria española de ciberseguridad, contribuir a la seguridad del ciberespacio a nivel internacional y desarrollar una cultura de ciberseguridad.

Por último, en el Capítulo V se indica la **estructura organizativa para Seguridad Nacional**, la cual está conformada por las siguientes seis instituciones:

1. El Consejo de Seguridad Nacional.
2. El Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis.
3. El Consejo Nacional de Ciberseguridad.
4. La Comisión Permanente de Ciberseguridad.

5. El Foro Nacional de Ciberseguridad.
6. Las Autoridades públicas competentes y los CSIRT de referencia nacionales.

Incluyéndose también en este capítulo una breve descripción de cada una de estas.

2.2. Guías CCN-STIC

Para facilitar la labor de los miembros de las administraciones públicas que tengan el deber de **aplicar el Esquema Nacional de Seguridad**, el Centro Criptológico Nacional ha definido las **guías CCN-STIC** (Centro Criptológico Nacional – Seguridad de las Tecnologías de las Tecnologías de Información y Comunicación).

Estas guías están divididas en series, siendo la serie ***800 – Guía Esquema Nacional de Seguridad***, la que utilizaremos en mayor medida. Los documentos que nos serán de más ayuda son:

- Guía CCN-STIC 811 – Interconexión en el ENS.
- Guía CCN-STIC 815 - Métricas e indicadores.
- Guía CCN-STIC 817 - Gestión de Ciberincidentes.
- Guía CCN-STIC 818 - Herramientas de seguridad.

Estos documentos serán explicados en el apartado 3.2. Ciberseguridad en España – Esquema Nacional de Seguridad. Además, también nos hemos apoyado en la guía *CCN-STIC 804 – Medidas de Implantación* en la cual se resumen las distintas medidas indicadas en el ENS y aporta bibliografía relacionada para cada una de ellas.

2.3. Trabajos relacionados

Entre algunos trabajos académicos que guardan relación con este, podemos encontrar los **TFGs**, *Clasificación y estudio de herramientas para periciales informáticas* (2015) de Alberto José Pedrera Ros, *Esquema Nacional de Seguridad: Protección de una infraestructura crítica del sector administración* (2019) de Jorge Revert Enguix y *Pruebas y evidencias telemáticas* (2015) de Jordi Magraner Gimeno.

Además, fuera de la UPV también podemos encontrar **otros trabajos** como *La protección de infraestructuras críticas* (2014) de Mónica Miranzo, *Security threats to critical infraestructura: the human factor* (2018) de Ghafir, I., Saleem, J. Hammoudeh, M. y *Caso práctico de informe experto de análisis digital forense* (2016) de Helena Taribó Gómez.

A nivel de **artículos académicos** también podemos contar con *Metodología para el análisis de incidentes de ciberseguridad o ciberataques durante las acciones de ciberdefensa de las infraestructuras críticas de la defensa nacional* (2019) de J.C. Liporace et al., *Desarrollo de una guía para el abordaje de incidentes de ciberseguridad en infraestructuras críticas industriales* (2021) de J. Kamlofsky, G. Gonzalez, y S. Trigo, *Developing a Digital Forensic Capability for Critical Infrastructures: An Investigation Framework* (2020) de A. Mahmoud y el **libro** Cybersecurity: *Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare* (2015) de T. A. Johnson.

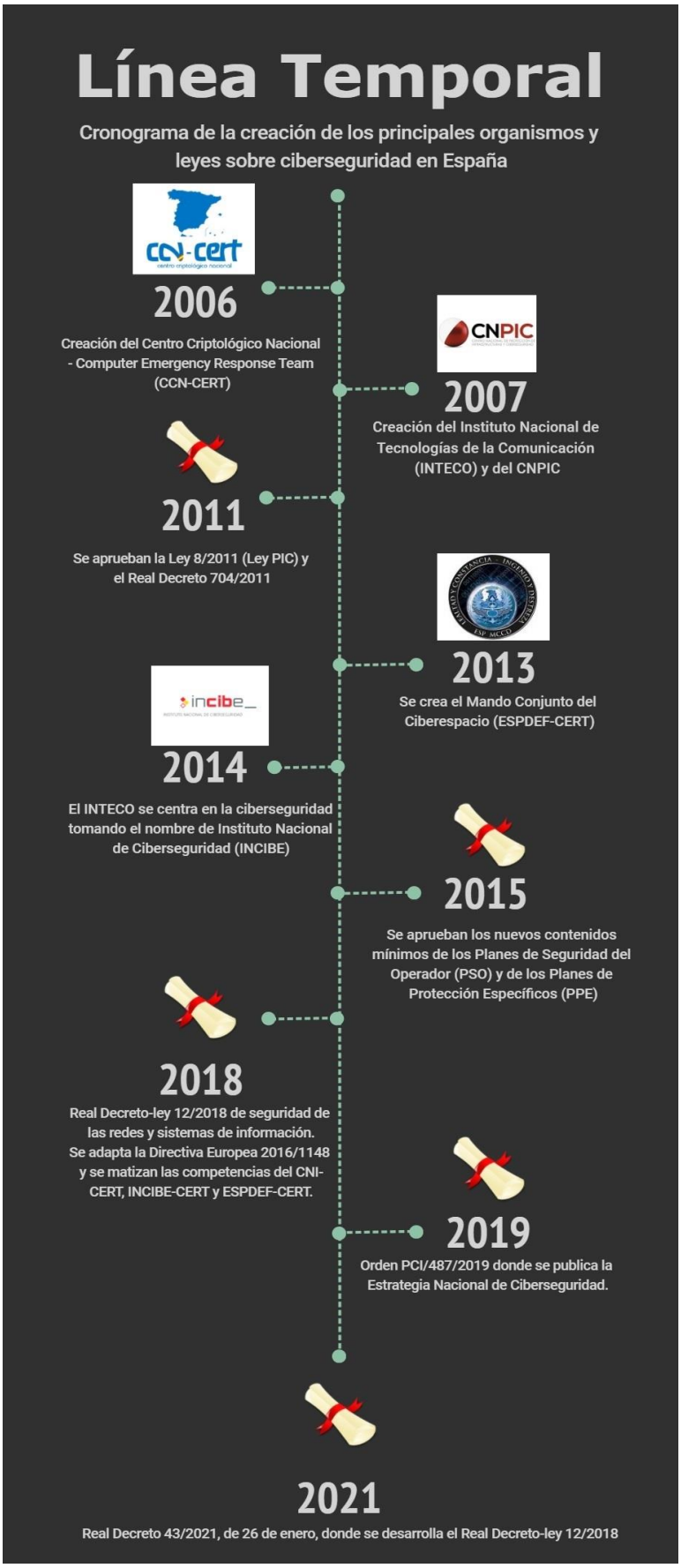

Figura 1. Cronograma de aprobación de las instituciones y leyes sobre Ciberseguridad en España. Elaboración propia. Fuente: web del CSIRT.

3. La Ciberseguridad en las Infraestructuras Críticas de España

Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores.
Kevin Mitnick.

Con la llegada de las nuevas tecnologías y la adopción de estas en nuestro día a día, hemos asumido una serie de riesgos que, por norma general, no solemos tener en consideración. Para poner en jaque una organización no hace falta un ataque masivo o una vulnerabilidad no descubierta, basta con un correo fraudulento a un empleado o un pendrive malicioso tirado frente a la organización [4]. Esto en una empresa estándar, puede ser un fastidio, ocasionando un mayor o menor problema económico y de imagen, pero en el sector de las Infraestructuras Críticas, todo esto se magnifica. Pongamos la siguiente situación; te despiertas una mañana y te das cuenta de que en casa no tienes ni electricidad ni agua corriente. Al salir de casa dirección al trabajo, intentas coger el metro, pero este no aparece, por lo que tendrás que ir andando (o más bien, corriendo). Como no te ves capaz de llegar a tiempo, decides llamar para avisar a algún compañero o a tu jefe… ¡pero tu teléfono no tiene cobertura! Además, tu jefe informa a toda la plantilla que este mes no podréis cobrar los sueldos a tiempo al estar el banco completamente inoperativo, y lo peor de todo, ¡Tampoco puedes ir a quejarte al ayuntamiento de tu ciudad por que este ha desaparecido!

Este sería un caso algo extremo en el que sean varias las infraestructuras afectadas, pero no por ello deja de ser posible. Por lo general, cuando una zona está en medio de una guerra, los distintos bandos tratan de sabotear las infraestructuras críticas del bando rival para crear caos, dejando situaciones muy parecidas a la antes descrita, y, ya en una medida mucho menor, un ciberataque a una infraestructura crítica pública o privada puede generar una situación de descontrol temporal, como pasó recientemente en algunas zonas de Estados Unidos ante un ataque *ransomware*[3] a una red de oleoductos [5].

En el caso de España, el número exacto de cuantas infraestructuras críticas es confidencial, pero en cambio podemos saber que contamos con un total de 180 operadores críticos en nuestro país, además de un total de 148 Planes de Seguridad del Operador (PSO) y 259 Planes de Protección Específicos (PPE) autorizados [6].

[3] **Ransomware:** El malware de rescate, o ransomware, es un tipo de programa maligno que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Estos ataques están ganando cada vez más presencia en el panorama actual, hasta el punto de que a nivel estatal se aportan diferentes soluciones específicas para ayudar a las empresas que sufren estos ataques. En España es el INCIBE el que aporta estas ayudas a través de su portal: https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware.

3.1. Qué son las Infraestructuras Críticas

Como hemos comentado en el apartado anterior (en la ***Ley 8/2011, de 28 de abril***), una Infraestructura crítica es aquella cuyo fallo o parada puede tener un impacto potencialmente dañino a nivel económico o social. Estas infraestructuras realizan una labor estratégica en el funcionamiento de nuestra sociedad, y se pueden dividir en los siguientes doce sectores críticos:

1. **Administración:** Servicios críticos, instalaciones, redes de información, activos, sitios y monumentos principales.
2. **Agua:** Embalses, almacenamiento, tratamiento y redes.
3. **Alimentación:** seguridad alimentaria, medios de producción, mayoristas e industria alimentaria.
4. **Energía:** Centrales y redes eléctricas, producción de petróleo y gas, instalaciones de almacenamiento y refinerías y sistemas de transmisión y distribución.
5. **Espacio:** Edificios y centros relacionados con la investigación del espacio exterior.
6. **Sistema financiero y tributario:** Banca, bolsa de valores y centros de inversión.
7. **Instalaciones de investigación:** Laboratorios que puedan producir o contener material peligroso o sensible.
8. **Industria Química:** Centros de producción, almacenamiento y transporte de material químico y biológico.
9. **Industria Nuclear:** Centros de producción, almacenamiento y transporte de material radiológico y nuclear.
10. **Salud:** Hospitales, centros de atención sanitaria y de suministro de sangre, laboratorios y empresas farmacéuticas, servicios de búsqueda y rescate y servicios de urgencias.
11. **Tecnologías de la Información y las Comunicaciones (TIC):** Centros de telecomunicaciones, sistemas de radiodifusión, programas informáticos y soporte físico y de redes.
12. **Transporte:** Aeropuertos, puertos, instalaciones intermodales, ferrocarril, redes de transporte público y sistemas de control del tráfico.

Aunque en España, sí que tenemos definidos los sectores a considerar como críticos, **las infraestructuras** que aquí hemos indicado como parte de estos, **no conforman una lista cerrada**. Estas forman parte de una recopilación que realiza la comisión de las comunidades europeas en su plan de *Protección de las infraestructuras críticas en la lucha contra el terrorismo* [7].

Como es esperable por su clasificación, estas infraestructuras cuentan con una gran importancia en el correcto funcionamiento de un país, siendo imprescindible no solo una protección física de estas, sino también un esfuerzo en su ciberseguridad. Esto cobra más importancia aún si nos fijamos en los números que nos enseña el departamento de seguridad nacional en el informe antes comentado. En él, en 2019 las infraestructuras críticas sufrieron un total de **8.086 incidentes en cuestión de ciberseguridad**, lo cual contrasta notablemente con los 89 incidentes que se notificaron en relación con la seguridad física [8].

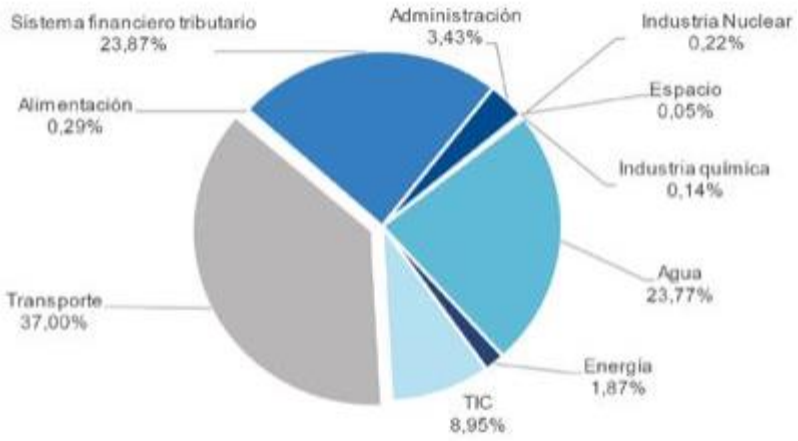

Figura 2. Porcentaje de ataques a infraestructuras críticas según el sector. Fuente: DSN.

Estos números suponen un aumento de aproximadamente el 16,3% respecto a los 6.954 casos notificados en 2018, cifras que ya están muy lejos de los 118 ataques notificados en 2015 y aún más de los 17 notificados en 2013. Por eso mismo cada vez es más importante una buena gestión de estos incidentes. En febrero del 2020 el Consejo Nacional de Ciberseguridad aprobó la *Guía Nacional de notificación y gestión de ciberincidentes* [9]. En este documento, se nos expone un proceso de **seis fases** a pasar para realizar una correcta gestión de estas incidencias.

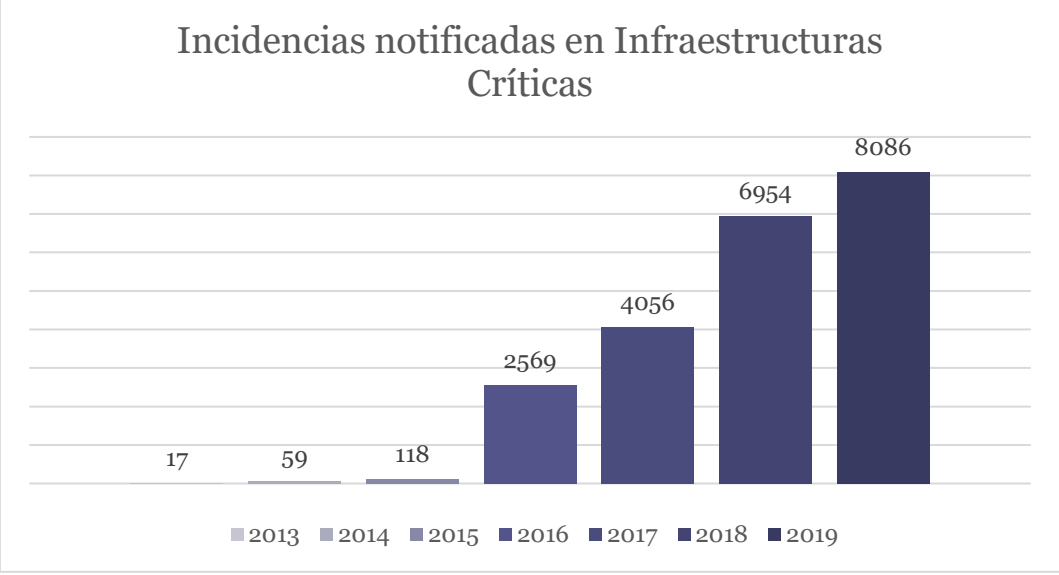

Figura 3. Número de incidencias notificadas en Infraestructuras Críticas en España desde 2013. Elaboración propia. Fuente: DSN.

Las seis fases son necesarias para realizar una gestión rápida y eficaz, pero la relación de ellas no tiene que ser lineal, sino que pueden estar relacionadas formando un bucle o realizarse de manera simultánea. Estas fases son [9]:

a) Preparación

Es la fase inicial, busca tener tanto al personal, como los procedimientos y la tecnología a punto para que puedan **responder de manera rápida y eficiente** ante cualquier acontecimiento.

Alguno de los puntos más importantes de esta fase es asegurarse de contar con información de contacto actualizada, mantener las políticas, procedimientos y análisis de riesgos al día, formar de manera teórica y práctica al equipo humano y tener herramientas útiles para todas las fases.

b) Identificación

El objetivo de esta fase es identificar o **detectar posibles sucesos que puedan representar una ciberincidencia**[4]. Esta fase se realiza en paralelo con la anterior, ya que es importante el mantenerse preparado hasta que aparezcan. En este punto cabe destacar que no todos los eventos son ciberincidencias, por eso mismo es muy importante contar con herramientas que nos permitan reducir al máximo tanto los falsos negativos como también los falsos positivos.

Una **correcta identificación** constará de una monitorización de las redes, sistemas y aplicaciones, una recolección de información que nos permita detectar anomalías, una correcta diferenciación entre eventos simples y ciberincidentes, una comunicación eficiente al contacto pertinente y una recopilación, almacenamiento y compartición de las evidencias para mejorar la capacidad de detección de otras.

c) Contención

En el momento en el que se detecta una ciberincidencia, la máxima prioridad del equipo pasa a ser la **contención y aislamiento de esta**. Se debe evitar que el problema se expanda a otros sistemas o redes y que exfiltre información.

En esta fase se deberá continuar con las acciones ya comentadas en la fase anterior, añadiendo el deber de evaluar todas las evidencias a nuestra disposición para realizar un cribado según el tipo y la criticidad de la información y los sistemas afectados.

d) Mitigación

Las medidas a tomar aquí dependerán mucho del tipo de ciberincidencia detectada. Algunas de las recomendaciones para esta fase serían: Determinar las causas y los síntomas de la ciberincidencia para realizar una mejor selección de las medidas a tomar, identificar y eliminar todo software utilizado por los atacantes, pudiendo llegar a ser necesario incluso el recuperar copias de seguridad previas a la aparición de esta incidencia y detectar si el atacante está haciendo uso de servicios legítimos para llevar a cabo sus propósitos.

e) Recuperación

Ya con la incidencia resulta y el posible agente malicioso aislado, el objetivo de esta fase pasará a ser **recuperar la operatividad previa** para que las áreas de negocio afectadas puedan volver a su correcto funcionamiento. Es **importante no precipitarse**, dado que se pueden estar dejando actividades maliciosas atrás. Por eso mismo, también es importante realizar una mayor

[4] **Ciberincidencia:** En el ámbito de la ciberseguridad, ocurrencia que tiene el potencial de provocar consecuencias adversas para un sistema de información o para la información que este procesa, almacena o transmite y que puede requerir un plan de acción para mitigar las posibles consecuencias.

monitorización durante esta fase, tratando de estar atentos ante cualquiera anomalía sospechosa que se hubiera podido escapar.

f) Posincidente

Una vez recuperada la situación de normalidad, es importante realizar una **correcta evaluación y recopilación de toda la información** sacada en claro de esta incidencia, tratando de que esta sirva como aprendizaje ante futuras situaciones similares. En esta fase se debe realizar un informe en el que se detalle la causa y coste de la incidencia, así como las medidas tomadas ante esta incidencia y ante futuras incidencias similares.

En este trabajo trataremos de aportar al lector una guía con algunas de las mejores herramientas disponibles para la identificación de ciberincidencias, entrando por ende en el contexto de las fases de **Preparación** e **Identificación**.

3.2. Esquema Nacional de Seguridad

La continua adaptación de nuestras vidas e infraestructuras a las nuevas tecnologías hace necesaria la adopción de medidas organizativas y nuevas técnicas que nos permitan mantener el nivel de seguridad esperable, reduciendo lo máximo posible el daño producido por la aparición de nuevas amenazas.

De esta manera, en 2007, se aprueba la *Ley de acceso electrónico de os ciudadanos a los servicios públicos* (ley 11/2007, de 22 de junio), la cual creará el Esquema Nacional de Seguridad (en adelante ENS). Tras esto, en 2010 primero y en 2015 después, se crean dos Reales Decretos que pasarán a regular al ENS.

En estos Reales Decretos, se establecen y desarrollan los siguientes **principios básicos** a tratar:

a) Seguridad integral.
b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica.
f) Función diferenciada.

Y a su vez se definen también una serie de **requisitos mínimos**, en los que se incluye la detección y gestión de incidentes de seguridad. En la descripción de este requisito se indica que se debe establecer un sistema de detección y reacción ante código dañino, además de un procedimiento de gestión y comunicación de ciberincidencias.

En este documento también se introducen las Guías de seguridad de las TIC, realizadas por el CCN. Estas guías están divididas en series, y dentro de la serie *800 - Esquema Nacional de Seguridad*, hay cuatro que nos ayudarán a la hora de enfocar las herramientas a utilizar:

3.2.1. CCN-STIC 811 – Interconexión en el Esquema Nacional de Seguridad

Esta guía tiene como objetivo analizar los distintos elementos disponibles para **interconectar sistemas que apliquen el ENS**. Para ello se deben establecer unas medidas de protección y monitorización de las conexiones que nos ayudarán en este trabajo a la hora de buscar indicios de actividades anómalas que puedan constituir parte de una acción maliciosa.

Aquí disponemos de una descripción de los elementos disponibles para construir una arquitectura de protección perimetral, además de un esquema de los distintos niveles de estas y los requisitos mínimos según la categoría del sistema a proteger. Además, se realiza una descripción de las **herramientas de protección necesarias**, lo cual nos puede ayudar de cara a la clasificación de las herramientas de análisis de red. La lista que ellos nos aportan es la siguiente:

- Detección de código dañino.
- Análisis de vulnerabilidades.
- Análisis de riesgos de actividad.
- Detección y prevención de intrusos (IDS/IPS).
- Monitorización de tráfico.
- Prevención de fuga de datos (DLP).
- Verificación de la configuración.

Ahora, a partir de esta lista, debemos sacar nuestras propias **conclusiones** sobre cómo aplica esto a nuestro caso de estudio:

1. En el caso de localizar código maligno, a través de los historiales de actualización de las herramientas podríamos detectar por donde entró este código. Además, si lo que hemos sufrido es la explotación de una vulnerabilidad, podríamos utilizar los registros de actualizaciones pendientes para revisar si esta es un 1-Day o una vulnerabilidad desconocida o aún no arreglada.
2. De detectar la presencia de virus o una actividad inusual, podemos utilizar los registros de actividad para analizar si se han realizado accesos a páginas web no autorizadas o maliciosas.
3. Podemos utilizar los IDSs para identificar alguna actividad por parte de usuarios no registrados o algún tipo de intrusión no autorizada en la red interna de nuestro sistema, además, con los registros de los IPSs podemos analizar si se trata de un caso aislado o si ya hubo más intentos que acabaron siendo bloqueados por dichas herramientas y tratar de analizar si dichos intentos están relacionados con esa actividad. Además, con los registros del tráfico de la red podemos tratar de reconstruir el camino realizado por el atacante.
4. SI se detecta alguna modificación remota de la configuración de seguridad de algún equipo, usuario o de la red, podemos revisar el origen de este y apoyándonos en los puntos antes comentados, intentar identificar de dónde surge este cambio.

3.2.2. CCN-STIC 815 - Métricas e indicadores

Este documento tiene como objetivo proponer una serie de **datos a monitorizar que nos ayuden a evaluar el estado actual del sistema**, además de un conjunto reducido de métricas e indicadores sobre dicho estado y los cuadros de mando para los escenarios típicos. Aquí se nos introducen cuatro términos que es importante diferenciar: dato, medida, métrica e indicador.

El **dato** es el detalle en bruto que se puede sacar del sistema (los archivos que se crean, las entradas en los registros, la información que se mantiene de cada documento que se destruye, …), las **medidas** son la clasificación cualitativa y cuantitativa de estos datos. Una vez tenemos estas medidas, si las relacionamos entre ellas y las representamos (por lo general de manera gráfica) pasamos a crear las **métricas** que nos ayudarán a interpretar estos valores. Por último,

cuando ya tenemos estas representaciones, si nos abstraemos de los valores en sí y los cambiamos por estados que resuman la situación del sistema, entonces ya hemos pasado a trabajar con **indicadores**.

Estas métricas e indicadores los podremos utilizar como si fuésemos un doctor analizando analíticas, con la excepcionalidad de que nuestro paciente es un sistema informático que no nos va a poder aportar más información de la que le sepamos preguntar. Por ello, se nos indican también los niveles de madurez de nuestras métricas y procedimientos, siendo necesario un nivel L3 – Proceso definido, para el caso de la monitorización del sistema. Este nivel implica un mantenimiento activo de las protecciones, aplicando correctamente la normativa y los procedimientos de prevención, detección y respuesta a incidentes.

3.2.3. CCN-STIC 817 – Gestión de ciberincidentes

El principal objetivo de esta guía es servir de ayuda para el establecimiento de capacidades de **respuesta a ciberincidentes** y a su adecuado tratamiento. También se muestran los distintos niveles de peligrosidad de los incidentes, ayudando así a una mejor clasificación y notificación.

Hay **cinco niveles de peligrosidad**, que van desde el Nivel Bajo, hasta el Nivel Crítico. Estos niveles a su vez se verán afectados según el nivel de peligrosidad del atacante y de la víctima, estando las **Infraestructuras Críticas** situadas en los **dos últimos niveles de peligrosidad**, el Nivel Muy Alto y el Nivel Crítico (clasificarán según el potencial impacto a nivel social, económico o humano). A su vez, el nivel de impacto del ataque situará a este a un nivel más bajo (por ejemplo, una campaña de SPAM) o más crítico (por ejemplo una Amenaza Persistente Avanzada, APT).

Por último, esta notificación se deberá realizar a su centro de respuesta de referencia, siendo por defecto el CCN-CERT y el INCIBE-CERT los que coordinan la notificación inicial, y habiendo cuatro organismos principales para la recepción de esta:

- **CCN-CERT:** Ciberincidentes relacionados con el sector público.
- **INCIBE-CERT:** Ciberincidentes relacionados con los ciudadanos, empresas y operadores de servicios esenciales.
- **CNPIC:** Ciberincidencias en Infraestructuras y Operadores Críticos.
- **ESPDEF-CERT:** Ciberincidencias en redes y sistemas utilizados por las Fuerzas Armadas.

A su vez, estos organismos colaborarán con los cuerpos de seguridad del estado para realizar la investigación y para tratar de identificar a los autores y responsables del ataque. En el caso de las Infraestructuras Críticas, que es el que nos atañe, la **comunicación es obligatoria si el nivel de peligrosidad o de impacto es Alto o superior**.

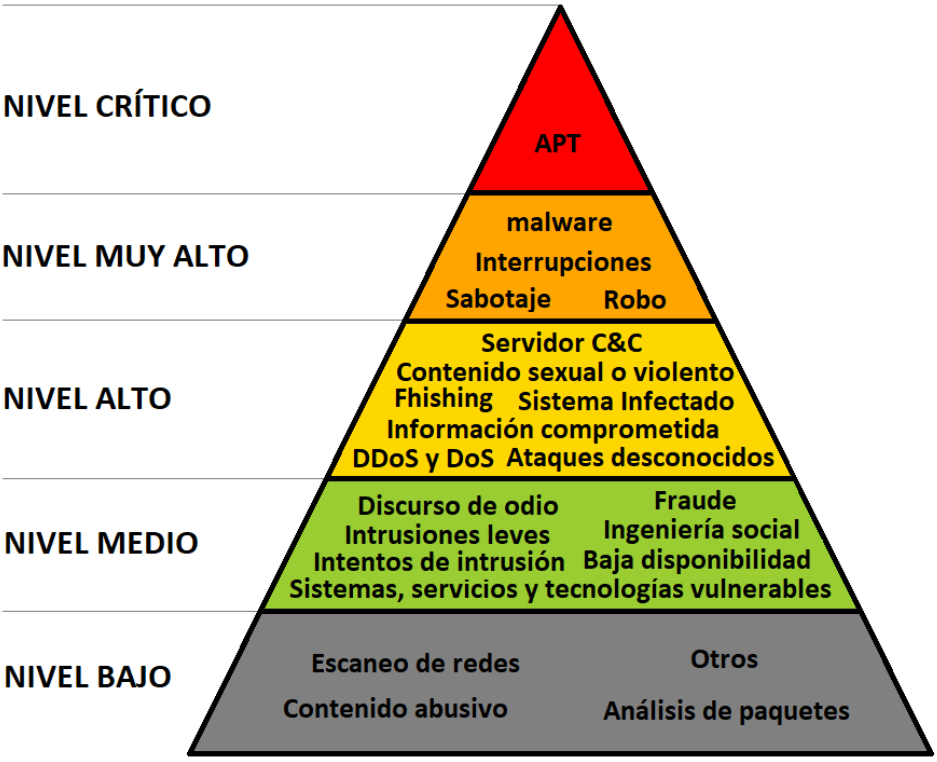

Figura 4. Listado gráfico de las distintas ciberincidencias según su nivel de peligrosidad. Elaboración propia.

3.2.3. CCN-STIC 818 – Herramientas de seguridad en el Esquema Nacional de Seguridad

En esta guía, se nos proporciona un listado de las **características a tener por las herramientas de seguridad** que se quieran utilizar siguiendo lo recomendado por el ENS. Además, ofrece también una lista de herramientas a modo orientativo que incluiremos parcialmente en el análisis que realizaremos en el apartado 7. Los **requisitos mínimos** que le asignan a estas herramientas son los siguientes:

a) **Control de acceso granular**, tanto para la información como para los recursos, y basado en el uso de perfiles de acceso.
b) **Explotabilidad** de la información resultante del uso de las herramientas, siendo posible realizar una interpretación y análisis correcto de esta.
c) **Trazabilidad de la actividad** a través del análisis de los registros logs que estas herramientas deben crear, o, en su defecto, que se creen a través de algún método alternativo.

Estas herramientas también deben pasar un **proceso de selección**, siendo necesario que estén aprobadas por el Responsable de Seguridad de la organización en cuestión, que cumplan el plan de Políticas de Seguridad de las TIC, que tengan algún tipo de certificación que las abale y que superen una evaluación según un Plan de Evaluación y Pruebas. Cabe decir, que obviamente este proceso se vuelve **más estricto según aumenta la criticidad** de la organización.

Por último, se realiza una **clasificación** de las herramientas **según cuatro categorías** (auditoría, protección, detección y reacción) y a su vez en subcategorías según el nivel de aplicación de estas. En nuestro caso nos centraremos en las dos últimas categorías y en las herramientas sugeridas en el Anexo A.

3.3. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (Ley PIC)

Como vimos en el estudio del estado del arte, el nuevo siglo trajo a Europa, y por ende, también a España, una mayor preocupación por la defensa interior. Ya no bastaba con tener a los potenciales enemigos vigilados, sino que también debíamos reforzar la vigilancia dentro de nuestras fronteras, para evitar que una organización, país o grupo terrorista llegase a la situación de poder poner en jaque a todo el país. Por eso mismo, la aprobación de la **Ley 8/2011** supuso un paso importante en la seguridad nacional, ya que se estaba creando así un marco de referencia en el que se buscaba proteger la parte más delicada del país: sus Infraestructuras Críticas.

El objetivo de esta ley, más conocida como Ley PIC, es establecer una serie de **estrategias y estructuras para una correcta coordinación** entre las distintas instituciones que colaboran para proteger las infraestructuras críticas, reduciendo así el tiempo de respuesta ante cualquiera incidencia y buscando reducir al máximo el daño potencial de un ataque a una infraestructura crítica.

Actualmente contamos con **nueve grupos de agentes** del sistema **que tienen responsabilidades** en mayor o menor medida sobre distintas partes de la protección de estas infraestructuras. Estos agentes son los siguientes:

- La secretaría de Estado de Seguridad del Ministerio del Interior.
- El recién creado Centro Nacional para la Protección de las Infraestructuras Criticas (CNPIC).
- Los distintos ministerios cuyas responsabilidades abarquen alguno de los sectores catalogados como críticos y por lo tanto tengan bajo su amparo alguna de estas infraestructuras.
- Las Comunidades y Ciudades Autónomas.
- Las Delegaciones del Gobierno en las Comunidades y Ciudades Autónomas.
- Las Corporaciones Locales a través de la asociación de Entidades Locales.
- La recién creada Comisión Nacional para la Protección de las Infraestructuras Críticas (más adelante referenciada como la Comisión).
- El recién creado Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (más adelante referenciado como el Grupo de Trabajo).
- Los operadores críticos.

Dentro de la propia Ley vemos que se han creado tres órganos diferenciados, los cuales tomarán distintas responsabilidades. Por un lado, el **CNPIC** pasa a ser el encargado de llevar el registro de las Infraestructuras Críticas de nuestro Estado, además de tener que actualizar dicho catálogo y establecer el nivel de criticidad de cada una. La **Comisión** será la responsable de aprobar los distintos Planes Estratégicos Sectoriales y de designar a los operadores críticos, mientras que el

Grupo de Trabajo será el encargado tanto de elaborar dichos Planes como de proponer a esos operadores.

A partir de entonces, el CNPIC pasó a ocupar una posición muy importante en la protección de las Infraestructuras Críticas, al ser el organismo encargado de **gestionar las ciberincidencias** relacionadas con ellas. De esta forma, cuando el CCN-CERT o el INCIBE-CERT reciben un aviso de ciberincidencia en una infraestructura registrada como crítica, estos organismos deberán pasarle el relevo al CNPIC, siendo este el **encargado de la coordinación** entre los responsables de la ciberseguridad en la infraestructura comprometida, el cuerpo de respuesta indicado y los distintos cuerpos policiales que puedan intervenir en la investigación del incidente de ser esto necesario.

4. Amenazas Persistentes Avanzadas (APT)

El único sistema seguro es aquel que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados.
Gene Spafford.

Como hemos visto en el capítulo anterior, en el ámbito de la informática contamos con tres letras que harían estremecerse hasta al más hábil de los expertos en ciberseguridad: **APT**. Una APT, o Amenaza Persistente Avanzada es un ataque informático mediante el cual se hace uso de múltiples vectores de ataque para lograr el **control total y continuado** del sistema infectado. Estos ataques suelen ser muy elaborados, siendo común que haya **organizaciones o estados** detrás de ellos [10].

A lo largo de este siglo hemos sido testigos de los APT más conocidos, siendo Stuxnet el que más fama ha logrado alcanzar [4]. Por lo general, estos ataques están dirigidos a objetivos de gran calado, ya que se suelen utilizar para **misiones de inteligencia**, para provocar **grandes daños** en una empresa o estado rival o para buscar un gran **beneficio económico**. Por este mismo motivo, cuando tratamos con Infraestructuras Críticas no podemos perder de vista la posibilidad de que estas estén en la lista de objetivos de algún actor malicioso.

En las guerras tradicionales, los ejércitos utilizan diferentes técnicas de inteligencia, siendo **SIGINT** la que está basada en la captura de señales de comunicación y electrónicas [11]. A niveles militares el SIGINT se sigue diferenciando de las operaciones informáticas (o Computer Network Operations, CNO), pero a un nivel más general, los APT ya se podrían entender como una captura activa mediante ataque. Este ataque además sería muy completo al permitir una monitorización, análisis, y si hace falta, modificación de la información del bando rival, siendo así una de las mejores herramientas de inteligencia de nuestros días y una de las más difíciles de detectar para un informático forense.

Figura 5. Distintas fuentes de inteligencia a nivel militar. Elaboración propia.

4.1. Detección

La detección de una APT puede llegar a ser un problema, dado que cuando se realiza un ataque tan completo es bastante común que se guarden las espaldas eliminando posibles rastros o incluso que se llegue a autodestruir la parte del *malware* que trabaja desde el equipo infectado. Como no es sencillo trabajar en el campo de minas que pueden suponer las APT, nos encontraremos con múltiples técnicas diferentes y complementarias. Una de ellas es la que ofreció la consultora Gartner en 2013 donde recomendaba **realizar análisis combinados a través de cinco aproximaciones distintas** [12][13]:

1. **Análisis en vivo del tráfico de red**. Análisis de eventos anómalos en la red a defender, tanto a nivel interno como en conversaciones con agentes externos.
2. **Análisis en *sandbox* [5]de la carga útil recibida**. Control fronterizo de amenazas que puede actuar tanto a nivel de la red (protección perimetral) como a nivel de dispositivos (protección de los sistemas).
3. **Análisis del comportamiento de los terminales**. Análisis de los eventos acaecidos en los equipos del sistema.
4. **Análisis forense del tráfico de red**. Análisis de los registros dejados por los eventos de red en las herramientas de acceso a la red, de monitorización y de protección perimetral.
5. **Análisis forense de los terminales**. Análisis de los registros dejados por los eventos en las distintas aplicaciones y en los registros del sistema de los equipos que conforman el sistema.

Otra aproximación interesante es la que se presenta en el artículo *HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows* [14]. En él presentan la herramienta HOLMES con la que tratan de detectar APTs en tiempo real buscando ciertas **relaciones entre flujos de información sospechosos**. HOLMES basa su funcionamiento en la generación de alertas ante eventos de bajo nivel que resulten sospechosos, dependiendo de las alertas que han aparecido, según la posible combinación de estas las catalogan como una posible señal de la presencia de una APT. Por último, de detectar esta correlación de alertas, comunica al responsable la información detectada de una manera resumida, generando también un grafo en el que resume los pasos realizados por el atacante que se han identificado.

De cualquier manera, la detección de esta amenaza no es un proceso sencillo, ya que si está bien organizado podría no dejar rastros sospechosos o incluso interferir con el software de detección de APTs para que este de resultados alterados. Esta dificultad la podemos ver en los casos más famosos que se han detectado en los últimos años, Stuxnet llegó a infectar más de 200.000 dispositivos antes de ser detectado, NetTraveler salió a la luz en 2013 pero se sospecha que llevaba infectando dispositivos desde 2005 [15], UROBUROS fue un ataque de alta complejidad y objetivos muy específicos que tardó cuatro años en ser descubierto [16], etc. Es decir, las APT bien realizada suelen tardar en descubrirse y aún más quién hay detrás de ellas, siendo en muchas ocasiones el detonante de que esto suceda la aparición de alguna información desde terceros que nos informe de que algo está pasando.

Como todo lo que llevamos dicho hasta ahora deja un sabor de boca algo pesimista para el encargado de la ciberseguridad en una IC y para los investigadores forenses, vamos a analizar dónde se puede cazar una APT según su **ciclo de vida** [13][14]:

[5] **Sandbox:** En el contexto de la seguridad informática, un sandbox proporciona un entorno estrictamente controlado en el que programas o scripts semiconfiables pueden ejecutarse de forma segura en memoria (o con acceso limitado al disco duro local).

- **Pasos previos**: Al igual que los demás ataques, para que una APT funcione correctamente el atacante debe preparar bien el camino. Para ello se suele recopilar información sobre el entorno a infectar, buscar las herramientas más útiles para lograr el objetivo y preparar la infiltración.
- **Infección**: Una vez el código malicioso está dentro, este puede requerir de alguna acción para que pueda comenzar a ejecutarse, esta puede ir desde una descarga maliciosa hasta introducir un pendrive malicioso.
- **Mando y control (C&C)**: Si la infección ha sido exitosa, el software malicioso puede intentar comunicarse con los atacantes para informar de la situación del ataque o para esperar nuevas instrucciones.
- **Actuación**: Esta es una fase cíclica en la que el atacante suele tratar de subir poco a poco en sus posibles acciones a realizar, a su vez la podemos dividir en:
    - **Escalada de Privilegios**: El atacante puede tratar de lograr más credenciales que las que obtuvo en un primer momento a través de la explotación de otras vulnerabilidades o de la captura de claves de acceso.
    - **Reconocimiento interno**: Cuando el programa maligno lleva un tiempo prudente en el sistema objetivo, puede tratar de identificar otros elementos de la infraestructura de red o el software que estos utilizan.
    - **Movimiento Lateral**: Tras conocer el entorno en el que se mueve, el *malware* puede tratar de utilizar la información recolectada o recursos compartidos para obtener acceso a otros equipos o capturar información que le interese. Este paso lo debe realizar de la manera más cautelosa posible, para así evitar ser descubierto.
    - **Mantener la persistencia**: Una vez se ha logrado infectar al objetivo se debe tratar de infectar los suficientes dispositivos como para que la detección del código malicioso en uno no suponga perder la posición de control del sistema.
    - **Exfiltración de la información**: Ya con los datos que nos interesan en nuestro dominio y con una cierta persistencia adquirida, el último paso es conseguir transmitir la información al atacante sin ser detectado. Para evitar que este tráfico de datos se detecte de manera sencilla, se suelen utilizar técnicas de ocultación como puede ser la esteganografía, además, en vez de enviar la información directamente, esta puede quedar a la espera de que el atacante mande una petición a un puerto concreto o que pida una dirección web concreta en la que se han introducido los datos a exfiltrar.
- **Fin de la infiltración**: Cuando el atacante considera que el objetivo ha sido alcanzado o que puede ser detectado, puede tratar de eliminar la APT para no dejar pistas. Esto puede hacerse desde borrando registros de conexiones solamente hasta directamente intentar destruir el dispositivo contaminado.

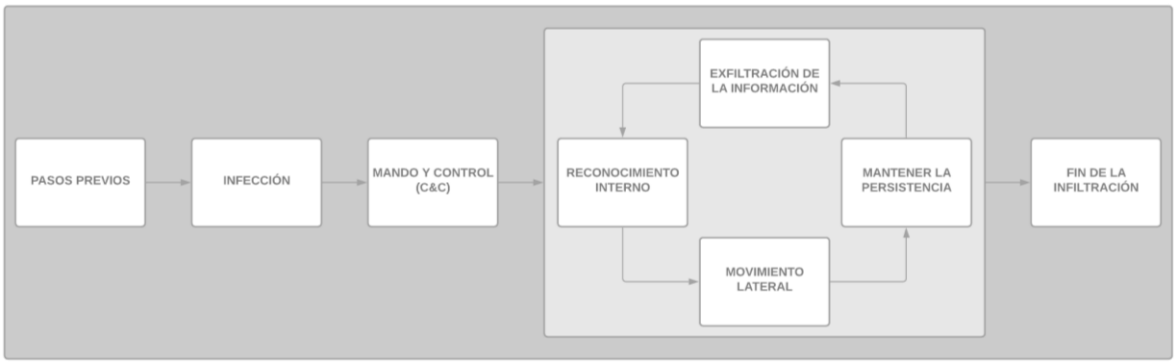

Figura 6. Ciclo de vida de una APT. Elaboración propia.

A pesar de que lograr una APT es un proceso largo y complejo, no hay muchas fases donde el investigador pueda descubrir que algo va mal. Pero no por ello es imposible detectar una APT bien realizada. Uno de los momentos de **máxima criticidad** para un atacante al realizar un ataque APT es **cuando trata de comunicarse con el equipo infectado**, dado que desde la organización objetivo podemos monitorizar las conexiones y el tráfico de red. En la mayor parte de las Infraestructuras Críticas, los protocolos de comunicación web más usados son **HTTP**, **DNS** y **SMTP**, de manera que el administrador de la red podría bloquear los servicios web que no usen estos tráficos o en su defecto monitorizar sus tráficos de datos con lupa. Otra medida de detección puede ser utilizar el proxy corporativo para centralizar el origen de toda información saliente en el tráfico HTTP y los servidores corporativos correspondientes para otorgar legitimidad al tráfico DNS y SMTP [13].

Pero como hemos recalcado en varias ocasiones en este trabajo, la vida de un encargado de ciberseguridad no es sencilla, por lo que esas medidas no pueden abarcar todo el tráfico. En el caso del tráfico HTTP, hay información que nos ayuda con la navegación que no es registrada en el proxy corporativo, por lo que debemos complementar esa política de seguridad con el uso de herramientas que nos permitan aumentar nuestra capacidad de detección de anomalías. En el caso del tráfico SMTP y DNS, también es recomendable añadir **herramientas de análisis del tráfico** para complementar la información que se almacena en los registros de acceso al servicio, especialmente en el caso del tráfico DNS al ser sus registros más limitados que en otros casos comentados.

Con estas medidas podemos mejorar la situación inicial de la que partíamos, pero sigue habiendo dos problemas: no siempre podremos vigilar a la vez todo el tráfico y de lo que logremos monitorizar la inmensa mayoría de la información será legítima, por lo que necesitaremos avanzar un poco más en la protección y comenzar con una detección activa. Esta detección activa se debe basar en la detección de usos indebidos y de anomalías y además debe ser un proceso automatizado.

En el caso de la detección de usos indebidos tenemos varios indicadores que nos pueden servir, como es el caso de la búsqueda de patrones, el acceso a dominios ilegítimos, uso de cuentas de correo no corporativas, etc. Estos indicadores son muy útiles no solo en nuestro caso de estudio sino también en otros muchos, como es el caso de los antivirus, las *IP-tables* o los filtros antispam del correo, pero no son perfectos y tienen en lo desconocido su talón de Aquiles.

Aquí es donde entra la detección de anomalías, la cual está ganando cada vez más peso. Esta está basada en tecnologías como los análisis estadísticos, máquinas de estados y cada vez más, inteligencia artificial basada en aprendizaje autonómico.

La otra fase donde el atacante puede dejar un rastro de su actividad es cuando comienza a actuar. En esta, se pueden tratar de utilizar las posibles órdenes destinadas a mantener la persistencia o a exfiltrar información tanto para detectar esta actividad como para realizar un análisis forense posterior con el objetivo de recopilar información. Esta detección también se puede abordar desde distintos ángulos, todos complementarios, incluyendo el análisis del tráfico entre procesos del entorno del sistema operativo, el análisis de tráficos de la red local o el uso de *honeypots*[6]. Este análisis se apoya en herramientas como son los NIDS, HIDS o detectores de anomalías similares a los expuestos anteriormente. Además, en muchos casos será importante que el programa a proteger sepa diferenciar las peticiones legítimas de las ilegítimas, por lo que deberíamos contar con alguna forma de discriminar según la fuente de la petición.

Otra forma de detectar posibles intrusiones es el análisis forense de malwares detectados y de los equipos infectados, de esta manera podemos identificar la información buscada por los atacantes y, en ocasiones, identificar al atacante (TECHINT).

El análisis forense del *malware* se debe hacer respetando un cierto orden de actuación. Antes de comenzar se debe realizar una planificación del proceso e identificar nuestros objetivos, tras esto debemos realizar la recolección de evidencias y el análisis de ellas para poder extraer no sólo datos sino también información útil. Por último, se debe realizar una correcta presentación de estas evidencias. Estas pruebas se suelen realizar sobre clonados del sistema a analizar, además, de cara a la realización de pruebas de ejecución (análisis dinámico), sería interesante realizarlas en un entorno de *sandbox*, controlando y limitando la actuación del posible programa maligno y evitando que establezca comunicaciones con el exterior.

Este proceso no te asegura detectar todos los programas malignos, dado que aún quedarían alguno que pueda puentear estas pruebas o también haber agentes durmientes o *backdoors*[7] en aplicaciones supuestamente legítimas (o incluso en el propio hardware). Aun así, puede servirnos como una primera capa de seguridad, además se puede reforzar si se revisan los foros donde se exponen los nuevos *malware* que van apareciendo (OSINT) y si se mantiene contacto con mediadores que nos informen sobre posibles amenazas contra nuestras infraestructuras (HUMINT).

[6] **Honeypot:** Los honeypots son ordenadores señuelos utilizados para atraer la atención de los ciberatacantes. Estos ordenadores están segregados del sistema principal, proporcionando una manera de desviar a los atacantes que entraron a la red o monitorizar sus actividades.

[7] **Backdoor:** Se trata de un programa que se introduce en el ordenador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario.

5. Metodología de la toma de evidencias

Ningún conocimiento humano puede ir
más allá de su experiencia.
John Locke.

Antes de empezar con este apartado, debemos hacer una matización, y es que no es lo mismo el análisis forense en una respuesta a un incidente que en un peritaje informático. En el primero de los casos, el encargado de la respuesta debe **detectar, contener y mitigar el incidente**, analizando las pruebas forenses una vez el sistema ya haya vuelto a su estado normal. En cambio, en un peritaje informático partirá de un sistema controlado, en el que se tratará de analizar el estado de este desde un entorno controlado por el informático forense.

Pese a estas diferencias, el objetivo de ambos sigue siendo el mismo: lograr **identificar posibles rastros de actividad ilegítima** o de algún evento que pueda haber causado una alteración en el correcto funcionamiento del sistema informático y tratar de identificar al responsable de existir este.

Podemos dividir las evidencias a buscar en cuatro grandes grupos según su **naturaleza** [17]:

1. **Datos volátiles**: Dependen del estado actual del sistema y engloban a servicios en activo, usuarios autentificados, procesos en uso o el estado actual de la memoria. Estos datos son muy sensibles dado que un paso en falso del forense podría sobrescribirlos.
2. **Datos no volátiles**: Estos datos están conformados principalmente por los archivos y documentos del sistema y los registros de logs de las distintas aplicaciones y servicios.
3. **Datos transitorios**: Incluyen la información localizada en memoria, siendo especialmente delicada la que se encuentra en memoria caché.
4. **Datos temporales**: Es información transitoria creada por un programa que en vez de guardarse en el espacio de memoria de este se almacena a parte y de manera temporal. Aunque deberían borrarse cuando la aplicación ya no está en uso, muchas no lo hacen.

5.1. Adquisición de evidencias

En el proceso de un análisis forense, la adquisición de las pruebas seguramente es la parte más crítica, especialmente si es un análisis en caliente (con el equipo aún encendido). En nuestro caso, lo más común es que podamos realizar este tipo de análisis al tratarse de sistemas que están siempre operativos y en los que la respuesta a incidentes cobra más fuerza.

Al realizar esta adquisición, deberemos respetar un orden, en el cual las evidencias volátiles deben ser las primeras en extraerse para así evitar que estas sean sobrescritas. Respetando esa prioridad de los datos volátiles, un posible **orden** es el siguiente [17]:

1. Registros y contenido de la memoria caché del equipo.
2. Tablas de enrutamiento de redes, caché ARP, tabla de procesos, estadística del núcleo y memoria.
3. Información temporal del sistema.

4. Datos contenidos en disco.
5. Logs del sistema.
6. Configuración física y topología de la red donde se encuentra el equipo afectado.
7. Documentos.

A partir de la información volátil substraída, podemos tratar de trazar un **mapa de los usuarios, conexiones y servicios activos** en el momento de la incidencia, por lo que intentar recuperar esta información nos sería de mucha utilidad. Además, sería importante identificar posibles elementos ocultos que puedan indicar que el sistema está comprometido, pudiéndonos encontrar en este caso en la situación más peligrosa para una Infraestructura Crítica: la **APT**.

Todos estos datos deben **recogerse sin extralimitarse ni vulnerar ninguna ley**, dado que de ser esta la situación, estos datos dejarían de ser válidos de cara a una posible investigación judicial.

De la misma manera, una vez hemos obtenido esta información, esta debe pasar por una **cadena de custodia** en la que se garantiza la integridad física y lógica de todas las evidencias. Una forma de garantizar esta integridad es mediante la aplicación de Hashes. Un **Hash** es un algoritmo matemático que convierte un bloque de información de un tamaño arbitrario en una serie de caracteres de una longitud fija que podemos utilizar para realizar una identificación prácticamente inequívoca de dicho bloque de datos [18]. Esta función hash debe ser **unidireccional** (con el resultado no se puede recrear la entrada), **resistente a colisiones** (el tiempo para localizar dos entradas con la misma salida es computacionalmente inviable) y **determinista** (una misma entrada siempre debe dar la misma salida). Actualmente, las funciones hash más utilizadas son **MD-5** y las funciones de la familia **SHA-2**.

Una vez tenemos las evidencias recogidas e identificadas, debemos buscar una forma en la que podamos manipularlas sin correr el riesgo de perderlas. Por ello, antes de realizar el análisis de las evidencias, debemos realizar una serie de **clonados** con los que trabajaremos, de manera que siempre nos quedará la copia original como una evidencia impoluta. Es preferente que este clonado se pueda hacer en un sistema apagado, de manera que no haya ningún proceso o usuario que pueda alterar su estado. Hay distintas formas de realizar este proceso de clonado, las cuales dependerán del hardware con el que contemos, del estado en el que nos encontremos el dispositivo a clonar y del sistema operativo en cuestión. Cuando este proceso de clonado esté completo, podemos revisar que todo ha ido correctamente a través de aplicar hashes otra vez, de manera que si coinciden con los de las evidencias originales, entonces podemos dar por válido el clonado. Al igual que pasaba con la copia original, cuando realizamos el proceso de clonado debemos hacerlo de manera que respetemos la legislación vigente, dado que en la información a clonar se pueden encontrar datos personales cuyo tratamiento está amparado por el Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos.

5.2. Análisis de las evidencias

Ahora que ya contamos con una copia original con las evidencias extraídas y una serie de copias de respaldo sobre las que trabajaremos, llega el momento de apoyarnos en una serie de herramientas para realizar el **análisis**. Este análisis deberá ser **lo menos intrusivo posible**, dado que no queremos corromper las pruebas. Que trabajemos con un salvavidas no significa que tengamos que actuar sin pensar.

Por último, la recolección y análisis de evidencias es un **proceso muy largo y traicionero**, en el que pueden pasar todo tipo de contratiempo o complicación. Si partimos de un análisis en caliente, el estado del equipo va a hacer que este análisis sea más o menos efectivo, además de que puede haber actores externos que nos compliquen esta labor ya sea sin querer o de manera intencionada. A parte de esto, en el proceso de análisis de evidencias nos vamos a encontrar con una gran cantidad de registros, datos y archivos, de los cuales solamente una pequeña parte tendrá información que nos pueda ser de utilidad, por lo que por muy buena metodología que aplique el informático forense, este proceso se puede alargar demasiado si no se cuenta con la cualidad más importante en esta situación: la **experiencia**.

6. Herramientas de análisis

La tecnología es un siervo útil, pero un amo peligroso.
Christian Lous Lange.

Como hemos podido ver en los capítulos anteriores, la seguridad de una Infraestructura Crítica está dividida entre la **seguridad física** y la **ciberseguridad**, la cual va ganando cada vez más peso, siendo hoy en día mucho más habitual la notificación de una ciberincidencia que la de una incidencia física. Hay muchos factores que ponen en jaque a esta ciberseguridad, pudiendo variar desde campañas de SPAM hasta las APT, las cuales suelen estar dirigidas a objetivos muy concretos y suelen contar con un gran apoyo de cara al despliegue. Para monitorizar la salud de una infraestructura a nivel de ciberseguridad, el encargado de esta deberá contar con una serie de etapas, que van desde la detección hasta la elaboración del informe tras la resolución de la incidencia y, en el medio, entrarán en juego nuestra amiga la informática forense.
Cuando se habla de realizar un análisis forense ante una ciberincidencia, este puede servirnos desde la **recolección de más pruebas** sobre cuántos dispositivos están infectados y cuáles son, hasta el **indicarnos los vectores de ataque utilizados** y tratar de establecer una **traza de las actividades realizadas** por el atacante dentro de nuestra red. Para realizar tanto una cosa como la otra, este encargado deberá contar con su propia caja de herramientas, de manera que, dependiendo de si quiere buscar información a través de un elemento o de otro, pueda hacerlo.
Como hemos comentado en la Introducción, la **utilidad de este trabajo** reside en el poder **presentar una serie de herramientas que les puedan servir** a informáticos forenses para realizar su trabajo, por lo que se podría decir que este capítulo es el que engloba la parte más importante del mismo. En las siguientes páginas, trataremos de presentar algunas herramientas que puedan servir de cara a la confección de su propia caja, mostrando también alguna de las suites de herramientas y distribuciones de análisis forense más completas y utilizadas. Debido al número y a la diversidad de estas herramientas, al final del trabajo incluiremos una serie de **tablas con las herramientas tratadas** en este capítulo.

6.1. Criterios de clasificación

Antes de comenzar con este apartado, nos gustaría recordar que la informática avanza a pasos agigantados, de manera que todo intento de guía se suele quedar desfasado en tiempos récord. Aun así, los puntos que vamos a comentar en este apartado llevan existiendo de manera estable bastante tiempo, por lo que confiamos en que, aunque dentro de dos o tres años puede que las herramientas dejen de tener soporte o salgan otras mejores, al menos quede claro lo que buscamos en una herramienta de análisis forense y que estas no son excluyentes entre sí, sino que pueden funcionar perfectamente como distintos engranajes de la misma maquinaria.

Para realizar esta clasificación, vamos a apoyarnos en los capítulos previos, siendo uno de los apartados las herramientas de **clonado**, con las que podremos realizar copias de las evidencias y así no ensuciar la escena del crimen. Como en la respuesta a incidentes también tendremos ocasión de realizar análisis en caliente, necesitaremos alguna herramienta de **volcado de la**

memoria volátil y la RAM, además de otra que nos muestre el **estado del sistema en tiempo real**, del registro del sistema operativo y que **vigile la actividad potencialmente peligrosa de los usuarios**. Es importante contar también con herramientas que nos permitan la **monitorización del tráfico de la red** y el uso de este que hacen las distintas aplicaciones.

Una vez pasamos a los datos más fríos, es imprescindible usar alguna herramienta que **analice las propiedades de los archivos** (file carving y análisis de metadatos) y que nos permita **recuperar información borrada**. A nivel de archivos de **log**, estos se pueden revisar a mano, pero si contamos con herramientas que nos acelere este proceso, mejor. En esta etapa tampoco nos podemos olvidar de la red, por lo que tendremos que buscar alguna herramienta que nos ayude con la **detección de intrusiones** (IDSs y HIDSs). Paralelamente, es bastante probable que nos veamos en la necesidad de utilizar alguna herramienta para **recuperar contraseñas**.

Además, al estar tratando con Infraestructuras también debemos añadir herramientas de **gestión de incidencias** y repasar las que nos ofrece el **CCN-CERT** ya que nos pueden ayudar. Si echamos la vista atrás, podemos ver que esta lista no difiere tanto de la que se nos presentó en *CCN-STIC 811 – Interconexión en el ENS*.

6.2. Metodología del análisis de las herramientas

Para la selección de las herramientas que vamos a incluir a continuación nos hemos basado en las recomendaciones que hemos encontrado en libros [17][19], en páginas oficiales [20][21] y en herramientas utilizadas a lo largo de la carrera en asignaturas como *Seguridad en redes y sistemas informáticos* o *Ciberseguridad en dispositivos móviles*. La información mostrada a continuación será extraída por orden de prioridad, de la **documentación oficial** de las distintas herramientas, de la **ejecución** de estas, **tutoriales** y **demostraciones de uso** en el caso de que no sea una herramienta accesible para el público general y de distintos artículos o blogs donde se hayan probado o donde se exponga opinión más detallada sobre la **experiencia de los usuarios** con ellas [22][23]. Además, la fuente de información principal dentro de cada herramienta será incluida junto con un listado de algunas características clave en una **tabla final que servirá de resumen** de lo expuesto a continuación.

Por último, el modelo de resumen que realizaremos se basará en una descripción del tipo de herramienta a tratar, una breve **descripción de la herramienta** comentada, un resumen de sus **ventajas e inconvenientes** y una breve **conclusión** sobre su posible adaptación en el entorno de las Infraestructuras Críticas. En los casos de las herramientas más completas o complejas, enfatizaremos en su descripción la parte que la defina más, ya sea su modo de uso, su forma de actuar para lograr su propósito o alguna característica que la diferencie de las demás.

6.3. Herramientas de clonado

Comencemos por el principio. Para realizar la adquisición de las pruebas, el ingeniero forense deberá realizar un clonado del disco o los discos comprometidos o donde se haya producido el problema. Para ello, se deberá realizar una **copia completa** de estos. Esta copia se puede realizar a través de la red, realizando una copia de todos los archivos a través de *ssh*, pero por lo general es preferible realizar una copia *offline* para agilizar el proceso y reducir posibles sabotajes en el proceso.

- **Upcopy**

Upcopy es una herramienta de línea de comandos disponible para dispositivos Windows de 32 y 64 bits. Esta herramienta permite copiar todos los archivos de un directorio origen a uno destino permitiendo tanto la recursividad (no solo copia las carpetas, sino también el contenido de estas) como especificar los archivos a copiar (tanto por nombre como por última modificación). Esta última funcionalidad le da una doble utilidad: sirve como una **herramienta de clonado** y como **actualización de copias** o *backups*[8].

Entre las ventajas de esta herramienta tenemos que **permite revisar el hash** tanto del archivo origen como del destino y que acepta nombres de ficheros de hasta 32.767 caracteres, lo cual evita problemas si tenemos una larga cadena de carpetas una dentro de otra. A su vez, es una herramienta se puede **ejecutar desde un dispositivo externo**, de manera que permite realizar el clonado sin realizar instalación alguna y sin tener que apagar o parar el sistema a clonar. Además, es **gratuita** y solamente ocupa **312 KB**.

Como desventajas de esta herramienta estarían el que no realiza el clonado de archivos que están bloqueados para su ejecución o archivos temporales que referencian a un archivo abierto. Además, **no realiza un clonado de todo el espacio de memoria**, sino solamente del sistema de archivos, por lo que dependiendo del análisis que se quiera realizar, esta copia podría llegar a no servirnos.

Como conclusión, upcopy es una herramienta eficaz y con muchas opciones para la ejecución del comando, **recomendable si estás trabajando en un dispositivo que realiza copias de respaldo con frecuencia** o si requieres que el clonado se realice rápido. Como contraparte, el que no pueda copiar memoria dinámica, archivos abiertos o archivos eliminados hace que haya **otras herramientas más completas** que según el caso **te puedan salir más rentables de usar**. Aunque el uso de suits o aplicaciones más completas puede ser preferente, si buscas solamente una herramienta para realizar un clonado rápido y eficaz de los archivos a analizar, upcopy es una buena opción.

- **FTK Imager**

FTK Imager es una herramienta gratuita creada por la compañía AccessData. Como principal funcionalidad, FTK Imager permite la **creación de imágenes forenses exactas**, copiando toda la información del disco **bit a bit**. Funciona en las tres principales familias de sistemas operativos y es una herramienta poco invasiva, al funcionar desde dispositivos externos.

Entre las ventajas de esta herramienta tenemos que el clonado es una **copia exacta del dispositivo original**, respetando tamaños de archivos y espacios y el contenido de las direcciones sin asignar, lo que permite que la imagen resultante **pueda servir como evidencia en un peritaje informático**. Además esta herramienta **genera un hash de la imagen creada** cuando el proceso de clonado se ha completado, lo que permite evaluar su integridad en todo momento. Entre otras funcionalidades, FTK Imager permite **realizar previsualizaciones** de archivos y directorios, permitiendo también visualizar todo el contenido e la imagen desde el navegador web Internet Explorer, también permite **exportar archivos y capetas** desde la imagen creada. Además, AccessData cuenta con una solución completa para el análisis forense

[8] **Backup:** La copia de datos en forma de backup ayuda a la recuperación de la información en el caso de que esta se pierda o dañe. Es recomendable realizar copias de seguridad periódicas de todos los datos importantes y mantener estas en un medio externo o en la nube.

llamada Forensic Toolkit (FTK), por lo que puedes formar un tándem completo y compatible al que solamente le tendrías que ajustar alguna aplicación de tus preferencias de así requerirlo.

Como desventaja más notable nos encontramos con que los algoritmos que utiliza para realizar el hash de la imagen son **algoritmos bastante vulnerables** (MD5 y SHA-1), el tiempo del clonado también puede ser una desventaja, dado que aunque es un programa que ha mejorado notablemente sus prestaciones en velocidad de creación de imágenes, el mecanismo utilizado sigue siendo **bastante lento**. Por último, también es recomendable el uso de bloqueadores de escritura para evitar **posibles interferencias con el sistema operativo**.

Como conclusión, FTK Imager es una buena herramienta de clonado que permite realizar una imagen completa del disco a analizar (incluyendo la memoria volátil). Esto hace que, aunque sea una opción más lenta, si lo que se quiere es un duplicado exacto, esta pasa a ser **una muy buena opción**. Una buena solución sería **combinar esta herramienta con otras más veloces** que realicen copias menos exhaustivas, de manera que cuentes con una primera copia del dispositivo original que sea exacta y posteriormente, para analizar el sistema de archivos o realizar ciertas comprobaciones como puede ser un análisis dinámico, puedes utilizar otras herramientas de clonado más rápidas.

- **DDrescue**

Como solución alternativa contamos con DDrescue, una herramienta del proyecto GNU que tanto se puede ejecutar por comandos como a través de una interfaz gráfica de usuario. La principal finalidad de DDrescue es la **recuperación de información de una unidad dañada**, realizando una copia de un dispositivo comenzando por la parte que permanece en buen estado y continuando con los archivos o espacios de memoria que estén dañados.

Entre las principales ventajas que tiene DDrescue se encuentra el ser **parte del proyecto GNU**, de manera que está integrada con una gran cantidad de herramientas del sistema, está **muy bien documentada** y mantiene una retroalimentación continua con los usuarios. Además, de tener **más de una copia** distinta del mismo dispositivo, DDrescue permite que estas **converjan solucionando posibles errores** que se puedan dar en ellas. DDrescue utiliza también un sistema de copia basado en el mapa de archivos, de manera que permite la pausa y reanudación de la copia sin tener que volver a empezar o sin tener que realizar grandes comprobaciones de por medio.

Entre las principales desventajas contamos con que es una herramienta de Linux, por lo que aunque haya alguna librería que pueda ayudar a que esta se ejecute desde otros sistemas operativos, por defecto esto no será así. Además, esta herramienta, al igual que upcopy **no realiza un clonado en profundidad**, sino que solamente copia el sistema de archivos y los que puedan estar dañados, dejando atrás los espacios de memoria sin información teóricamente vacía. Además, la que seguramente es la desventaja más grande es que **el disco a clonar debe estar desmontado** para evitar posibles problemas, lo cual no siempre va a ser posible.

Como conclusión, DDrescue es una herramienta que, **combinada** con otras herramientas del propio sistema (dd, hash, etc.) **puede ser de gran utilidad**. En cualquier sistema es bastante habitual contar con copias de respaldo, por lo que una Infraestructura Crítica no debería ser menos (o más bien debería ser aún más común), por lo que esta herramienta nos puede ayudar a la hora de analizar las copias de respaldo recuperando información que se encuentre dañada.

6.4. Herramientas de volcado de memoria volátil

En el apartado anterior hemos tratado con la copia o clonado de una unidad de memoria, presentando herramientas que permiten recuperar desde el sistema de archivos hasta los espacios de memoria que no están siendo utilizados. Pero hay una parte de la información que se queda atrás; la **información volátil**. En muchos casos, en una Infraestructura Crítica es posible el análisis en caliente de una incidencia, siendo necesario recuperar la información volátil antes de nada. Para realizar esto, el informático forense deberá volcar la información almacenada en memorias no persistentes, como es el caso de la RAM, las caché o la tabla de procesos del sistema.

- **Dumpit**

Dumpit es una herramienta de **volcado de RAM** que resulta como una evolución de win32dd y win64dd, funcionando **en sistemas Windows** de 32 y 64 bits indiferentemente. Para usar esta aplicación, puedes ejecutarla directamente desde un disco extraíble haciendo doble clic en ella o a través de comandos si quieres hacer uso de alguna funcionalidad en concreto. Una vez ha realizado el volcado, genera un documento en crudo en el mismo directorio donde se encuentra el ejecutable.

Entre sus principales ventajas se encuentra la **facilidad de uso**, ya que es una herramienta que no requiere una gran preparación, simplemente se ejecuta y obtienes el resultado, además al exportar el **resultado** en un formato *.dmp*, este es algo **más ligero** que la salida en formato *.mem* o *.raw*.

Entre los puntos negativos tenemos que la versión completa es de pago, vendiéndose con el pack completo de MoonSols desde 190USD (155,91€) si no se contrata soporte hasta 7.500USD (6154,50€) si se contrata soporte y licencia ilimitada. La última versión gratuita disponible está solamente abierta para 32bits, mientras que la versión para 64bits disponible ya está en desuso por la empresa [24]. Por último, aunque el tiempo de volcado no es demasiado grande, esta herramienta es **la que más tiempo tarda** entre las demás presentes en este apartado.

Como conclusión, a nivel de una organización, dumpit es una **herramienta bastante útil**, dado que te permite realizar un volcado rápido de la memoria RAM y posteriormente con otras herramientas de este toolkit puedes analizar su resultado. En cambio, en el caso de que seas un particular, toolkit puede resultar bastante cara o quedarse pequeña la versión gratuita, **habiendo soluciones mejores** en ambos casos.

- **Volatility**

Quizás una de las herramientas más conocidas en este campo, Volatility es un software colaborativo, administrado por la Volatility Foundation. Esta herramienta está **basada en Python**, haciendo que sea multiplataforma, siendo posible utilizarla en dispositivos Windows, Linux, Mac o incluso Android. A su vez cuenta con una gran variedad de comandos que se le pueden pasar por argumentos.

Entre las distintas ventajas, encontramos que es un software con **licencia GPLv2**, es decir, que puedes extender sus funcionalidades libremente si quieres. Cuenta con **una gran variedad de opciones** de uso que incluyen análisis de uso de recursos de red, información del sistema, procesos activos, procesos del núcleo, detección de rootkits[9] y más, haciéndola una herramienta

[9] **Rootkit**: Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los propios normalmente). Este tipo de software no es malicioso en sí mismo, pero

muy completa y versátil. Entre las funcionalidades con las que cuenta, Volatility permite ampliar las acciones que realiza el depurador del núcleo de Windows, como son la creación de estructuras de datos de red o la creación de historiales de comandos. Además, cuentan con una **gran documentación** detrás y una **comunidad muy activa** en la respuesta a los problemas expuestos en su página de github [25].

Como desventajas podemos mencionar que al ser una aplicación que no tiene ningún organismo o empresa detrás, la **asistencia a incidencias no está garantizada**, siendo probable que en el foro antes comentado te puedan ayudar pero sin la garantía de ello. Además, al igual que en todos los proyectos colaborativos, algún miembro puede tratar de introducir vulnerabilidades a propósito como ha pasado recientemente con el núcleo de Linux [26].

En conclusión, Volatility es una de las **herramientas de volcado** y análisis de memoria volátil **más versátiles del mercado**, siendo posible utilizarla en cualquier sistema operativo que permita instalar sus dependencias (Python y poco más). Además, al contar con una licencia GPLv2, si desde la Infraestructura Crítica a analizar requiere algún cambio en su funcionamiento o una revisión del código para evitar posibles amenazas, ambos procesos serían posibles, por lo que no habría ningún problema en utilizar esta herramienta.

- **Magnet RAM Capture**

Al igual que las herramientas antes analizadas, el capturador de memoria volátil de Magnet es una herramienta de **volcado de RAM** ejecutable **sin necesidad de instalación**. Está disponible para sistemas Windows de 32 y 64 bits desde XP hasta Windows 10.

Esta herramienta comparte muchas características con DumpIt, aunque con las ventajas de que es ligeramente **menos invasiva y más rápida** y que mantiene el soporte sobre la versión gratuita, de manera que esta se mantiene actualizada. Otra ventaja de esta herramienta es que **permite cambiar el formato del resultado**, teniendo la opción de archivos .dmp, .raw o .bin. Además, cuenta con otras

Entre las contras encontramos que **requiere de otras herramientas para realizar el análisis** del archivo resultante, además, entre las herramientas disponibles hay otra que tiene mejores prestaciones.

Como conclusión, Magnet RAM Capture es una **herramienta útil** para el volcado de memoria volátil, **pero no es la mejor disponible**. Aún así, de tener complicaciones con Volatility o con la próxima herramienta a comentar, esta es una buena alternativa a ellas.

- **Belkasoft Live RAM Capture**

Continuando con las herramientas corporativas, las soluciones Belkasoft son de las más utilizadas a nivel institucional en países como Estados Unidos, Canadá o Australia. Al igual que en las herramientas antes comentadas, en este caso Live RAM Capturer **no requiere de una instalación** para funcionar, desde un dispositivo extraíble (o desde el propio equipo) se puede ejecutar la herramienta y en cuestión de unos pocos minutos generará un documento *.mem* analizable posteriormente por la solución principal de la compañía, B. Evidence Center X. Por ello, aunque la herramienta en sí es gratuita, la solución completa de adquisición y análisis no lo es, variando su precio según la configuración requerida.

---

es utilizado por los piratas informáticos para esconder evidencias y utilidades en los sistemas previamente comprometidos.

A la hora de comparar Live RAM Capturer con sus competidores, nos encontramos con que es la que **requiere menos espacio en memoria RAM**, de manera que solamente sobrescribe menos de 2MB por los 8MB o 12MB de otras herramientas [27]. A su vez, también permite el **capturar información protegida**, al correr bajo el modo administrador, siendo capaz de evitar medidas antidepuradores y antivolcados.

Como punto negativo, contamos con que esta herramienta aunque permita realizar un volcado gratuito de la memoria RAM, no es una solución completa, sino que **depende de Evidence Center X para poder realizar el análisis** de los resultados.

Para concluir, Belkasoft Live RAM Capturer es una herramienta que funciona correctamente, dando un **resultado casi óptimo y rápido**. Como las Infraestructuras Críticas suelen depender o de empresas o de organizaciones gubernamentales, el precio de la licencia no sería un problema para adquirirla y se obtendría una asistencia técnica en caso de problemas con la herramienta. Si esta asistencia no es una prioridad para el encargado, **esta alternativa continuaría por detrás de Volatility** debido a la mayor variedad de funcionalidades que proporciona la herramienta gratuita.

6.5. Herramientas de monitorización del sistema y usuarios en tiempo real

Una vez hemos capturado la información volátil del sistema a analizar y hemos realizado un clonado de este para poder comenzar las pesquisas sin correr el riesgo de alterar las pruebas originales, llega el turno de analizar la **información temporal**. Esta información está compuesta por distintos tipos de datos, incluyendo archivos de log, archivos de configuración del sistema, archivos de actividad de los usuarios y registros del sistema. A continuación veremos tres herramientas de **monitorización del sistema** y una tercera de **lectura de la configuración** del dispositivo a analizar.

- **Intella W4**

Intella W4 es una solución forense que **guarda un resumen de todas las acciones realizadas** en un período de tiempo estipulado **por los usuarios del sistema**, aportando estadísticas y gráficas de estos y permitiendo al ingeniero forense revisar estos datos desglosándolos por su autoría.

Entre los datos que esta herramienta almacena están incluidos:

- **Datos del sistema**. En este apartado incluyen los sistemas operativos, usuarios, sesiones y los registros de eventos de Windows.
- **Programas**. Incluye no sólo los programas instalados sino un registro de cada vez que se ejecuta uno de ellos y el registro de los programas que se ejecutan automáticamente al iniciar el equipo.
- **Dispositivos**. Incluye dispositivos USB, actividad de los dispositivos USB, interfaces de red, conexiones de red activas e interfaz bluetooth.
- **Archivos y carpetas**. Incluye archivos y carpetas que muestran información sobre la actividad reciente del usuario (modificaciones, movimientos y creaciones) y elementos borrados.

- **Buscadores**. Incluye información sobre el historial, cookies[10], formularios rellenados, descargas, inicios de sesión y marcadores.
- **Elementos y programas notables**. Incluyen elementos de un interés particular, como son los elementos encriptados, imágenes con etiquetas de geolocalización, emails con información de geolocalización, la papelera de reciclaje y los archivos descargados de internet. Como programas, incluye las aplicaciones de torrents, criptomonedas, accesos a la darknet[11] y accesos remotos.
- **Dispositivos móviles**. Incluye si se ha conectado a dispositivos móviles, datos de geolocalización y otros dispositivos móviles.
- **Comunicaciones**. Incluyen mensajes de correo, aplicaciones de mensajería, llamadas registradas, contactos, citas del calendario y otras comunicaciones.
- **Documentos y media**. Incluye distintos tipos de documentos, desde archivos de ofimática hasta imágenes, vídeos, audios y documentos varios.
- **Información de traspasos**. Incluye información sobre qué accesos se han realizado a través de dispositivos USB, de internet o del correo y qué información se ha compartido entre el elemento externo y el equipo.
- **Etiquetas y palabras clave**. Incluye etiquetas que puede crear el usuario de esta aplicación y palabras clave a rastrear.

Esta información se desplegará en un panel a su vez dividido en tres partes: el panel principal donde se mostrará la información seleccionada, un panel inferior que mostrará la línea temporal de los eventos seleccionados y un panel lateral donde se puede cambiar la forma de representar la información (lista, árbol, imágenes o elementos geolocalizadores), también puedes crear gráficos, ver el árbol de las acciones realizadas, abrir aplicaciones que contengan información relacionada, guardar los datos. Además, al **permitir la selección múltiple** de elementos a visualizar, **podemos relacionar los eventos del sistema con su autor**, estableciendo así una traza de la actividad de cada usuario en cada conexión realizada.

Como podemos ver, las principales ventajas de esta aplicación es la **gran cantidad de actividades realizables**, teniendo mucha información que es captada en tiempo real pero a su vez **bien organizada**, de manera que no se vuelve una tarea imposible el localizar los eventos que nos interesan para realizar el análisis. Además, la herramienta **permite realizar gráficos y exportar la información** que se seleccione para así facilitar la creación del informe posterior.

Como contraparte negativa, encontramos que esta solución solamente está disponible para entornos Windows y para sistemas en la nube, SaaS o sistemas web. Además, las **acciones modificables por el usuario son muy limitadas**, haciendo que no puedas desplazarte mucho más allá del esquema de análisis predefinido.

Como conclusión, Intella W4 es una **solución que considerar** para una gran empresa o una Infraestructura Crítica, teniendo una **interfaz bastante intuitiva y una buena organización** de los distintos eventos.

[10] **Cookies:** Es un fichero de texto que, en ocasiones, se envía a un usuario cuando éste visita una página Web. Su objetivo es registrar la visita del usuario y guardar cierta información al respecto

[11] **Darknet:** Red de superposición (es decir, una red construida sobre otra red, en este caso, Internet) que no es detectable por métodos normales y solo se puede acceder haciendo uso de software especializado como Tor. Las Darknets están diseñadas para preservar la privacidad de quienes las usan.

- **IBM QRadar SIEM**

Esta herramienta permite al usuario que monitorice las actividades de distintos servidores y equipos, siendo una herramienta para Windows pero que puede monitorizar otro tipo de sistemas operativos. QRadar se sitúa a caballo entre este apartado y el siguiente, realizando un seguimiento de los eventos detectados en los sistemas y a su vez **rastreando las direcciones IP** y la información asociada a dichas comunicaciones potencialmente maliciosas.

El principal objetivo de esta solución es la **monitorización de los eventos del sistema para identificar posibles ataques y poder avisar** de estos. En la descripción de las incidencias incluye un grado de peligrosidad, una descripción de la incidencia mencionando los eventos sospechosos involucrados en ella, el número de eventos y flujos creados, las direcciones IP involucradas, un resumen del usuario afectado, una serie de tablas con información que puede añadir el usuario a modo de notas y otras tablas con la información antes indicada expuesta de una manera más detallada. Desde la pestaña de alertas se puede acceder a un **resumen de los eventos sospechosos**, dividiéndolos según el tipo de evento, de manera que se filtra la información según la gravedad o fecha, localizando así el origen de la intrusión. Dependiendo de la manera que tenga el atacante de realizar el primer contacto, esta aplicación mostrará distinta información, incluyendo en todas la dirección IP origen y una geolocalización de esta. En esta lista de eventos, también se muestra el número de instancias de cada evento, permitiendo detectar si estos sucedieron de una manera demasiado condensada (lo que indicaría un posible ataque semiautomatizado). Seleccionando la información de las direcciones que intervienen en los eventos se puede ver una evaluación del riesgo de estas.

Pero esta herramienta no se queda en el análisis del peligro del atacante, si en vez de acceder a la información de los eventos potencialmente peligrosos nos centramos en el **elemento atacado**, se nos desplegará una lista de los ataques que ha recibido este elemento, indicando también su criticidad. Desde el menú de eventos también se puede realizar un filtrado por las direcciones IP, pudiendo seleccionar una determinada dirección IP destino para ver cuántos eventos potencialmente maliciosos se han dirigido a ese sistema o usuario y establecer una traza de estos. En el caso de que se detecte una posible IP maliciosa, se puede tratar de aislarla para evitar que realice más acciones, además, se puede realizar una comprobación de qué otros usuarios o sistemas estuvieron en contacto con este actor malicioso.

A nivel de estadísticas IBM QRadar proporciona también un **panel de análisis**, en el que se nos presentan los usuarios monitorizados, el número de eventos potencialmente peligrosos, una lista de los usuarios y una valoración del riesgo de estos, una lista de las últimas amenazas detectadas con información desglosada, un resumen del estado de los modelos de detección de amenazas y una serie de gráficas que resumen el resto de la información comentada.

Esta solución tiene las ventajas de que es una **herramienta muy completa**, que engloba todo tipo de evento que pueda causar problemas al sistema, realiza un **seguimiento en profundidad** de los elementos que son potencialmente maliciosos y tiene una buena organización de las estadísticas de riesgos. Además, el **filtro de los eventos** potencialmente dañinos lo realiza **mediante modelos de Machine Learning**[12], por lo que si detecta un comportamiento que siga un patrón similar a un evento malicioso, aunque sea un ataque nuevo que no esté registrado en su lista de ataques conocidos, lo podría detectar.

[12] **Machine Learning:** Rama de la inteligencia artificial que consiste en utilizar conjuntos de datos para entrenar algoritmos. Al analizar las soluciones que se dan a un gran número de problemas similares, los sistemas informáticos comienzan a identificar patrones y ofrecer soluciones a tales problemas.

Como lado negativo os volvemos a encontrar que es una **solución muy cerrada**, sin opciones a que el usuario la personalice según busque unas características más concretas y **no cuenta con una gran documentación**.

Como conclusión, esta herramienta aporta un **mecanismo de detección y notificación de incidencias bastante bueno**, que mejora con el uso debido a su sistema de detección de amenazas no basado en patrones y aunque no cuenta con los mejores gráficos **realiza un análisis muy detallado del posible origen de la incidencia** por lo que su propósito lo cumple perfectamente.

- **Magnet Axiom**

Al igual que con las herramientas anteriores, Magnet Axiom presenta una solución a la **recopilación de evidencias**, pudiendo seleccionar los archivos que incluir en este análisis y permitiendo la evaluación de sistemas remotos, locales, dispositivos de memoria y servicios en la nube. También **cuenta con una inteligencia artificial** que ayuda al forense a detectar posibles anomalías en las pruebas seleccionadas, lo que mejora las capacidades de búsqueda que suelen ser habituales en una persona.

Desde el menú inicial, se nos presenta un resumen del último caso analizado, en el que el investigador puede presentar sus apuntes del caso, ver un listado de las fuentes de evidencias, acceder a la bitácora del procedimiento realizado, acceder a la información analizada por la inteligencia artificial, ver un resumen de las evidencias disponibles según su categoría y acceder a un listado de perfiles, palabras clave y contraseñas de usuario localizadas. Toda esta información depende de las fuentes seleccionadas, de manera que si añades más, se modificaría la información.

El **proceso de selección de evidencias** es **muy intuitivo**, teniendo un esquema jerárquico de las fuentes de datos, de manera que si se quiere acceder a los datos de mensajería de una herramienta web concreta, basta con seguir los pasos de buscar en la nube, seleccionar dicha herramienta y dentro de esta seleccionar la familia de elementos de interés que se busca. Además, en el mismo menú se puede definir una serie de palabras clave y elementos que nos gustaría que la inteligencia artificial detectase (caras en fotos, indicios de acoso en conversaciones, archivos con ciertas características, etc.). Una vez el forense cuenta con los elementos deseados, puede acceder a ellos y revisarlos de manera individual, estableciendo marcas sobre ellos para categorizarlos según el interés para el caso o colocar las pruebas en un grafo con las relaciones entre ellas. Toda la información utilizada como evidencia está clasificada según su tipo de archivo, utilizando también sus metadatos para permitir establecer una línea temporal de los distintos archivos.

Las principales ventajas de esta herramienta es que permiten una **gran gama de fuentes de adquisición**, siendo una herramienta realmente útil cuando se requiera realizar un peritaje o un análisis de una incidencia; tiene **varias formas de analizar la información y exportar el resultado**, haciendo este proceso algo más abierto que en los casos anteriores; por último, al poder seleccionar el forense los documentos que entran en la investigación**, se realiza un filtrado de los datos** que estén amparados por la ley orgánica de protección de datos, evitando posibles negligencias en el caso de que esas pruebas sean requeridas en un juicio posterior.

Como contraparte negativa, contamos con que, como **la selección de la información a analizar se realiza a mano**, el forense se puede dejar más información atrás que con las otras

herramientas, además, en esta solución, el análisis del origen de la incidencia no entra tan en profundidad como en el caso de la herramienta anterior.

En conclusión, entre las distintas opciones vistas hasta ahora, esta es la herramienta que deja más campo de actuación al investigador, siendo una **buena opción para los casos en los que este cuente con** la **experiencia y conocimiento** necesarios para que el análisis termine en buen puerto. Si la Infraestructura Crítica cuenta con un buen proceso de selección para este trabajo, Axiom le permitirá tener una mayor libertad de actuación, pero en cambio si se apuesta más bien por responsables de menos experiencia o sin una especialización clara en el ámbito de la ciberseguridad, esta solución le puede quedar demasiado genérica siendo más recomendable alguna de las herramientas comentadas anteriormente en este mismo apartado.

- **Windows Registry Recovery**

Entre los analizadores menos automatizados, destaca Windows Registry Recovery, el cual nos permite realizar una **búsqueda de aquella información temporal y de configuración de la máquina analizada**. Esta herramienta está disponible para sistemas Windows de 32 bits y de 64 bits.

WRR cuenta con trece **exploradores** distintos, que se pueden clasificar según sus características en:

- **Explorador de archivos**. Evalúa las propiedades y hashes de los archivos básicos del sistema.
- **Elementos de seguridad del sistema**. Incluye el análisis de los registros de seguridad y del SAM (*Security Account Manager*, Administrador de cuentas de seguridad de Windows). El primer explorador muestra características de seguridad de los usuarios, listas de claves, permisos de acceso e intentos de acceso, todo esto indicando las marcas y permisos. En segundo realiza una labor similar con el SID de la máquina y los usuarios y grupos con acceso al SAM.
- **Elementos del sistema**. Incluye los exploradores de la configuración del sistema, de las variables de entorno, del hardware conectado y de las carpetas shell. En este grupo se encuentran las visualizaciones de la información del sistema, del software instalado y del hardware conectado y las variables de entorno del equipo. Toda esta información vendría detallada incluyendo datos de accesos al sistema, inicios, apagados y en general toda la información que podamos relacionar con la configuración del equipo. Además se incluye un explorador para el caso de las carpetas de perfil de usuario o carpetas Shell.
- **Aplicaciones y servicios**. Incluye los exploradores de aplicaciones de inicio y de servicios y *drivers*[13]. Estos muestran una lista de aplicaciones que se ejecutan automáticamente en el arranque del sistema y otra lista con servicios instalados y disponibles y los *drivers* instalados. Entre los servicios disponibles se menciona aparte el caso de Outlook, que es el buzón de correo por defecto en Windows.
- **Configuración en red**. Incluye exploradores de la configuración de red y de la configuración del cortafuegos. En este grupo podemos encontrar los clientes web instalados, protocolos utilizados y servicios disponibles, indicando el tipo de conexión

[13] **Driver:** Es un programa, conocido como controlador, que permite la gestión de los dispositivos conectados al ordenador (generalmente, periféricos como impresoras, unidades de CD-ROM, etc).

que utilizan y su configuración TCP/IP. También se muestran las reglas que se aplican en el cortafuegos

- **Información en crudo**. Este buscador realiza un listado de todos los registros disponibles en una estructura de árbol según se localicen los archivos. Al contener todos los datos de los registros, es el explorador más completo pero también el que aporta una información más densa.

Entre las ventajas que tiene esta herramienta encontramos la **simplicidad**, dado que realiza lo que se le solicita, sin más complicaciones, de manera que si el investigador forense sabe lo que quiere buscar, con esta herramienta lo puede conseguir directamente. Además, al ser una **herramienta externa** permite realizar un análisis de los registros con una menor probabilidad de que el resultado esté alterado por un posible software malicioso.

Entre las desventajas contamos con que al ser una **herramienta muy sencilla**, si el investigador forense prefiere utilizar pocas herramientas pero muy potentes, esta aplicación desentonaría con su objetivo buscado. Además, al ser una herramienta **orientada al sistema de gestión de registros de Windows**, no serviría para realizar una búsqueda de evidencias en un servidor o terminal con un sistema operativo distinto a los creados por dicha empresa desarrolladora.

En conclusión, de cara a un **análisis** centrado en la configuración de un sistema **Windows**, Windows Registry Recovery es una **alternativa útil y rápida**, diseñada para extraer un conjunto concreto de datos para un análisis posterior de estos. Si lo que se busca es una solución que analice los datos y cree informes sobre estos, como estuvimos viendo en las demás herramientas, esta se quedaría corta, pero si en vez de una solución forense se busca una herramienta simple y directa, WRR puede ser muy útil.

6.6. Herramientas de análisis de la red

Entre las posibles acciones que puede realizar un software malicioso está la **exfiltración de información** y el Mando y Control (C&C). En ambas situaciones, el *malware* deberá hacer uso de los recursos de red para poder enviar o recibir información, por lo que será necesario realizar una **monitorización del tráfico de red** para comprobar que no se han producido conexiones ilegítimas o que no se han activado falsos recursos web camuflados para realizar la exfiltración. A continuación, vamos a comentar de una manera algo más extendida las dos herramientas más utilizadas para este propósito: tcpdunp/WinDump y Wireshark.

- **Tcpdump/WinDump**

La primera herramienta que analizaremos es tcpdump, la cual está disponible para todas las distribuciones Unix, incluyendo MAC OS. También cuenta con una adaptación para sistemas Windows llamada WinDump, que utiliza las librerías de software libre Winpcap [28]. Esta es una de las **herramientas más completas y eficaces para el rastreo de redes**, permitiendo una gran variedad de parámetros y filtros que se aplican a bajo nivel.

El principal objetivo de tcpdump es la **monitorización del tráfico de una red**, pudiendo poner el foco sobre una red o aplicación en concreto para realizar un análisis más personalizado sobre las posibles amenazas.

El primer paso de esta monitorización se realiza a través de la aplicación de opciones. Como el total de estas opciones asciende hasta las **62 opciones**, vamos a comentar solamente algunas de las más usadas, pero están todas disponibles en su *man page* [29].

- **-A**. Imprime cada paquete recibido en ASCII. Útil para capturar el tráfico de páginas web.
- **-c** *count*. Termina el rastreo tras recibir *count* paquetes.
- **-D**. Imprime una lista de las interfaces de red disponibles sobre las que se puedan capturar paquetes aportando una pequeña descripción de estas. Otro alias de esta opción es ***--list-interfaces***.
- **-e**. Imprime la cabecera de nivel de enlace en cada línea volcada. Útil para identificar direcciones MAC.
- **-i** *interface*. Selecciona una interfaz en concreto para monitorizarla. Si no se especifoca, el programa seleccionará la interfaz activa del sistema con un identificador más bajo, excluyendo la interfaz *loopback*. Otro alias para esta opción es ***--interface***=*interface*.
- **-n**. Imprime las direcciones (de red, host o puerto) en formato numérico, sin convertirlas a un significado verbal.
- **-#**. Numera los paquetes incluyendo esto al comienzo de la línea mostrada. Otro alias para esta opción es ***--number***.
- **-r** *file*. Utiliza el archivo file como fuente de entrada. Esta opción nos ayuda analizar los paquetes guardados con *-w*.
- **-tt**. Incluye en paquete volcado un timestamp en segundos desde la medianoche del 1 de enero de 1070 UTC, también incluye fracciones de segundo desde esa misma fecha.
- **-v**. Imprime el resultado de las capturas en un formato verbalizado. Es muy útil combinado con -w para facilitar posteriores revisiones.
- **-w** *file*. Escribe la información capturada de los paquetes (tras aplicarles las demás opciones y filtros) en vez de imprimirla por la salida estándar (línea de comandos).
- **-XX**. Imprime las cabeceras de cada paquete capturado (incluyendo la cabecera a nivel de enlace) en formato hexadecimal y ASCII.

Como podemos ver, hay una gran variedad de opciones, y es muy importante tener cuidado en cómo se usan, dado que no es lo mismo -w que -W (establece un número máximo de archivos creados) ni -t (no imprimir el timestamp) que -tt o que -ttt (imprimir el tiempo transcurrido entre la recepción de ese paquete y el anterior). Estas opciones **suelen combinarse también con un conjunto de filtros**. Hay tres clases de **primitivas** de filtrado, las cuales son **heredadas de pcap-filter**. Estas clases son combinables entre ellas, y son las siguientes [30]:

- **De tipo**. Permiten filtrar según quieras identificar **máquinas** (*host*), **redes** (*net*) o **puertos** (*port* y *portrange*).
- **De direcciones**. **Especifican las direcciones** origen (*src*) o destino (*dst*) de los paquetes a inspeccionar. Estas direcciones son combinables mediante operadores *or*, *and* y paréntesis, y de incluir solamente una dirección se entiende por defecto *src or dst*. Para las redes IEEE 802.11, se incluyeron también las expresiones *ra*, *ta*, *addr1*, *addr2*, *addr3* y *addr4*.
- **De protocolo**. Indican el **protocolo a capturar**. Algunos protocolos disponibles son: *tcp*, *udp*, *decnet*, *ip*, *ip6*, *ether*/*fddi*/*tr*/*wlan* (distintos alias para *ether*, que filtra paquetes de nivel de enlace), *arp* y *rarp*.

A su vez, estas expresiones también son combinables con el uso de los operadores lógicos de negación (! y not), concatenación (&& y and) y alternancia (|| y or), con paréntesis, con las primitivas opcionales ([ ]) y or exclusivo (|) y con los términos *gateway* (*true* si la puerta de enlace indicada ha sido usada), *broadcast* (*true* si es un mensaje de difusión), *less* y *greater* (*true* si el tamaño del paquete es menor/mayor del tamaño indicado).

Como hemos podido ver, esta herramienta es muy completa, ofreciendo **una gran variedad de funcionalidades distintas**, lo que permite que puedas modificar el funcionamiento de tcpdump según se prefiera realizar una captura más profunda sobre un rango menor de paquetes o capturar el máximo número de estos sin centrarse demasiado en su contenido. En el caso de detectar una vulnerabilidad y querer analizar si una aplicación está enviando mensajes ilegítimos a través de la red, una solución sería ejecutarla en un espacio de pruebas controlado (una máquina virtual, por ejemplo) sin conexión a la red externa y con tcpdump analizando los paquetes que envía dicha aplicación.

Como conclusión, son muchas las ventajas de utilizar tcpdump/WinDump en el análisis forense de una red, al ser una herramienta bastante eficaz al aplicar los filtros a bajo nivel, con una gran variedad de opciones y expresiones combinables entre sí, al ser una herramienta de línea de comandos es bastante liviana y además es gratuita y multiplataforma, con la única desventaja de que al no contar con una GUI, este análisis se puede hacer más laborioso, aunque si lo que se desea es un análisis más visual, se puede combinar con la herramienta que veremos a continuación para que el análisis pase a realizarse con ella. Dadas sus ventajas, **esta herramienta debería estar siempre presente entre las conocidas por el informático forense** si se quiere saber qué está pasando (y qué ha pasado) en la red a analizar.

- **Wireshark**

El proyecto Wireshark es quizás la herramienta de análisis de paquetes de red más utilizada a nivel global, convirtiéndose en **un estándar en esta materia**. Esta herramienta está disponible en la mayoría de las distribuciones basadas en Unix (incluyendo Mac OS) y en Windows, funcionando tanto a través de una interfaz gráfica (GUI) como a través de línea de comandos.

Entre sus principales usos están:

1. Analizar y solucionar los **problemas de red**.
2. Examinar posibles **vulnerabilidades de seguridad**.
3. Verificar el **funcionamiento** en red **de distintas aplicaciones**.
4. **Depurar las implementaciones de protocolos** al desarrollar aplicaciones.
5. Aprender el funcionamiento interno de los protocolos de red.

En nuestro caso, tanto el segundo como el tercer uso serán lo que nos lleven a utilizarlo.

A su vez, lo que nos interesa es realizar un análisis forense a partir del resultado de la monitorización de las redes, por lo que a continuación vamos a ver cómo Wireshark nos puede ayudar.

La primera funcionalidad del análisis que nos puede servir con Wireshark es la propia **interfaz principal**, la cual está dividida en tres paneles:

- **Panel del listado de paquetes**. En este se identifican los distintos paquetes resultantes de la aplicación de los filtros (o todos los paquetes capturados), indicando verbalmente el número de secuencia del paquete, su marca temporal (relativa al comienzo de la captura), las direcciones origen y destino, el protocolo utilizado, la longitud del paquete capturado e información adicional sobre este. El color de la línea también nos va a proporcionar información añadida, ya que este varía de color según el tipo de mensaje que es, pasando también al negro cuando el paquete pertenece a un flujo erróneo. Por último, en este panel podemos observar como se relacionan los paquetes entre sí,

apareciendo una serie de símbolos que indican qué paquetes forman parte de una misma conversación (indicando además tanto el primero como el último), si hay algún paquete que se cuela en el medio de la conversación pero no pertenece a esta, los mensajes de petición y respuesta, si se trata de un mensaje ack, si se trata de un ack repetido o si el paquete seleccionado está relacionado con otros paquetes de alguna manera.

- **Panel de detalles del paquete**. En este panel se realiza una traza de la pila de protocolos utilizados en el paquete seleccionado, indicando con mayor detalle el contenido de cada apartado y sus características. Wireshark también indica si se ha generado alguna información extra sobre dicho protocolo o qué otros paquetes están relacionados con este a través de dicho protocolo.
- **Panel de Bytes**. En este último panel, se muestra la secuencia de Bytes recibidos dentro del paquete seleccionado, mostrando a su lado la codificación ASCII de estos. En el caso de que el protocolo utilizado no realice una encriptación o codificación del mensaje, este se podrá ver en claro en este panel. Además, según se seleccione un protocolo u otro en el panel anterior, la parte correspondiente a dicho protocolo se remarcará en azul, sabiendo así donde comienza y donde acaba cada cabecera y el contenido útil enviado.

Otra de las funcionalidades para el análisis que nos permite Wireshark es la **aplicación de distintos filtros** a través de un lenguaje de alto nivel. Para realizar este filtro, se puede acceder al menú opciones e introducir el filtro desde la captura o aplicarlo desde la ventana principal para que así no se realice un filtro del tráfico a capturar (esto ya se ha realizado previamente), sino solamente de los paquetes que queremos filtrar para localizarlos. Como único apunte sobre el proceso de captura de paquetes, desde el menú opciones Wireshark permite establecer condiciones para la creación de documentos de salida, de manera que se le puede dejar programado para que exporte la información a un documento cuando se haya alcanzado un cierto tamaño (en paquetes o en cantidad de información) o cada cierto tiempo. De esta manera podemos dejar distintas capturas de manera que se dividan la tarea y que a la hora de realizar el análisis forense posterior podamos tener separadas las capturas según el protocolo, host, red o puerto.

Para realizar **filtros de visualización**, Wireshark cuenta con una gran variedad de opciones, teniendo distintos tipos de filtros:

- **Operadores de búsqueda y comparación**. Permiten filtrar los paquetes según ciertos términos, direcciones o valores de sus distintos campos. Esto puede realizarse según se busque una coincidencia exacta (matches y ~) o según se incluya dentro de dicho campo (contains).
- **Filtros de protocolos**. Hay más de 261.000 filtros incluidos en este apartado, pudiendo utilizar para el cribado tanto identificadores como direcciones o valores de campos. Los protocolos que se pueden utilizar engloban los distintos niveles de la pila de protocolos, siendo los más útiles para nuestra causa: eth, wlan, ip, icmp, arp, tcp, udp, dns, smtp y dhcp [31].
- **Pcap-filtres**. Al igual que tcpdump, Wireshark también puede hacer uso de los filtros incluidos en la librería pcap-filtre y combinarlos con los demás de esta lista.
- **Operadores de cortes**. Estos operadores permiten realizar divisiones en los filtros si estos hacen referencia a cadenas de texto o a vectores de Bytes.

- **Operadores a nivel de bit**. Al igual que en el caso de los campos, también es posible realizar filtrados según ciertos valores a nivel de bite. Estos filtros se suelen utilizar en conjunción con los operadores de corte o con filtros según campos de los protocolos.
- **Expresiones lógicas y de comparación**. Para establecer relaciones entre filtros podemos hacer uso de operadores de comparación (igualdad, desigualdad, mayor que, menor que, etc.), operadores lógicos (AND lógicos, OR lógicos y NOT lógicos) y operadores de membresía, en los que se puede incluir una serie de valores entre los que se les aplicará un OR lógico entre ellos.

Estos filtros pueden definirse desde el menú Análisis, dejándolos guardados para utilizarlos en otras ocasiones. Desde este menú también se pueden activar o desactivar protocolos, decodificar paquetes y utilizar las trazas de los paquetes para reproducir gráficamente flujos de las conversaciones en TCP, UDP, TLS y HTTP.

Por último, también disponemos de un **menú Estadísticas**, que nos presenta de una manera resumida y gráfica información sobre los filtros, resolución de direcciones (como o hace un servidor DNS), el árbol de jerarquía de los protocolos aplicados, tablas de conversaciones entre determinados terminales, qué terminales han formado parte de las conversaciones capturadas y con qué protocolo, estadísticas sobre los paquetes recibidos, gráficas del tráfico de la red tanto entrante como saliente, gráficos de flujos de conversaciones, estadísticas de os servidores DNS utilizados, y muchas más estadísticas que varían según el protocolo utilizado. El total de las estadísticas disponibles no llega a los números de los filtros aplicables, pero continúa siendo bastante más amplio del que podemos englobar en este punto, por lo que si quieren saber más, en la guía de usuarios de Wireshark indican más información al respecto [32].

Además de estas dos herramientas, hay **otros rastreadores** de tráfico web bien valorados y con interfaces gráficas como son **Telerik Fidder** [33] y **NetworkMiner** [34]. Ambas son multiplataformas, con la diferencia entre ellas de que la primera es instalable en el sistema y la segunda es un ejecutable externo. NetworkMiner cuenta con una versión gratuita y con una versión de pago (900USD, aproximadamente 740€). Estas herramientas pueden servir como alternativas o complementos a las dos anteriormente expuestas, aunque esas ya cubren un gran abanico de funcionalidades y están disponibles para las tres grandes familias de sistemas operativos.

6.7. Herramientas de detección de *malware*

Una vez hemos analizado la información volátil y temporal, podemos pasar a realizar un análisis del software que se encuentra en nuestro dispositivo. Este análisis permitirá detectar una serie de **patrones de comportamiento o de código** catalogados como maliciosos. Estos mecanismos de detección de *malware* no son fiables en su totalidad, dado que un virus que utilice patrones desconocidos o que ofusque su código de una manera que no se pueda identificar el patrón no será detectado como tal. Aun así, es un buen método de filtrado de código malicioso.

- **YARA**

YARA es una **herramienta de creación de reglas** basadas en patrones textuales o binarios que se juntan formando expresiones lógicas evaluables. El formato de estas reglas es muy sencillo, tienen una declaración que las identifica y un cuerpo compuesto por tres partes:

- ***Meta***. Información explicativa de la herramienta, indica **información añadida** de la regla aunque no tiene efecto directo sobre su funcionamiento. Es **opcional**.
- ***Strings***. **Definiciones de variables** para utilizar en las condiciones. Puede estar formado por expresiones regulares, por cadenas de texto, por cadenas hexadecimales e incluir modificadores o condicionales. Esta parte también es **opcional**, aunque de incluirse sí tiene efecto sobre el funcionamiento de la regla.
- ***Condition***. **Expresión booleana** por evaluar, es la parte que **indica si se cumple o no la regla**. Puede tener referencias a strings, realizar iteraciones, comparaciones, aplicar condiciones, referenciar a otras reglas y más. Esta es la única parte **obligatoria** de la regla.

YARA también permite definir **reglas privadas** o crear **módulos** referenciables.

Para hacer uso de las reglas YARA, basta con llamarla desde la línea de comandos indicando la regla que se quiere aplicar y el archivo, carpeta o proceso a evaluar. Si se quiere evaluar más de una regla, en vez de indicar la regla en sí, se le puede **pasar uno o varios archivos con las reglas**, de manera que se aplicarán todas de manera secuencial. Esto se puede hacer con la opción -C. También cuenta con otro comando llamado ***yarac***, el cual **compila las reglas** para que estas puedan ser aplicadas correctamente. Si no se quiere aplicar la totalidad de las reglas localizadas en esos archivos se puede indicar que solamente se apliquen si contienen una cierta etiqueta (*-t tag*) o un cierto identificador (*-i id*). YARA además cuenta con más opciones que también la hacen bastante moldeable por el investigador forense [35].

Como **ventajas** de esta herramienta tenemos su **ductilidad**, haciéndola idónea para investigadores experimentados; muchas herramientas de detección de *malware* aplican las reglas yara en sus búsquedas, de manera que **se pueden localizar distintas fuentes** de reglas que sirvan como referencia para la creación de otros (o para ser aplicadas).

Entre as desventajas podemos contar con que se trata de un **sistema de detección basado en patrones**, por lo que es vulnerable a ofuscaciones del código y a amenazas aún no identificadas. Otra desventaja para tener en cuenta es que si el usuario no está acostumbrado a tratar con sistemas de creación de reglas, la programación y comprensión de las reglas YARA se le puede hacer muy cuesta arriba.

Como conclusión, esta es una herramienta muy potente, cuya efectividad dependerá principalmente de la pericia del responsable de ella. Respecto a las Infraestructuras Críticas, esta herramienta puede servir como un **filtro inicial**, aplicado sobre algún sistema que posea Linux y que pueda servir **como parte de la seguridad perimetral**. Aun así, esta herramienta no se puede entender como una solución única, dado que ya hemos comentado las limitaciones con las que cuentan los sistemas de detección basados en reglas.

- **rkhunter/chkrootkit**

Continuando con las herramientas de línea de comandos, en este apartado disponemos de dos **detectores de rootkits pasivos** diseñados para una **aplicación posincidente**. Ambas herramientas están disponibles en entornos Unix (incluyendo Mac OS). Aunque se les suele mencionar juntos, en realidad actúan de maneras distintas:

- ***rkhunter***: utiliza como pista la **comparación de hashes**, la **búsqueda de directorios** comunes para la presencia de virus, la presencia de **permisos incorrectos**, **archivos**

ocultos, **cadenas sospechosas** y algunas pruebas concretas según la distribución sobre la que se aplique.

- ***chkrootkit***: realiza una **amplia gama de comprobaciones** que van desde el análisis de las interfaces web para detectar programas en modo promiscuo hasta la búsqueda de coincidencias con cadenas de código malicioso o búsqueda de actividades ilegítimas típicas en malwares. Actualmente tiene registrados setenta y un virus distintos que son capaces de detectar.

Ambas herramientas es recomendable que se ejecuten de manera externa al disco a analizar para prevenir la interferencia de agentes maliciosos, aunque también pueden ser aplicados desde un sistema seguro sobre todos los elementos que entren nuevos en el sistema. De esta última forma perderían algo de eficacia (no tendrían una manera de revisar la actividad de los elementos sospechosos), pero funcionarían como parte del sistema de prevención de amenazas.

Como principales **ventajas** de estas herramientas contamos que son **gratuitas** y **fácilmente aplicables**. Entre las dos realizan una **alta gama de pruebas**, de manera que si lo que se está utilizando para atacar o sabotear nuestro equipo es una amenaza ya conocida, estas utilidades de línea de comandos pueden ayudarnos a identificar la amenaza.

Como principales **puntos negativos** contamos con que el mecanismo que utilizan para detectar los rootkits es el **uso de patrones de código y de comportamiento**, de manera que si el virus utiliza alguna metodología nueva, si aplica una mayor ofuscación del código o si hace uso de varios ejecutables distintos y aparentemente aislados, enredando así su comportamiento, estas herramientas lo tendrán muy difícil para detectarlos.

Como conclusión, a la hora de detectar un a amenaza, la aplicación de distintas herramientas de localización de *malware* es una buena idea. Por ello, las dos herramientas expuestas aquí pueden ayudar al investigador forense a realizar un **filtro de posibles virus menos complejos**. Nuestra recomendación con estas herramientas es que si se tiene la sospecha de que el sistema está infectado con un software malicioso, el forense puede hacer uso de un dispositivo externo al disco comprometido para analizar este y realizar así un primer filtro, que a continuación se debería completar con la aplicación de otras herramientas de análisis forense.

- **IDA hex-rays**

Cambiando un poco lo visto hasta ahora, IDA es una herramienta propietaria de análisis de *malware*. Esta utiliza un **proceso de desensamble y una posterior depuración** para tratar de realizar el análisis posterior sobre un código lo menos ofuscado posible. Actualmente está disponible para sesenta y ocho familias distintas de sistemas operativos, incluyendo las principales distribuciones y dispositivos móviles.

Cuando se le pasa un ejecutable a IDA, esta trata primero de desensamblarlo para identificar sus partes internas y su código máquina. De tener un sistema de ofuscación que imposibilite esto (por ejemplo, mediante el uso de direcciones irresolubles por la herramienta, importaciones rotas o saltos a ninguna parte), el usuario puede realizar una ejecución controlada a mano. Para esto, el programa es altamente recomendable que se esté ejecutando en una máquina virtual o en un entorno *sandbox* (si un archivo es sospechoso de actuar maliciosamente, nunca se debe ejecutar sobre un equipo de uso corriente, ya que podría infectarlo todo).

Al comenzar esta ejecución, IDA permite **visualizar el flujo de actividad** del programa, mostrando de manera visual las alteraciones en la línea de ejecución y si estas convergen en una

salida o si tienen varias posibles maneras de terminar su ejecución. Sabiendo esto, el investigador puede establecer una serie de *breakpoints* para analizar el estado del sistema al terminar la ejecución de esa parte del código. En el caso de que parte del código esté dispuesto en zonas de memoria en las que no es posible realizar modificaciones (por ejemplo, zonas con permiso de sólo lectura), no se podrían colocar *breakpoints* en estas líneas. La información que se obtenga de este análisis **puede ser exportada** de manera directa a una base de datos de IDA o a través de la ejecución de scripts.

Como principales **ventajas** podemos mencionar que esta herramienta **permite** (si se dispone de la licencia de pago) **realizar modificaciones en su código**, siendo así adaptable a las preferencias del cliente. Otra ventaja importante es el que **representen gráficamente el flujo** de la actividad, de manera que ayuda a comprender mejor los programas ofuscados con una alta complejidad en el uso de saltos y referencias a otras partes del código.

Por el contrario, esta herramienta es un **analizador del *malware* semiautomático**, de manera que según la complejidad del programa se podría dar el caso de que el investigador se encuentre ante una versión de pago de un depurador como puede ser el GDB.

Como conclusión, esta herramienta **aporta una manera distinta** a las antes vistas **de analizar el código** de un programa potencialmente malicioso, resolviendo el problema en el mejor de los casos y siendo un entorno gráfico de depuración en el peor.

- **Hijackthis**

Para terminar con este apartado, contaremos con una herramienta de **análisis de comportamientos sospechosos**. El objetivo de *hijackthis* es identificar todas aquellas acciones y modificaciones que suelen ser utilizadas por los softwares maliciosos para llevar a cabo su propósito. Esta herramienta **no indica si un programa es maligno o benigno** ni desinstala o aísla ningún proceso, sino que crea un registro de la actividad detectada que presentará en forma de documento de texto y que el investigador puede revisar en busca de comportamientos anómalos. Por ejemplo, si el sistema cuenta con una calculadora instalada y esta herramienta detecta que la calculadora solicita la apertura de sockets de red, incluirá esto en su lista de actividades sospechosas, pero será responsabilidad del investigador el revisar si este socket se utiliza para actividades legítimas o si es un indicio de un comportamiento malicioso.

El modo de empleo de esta herramienta es muy sencillo, realizando un **análisis del sistema** según solicite el usuario y mostrando una **lista de actividades detectadas** que se podrá utilizar tanto como referencia para una investigación más detallada de cada caso (esta lista es exportable) como para seleccionar elementos que se desee que dejen de actuar.

Como puntos **positivos** esta herramienta cuenta con su **velocidad en la detección** de las actividades, centrándose en los métodos que se aplican y no en cadenas de texto. También presenta funcionalidades extra como son la **posibilidad de quitar servicios de arranque**, **desinstalar programas o eliminar archivos** que el usuario considere. *Hijackthis* no funciona como un juez, solamente aporta información al usuario sin realizar ningún juicio sobre la legitimidad de las acciones detectadas, de manera que trata de no condicionar hacia ningún lado al usuario.

Como **contraparte negativa** tenemos que al no diferenciar entre actividades legítimas e ilegítimas se puede considerar que su **tasa de falsos positivos es altísima**, de manera que el análisis de su resultado puede resultar muy complejo si el investigador forense es inexperto y no

tiene un conocimiento detallado de qué características y actividades son comunes en un programa o qué procesos forman parte del funcionamiento del propio sistema operativo.

Como concusión, esta herramienta puede ser **de gran utilidad** en un sistema en el que el responsable del análisis de los eventos sea una **persona con experiencia**, ya que proporciona una respuesta rápida de qué está pasando en el equipo analizado, dando pistas de posibles actividades sospechosas. Además al tratarse de una herramienta portable, se puede utilizar desde dispositivos externos al comprometido.

6.8. Herramientas de detección de intrusiones

Pero la legitimidad de una acción no depende solamente de la aplicación que la lleva a cabo, sino también del usuario que la ejecuta. En toda empresa u organización es común encontrarnos con distintos rangos de permisos, estando la mayoría limitados a ciertos grupos de profesionales. ¿Qué pasaría entonces si una persona externa o interna ejecuta un programa en el sistema de dicha organización cuando no debería tener acceso? En el caso de que esto suceda, estaríamos en un contexto de una **intrusión informática** en la que se está haciendo uso de una escalada de privilegios para lograr realizar actividades ilegítimas. Para filtrar dentro de un sistema las acciones que realizan los usuarios legítimos de los demás, contamos con una familia de herramientas conocidas como los **sistemas de detección de intrusiones** (IDS, por sus siglas en inglés), que a su vez pueden especializarse en las intrusiones en red (Net IDS o NIDS) o a nivel del sistema (Host IDS o HIDS). A continuación veremos algunas de las herramientas más recomendables para dicho propósito.

- **SNORT**

SNORT es una herramienta de software libre que funciona como un híbrido entre un **sistema de detección de intrusiones** (IDS) y un **sistema de prevención de intrusiones** (IPS). Su principal objetivo es la **identificación de amenazas a través de la red**, generando una alerta manejable por el usuario del sistema. También puede realizar tareas de prevención adaptando sus reglas de detección a reglas de IPtables.

La **base** del correcto funcionamiento de SNORT está en **sus reglas**, si el usuario incluye un buen conjunto de estas realizando filtrados sobre páginas web indeseadas, descargas de archivos no autorizadas o conexiones con servidores desconocidos, se puede llegar a obtener un buen conocimiento de la actividad ilegítima de la red perimetrada, reduciendo los falsos positivos y dejando solamente falsos negativos que provengan de situaciones anómalas que no estén reconocidas como maliciosas.

SNORT tiene tres **modos de funcionamiento**, los cuales son complementarios entre sí:

1. Modo **rastreador**. **Lee** los paquetes recibidos **y los muestra** por pantalla.
2. Modo **registrador de paquetes**. **Crea entradas de log** con los paquetes que va recibiendo.
3. Modo **NIDS**. Realiza una **detección y análisis del tráfico** de la red.

Los dos primeros modos son aplicables mediante el uso de las opciones *-v* (verbose) y *-l* (logs). Para activar el tercer modo, que es el que nos interesa, se utiliza la opción ***-c*** y se le pasa un **archivo de configuración** que incluya una referencia a las **listas con las reglas** que se utilizarán para el análisis de la red. También se le puede especificar un host concreto a monitorizar, de manera que se puede aplicar este sistema de detección sobre elementos

concretos como pueden ser los servidores o los equipos utilizados por las áreas más críticas de la empresa.

Una de las cosas que caracterizan a SNORT es que **las reglas están abiertas**, de manera que cualquier usuario o empresa que se instale esta herramienta por primera vez no tendrá que pasar por el tedioso proceso de crear una regla para cada elemento que quieran filtrar, sino que probablemente **la inmensa mayoría de estos elementos ya tendrán una regla creada** [36].

El **formato** de las reglas es el siguiente [37]:

- **Acción**. Indica la **medida a tomar** si se cumple la condición. Puede ser de alerta (*alert*), registro (*log*), ignorar el paquete (*pass*), rechazar el paquete (*drop*), eliminar el paquete (*reject*) o eliminar el paquete sin generar registro de este (*sdrop*). También se pueden crear tipos de acciones con *ruletype*.
- **Protocolo**. Es el **protocolo sobre el que actuará** la regla. Puede ser: IP, ICMP, TCP, UDP, HTTP, …
- **Dirección origen**. **Par IP-Puerto del origen** del mensaje. También puede ser del destino si es una regla bidireccional. Puede indicar direcciones internas como externas a la red monitorizada.
- **Sentido del paquete**. Indica el **sentido de aplicación** de la regla. Puede indicar una dirección única (`->`) o ser bidireccional (`<>`).
- **Dirección destino**. **Par IP-Puerto a la que va dirigido** el paquete. En el caso de una regla bidireccional también puede funcionar como dirección origen.
- **Cuerpo**. Añade **condiciones de detección y otra información adicional** como prioridades, mensajes a mostrar o metadatos. Esta parte va entre paréntesis y los distintos elementos contenidos se separan con un punto y coma.

La gran flexibilidad que ofrecen las condiciones del cuerpo permite que las reglas sean muy adaptables a distintas situaciones, permitiendo realizar rastreos por contenido del cuerpo, por datos de la cabecera, por direcciones IP, …

Los **puntos a favor** de esta herramienta son la **versatilidad** que ofrece, la gran **variedad** de reglas, la presencia de **centenares de miles de usuarios** que ayudan a actualizar las reglas y la herramienta, que permite realizar un **reenvío de las alertas** a un dispositivo que pueda ejercer de centralizador de los avisos y que es **aplicables tanto para una red, como para un dispositivo concreto o para una aplicación** de este.

Como **punto negativo** contamos con la **potencial complejidad** que pueden alcanzar las reglas de SNORT. Una mala organización a la hora de guardarlas o una actualización de estas sin prestarle atención a los cambios puede generar que los archivos de configuración pasen a ser documentos de decenas de miles de líneas sin una comprensión clara por parte del administrador de la herramienta. Otro punto en su contra es que si se aplica sobre una red muy concurrida con demasiadas reglas o reglas demasiado genéricas, **puede ocasionar un efecto embudo**, reduciendo la velocidad de la red interna y pudiendo llegar a causar problemas de funcionamiento.

Como conclusión, SNORT es una de las mejores herramientas de detección de intrusiones en red, permitiéndole una gran flexibilidad al usuario y contando con una gran cantidad de reglas aplicables para la monitorización y detección de eventos en red inesperados. Respecto a su aplicación en Infraestructuras Críticas, esta herramienta **podría ayudar a la detección de**

actividades maliciosas si se aplica correctamente **sobre elementos claves** de la arquitectura de red, como pueden ser las subredes de los departamentos más críticos o los servidores con acceso al exterior.

- **Suricata**

Si antes nos encontrábamos con que SNORT es prácticamente un estándar entre los sistemas de detección de intrusiones en red (NIDS), con Suricata nos encontramos a otra gran herramienta que comparte muchas características con SNORT pero que también les **añade funcionalidades y una interfaz de usuario** a través de la cual se puede extraer información parametrizada.

Lo primero que nos puede llamar la atención de esta herramienta es que su funcionamiento está basado en el uso del **mismo formato de reglas de SNORT**. En este caso, utiliza las creadas por Emerging Threats [38] como la fuente por defecto, aunque también permite descargar nuevas reglas desde otras fuentes como puede ser Oinkmaster [39]. A pesar de esto, hay una diferencia muy importante entre estas dos herramientas: mientras SNORT es originalmente un proceso de un solo hilo, Suricata es **multihilo**, de manera que mejora las prestaciones de su competidor en sistemas que tengan varios núcleos [40]. Como apunte a esto, a partir de la versión 3.0, SNORT ha comenzado a aplicar un procesamiento multihilo al análisis de paquetes.

Algunas de las **diferencias** que podemos encontrar entre Suricata y Snort son [41]:

- Procesos multihilo.
- **Uso de la tarjeta gráfica para analizar el tráfico** más rápidamente.
- Permite **aislar y estudiar los documentos detectados** como *malware*.
- Uso del **motor de scripting LuaJIT**.
- Uso de una **Interfaz gráfica de Usuario**.

La **principal ventaja** de esta herramienta es la **usabilidad**, al contar con una interfaz gráfica que permite visualizar con gráficos y números los avisos y los eventos que han sucedido. Además, hasta hace no mucho presentaba una gran ventaja en **rendimiento** respecto a SNORT, aunque con la nueva versión y la conversión a la programación multihilo, esta diferencia se ha reducido.

Como **desventajas** podemos incluir que, aunque Suricata tiene una **comunidad** bastante activa detrás, **sigue sin llegar a los niveles de su competidor**, de manera que de producirse algún cambio de tendencia en las reglas o en los patrones a buscar para filtrar virus, es probable que SNORT le lleve la delantera.

Como conclusión, el único motivo por el que no sería recomendable utilizar Suricata es que ya se esté utilizando SNORT, y viceversa. Por lo general es una **herramienta con muy buenas prestaciones y un rendimiento que la ha colocado como la única competencia estable** del que hasta ahora es el estándar de los NIDS. Aun así, si la infraestructura a monitorizar no cuenta con ningún NIDS, puede ser una buena idea incluir Suricata en vez de SNORT para permitir que el administrador de estas herramientas cuente con una interfaz más amigable que la que ofrece la línea de comandos.

- **OSSEC**

Cambiando el campo de análisis de las redes a los terminales, también nos podemos encontrar con herramientas muy útiles para la detección de intrusiones. Este es el caso de OSSEC, un

HIDS (Host IDS) que permite la **monitorización de múltiples sistemas a través de una arquitectura centralizada**. Esta arquitectura se divide en tres **partes**:

- ***Manager***. Es la **pieza central del sistema**, funcionando como el servidor. **Almacena la base de datos** de los registros de integridad de los archivos, **registros** de logs, **eventos**, un **registro de las auditorias** al sistema, además de las herramientas para su correcto funcionamiento como son las **reglas, decodificadores y archivos** de configuración. Se comunica con las demás partes con un tráfico UDP.
- ***Agents***. Los agentes son pequeños **programas instalados en los sistemas a monitorizar**. Su principal tarea es recoger información (en tiempo real o periódicamente) y trasladarla al *manager* para que desde ahí sea analizada.
- ***Agentless***. El "sin agente" es la **parte encargada de monitorizar sistemas donde no se pueda instalar el agente**. Generalmente estos sistemas son cortafuegos, rúters e incluso algunos sistemas Unix.

Como se puede observar, OSSEC es capaz de monitorizar tanto sistemas terminales de usuarios como una gran variedad de los demás elementos que conforman la arquitectura de red e incluso máquinas virtuales, transmitiendo toda esa información y análisis posterior al dispositivo del encargado de realizar la monitorización.

Entre las funcionalidades de OSSEC, podemos destacar el **análisis** de archivos **de log en tiempo real**, la **detección** de distintos tipos **de softwares maliciosos**, el **uso de scripts para la aplicación de una defensa activa**, la realización de **auditorías del rendimiento** según distintos estándares y *benchmarks*, el **control de la integridad de archivos y registros** a través de firmas y copias forenses y la **realización de inventarios del sistema** donde se incluyen tanto dispositivos hardware, como aplicaciones o distintas métricas de uso.

Entre las **ventajas** de esta herramienta contamos con su **gran variedad de acciones** realizables, la integración de distintas herramientas especializadas y de software libre para la realización de los análisis, una monitorización centralizada que permite una administración más rápida de las alertas y una comunidad muy activa.

Como **contraparte negativa** tenemos que al ser un **sistema centralizado** puede dar problemas de escalabilidad de encontrarse con una gran densidad de eventos a analizar. Además, en la versión gratuita no cuenta con una interfaz gráfica al uso y en la versión comercial esta interfaz solamente está disponible para dispositivos basados en la nube o con un sistema operativo Windows.

Como conclusión, OSSEC permite realizar un control centralizado de esos componentes de la arquitectura de red que no es fácil que tengan a un experto en ciberseguridad observando su comportamiento de manera continuada, por ello, nos parece una muy buena herramienta de monitorización. **Seguramente, el mejor HIDS del mercado**.

6.9. Herramientas de análisis de archivos

En apartados previos hemos visto cómo sacar información de utilidad a partir del análisis del comportamiento y del código de las aplicaciones y archivos, pero no es la única fuente de información que estos nos dan, también se puede obtener a partir de otras partes de estos. Cuando se crea o modifica un archivo se deja un rastro en forma de metadatos, que son una serie de **características del archivo** como la fecha de creación, el autor o en el caso de las

imágenes, la geolocalización de dónde se ha realizado. Estos metadatos nos pueden proporcionar información sobre una posible exfiltración de información o sobre un mal uso del sistema por parte del usuario. Las primeras herramientas que mostraremos en esta lista están orientadas al **análisis de los metadatos** de los archivos, mientras que la última es una herramienta de Unix que permite **identificar la verdadera extensión del archivo** a analizar (lo que es conocido como *file carving*).

- **FOCA**

FOCA es una herramienta de extracción de metadatos creada en 2008 por informática64 (actual ElevenPaths) y migrada a un proyecto OpenSource en 2017. Es quizás la herramienta de análisis de metadatos más conocida en nuestro país, contando con versiones de pruebas de penetración (Pentesting Driven By FOCA), de análisis de redes IPv6 (Evil FOCA) y de análisis forense (Forensics FOCA). FOCA permite el análisis de multitud de archivos, incluyendo documentos localizados en páginas web, PDF y documentos de ofimática tanto de Microsoft Office como de Open Office.

Desde FOCA se puede realizar un **escaneo de los metadatos de archivos y carpetas** de una manera rápida e intuitiva, basta con seleccionar la opción de análisis de metadatos, añadir archivos, carpetas o una URL a partir de la que obtener los archivos y extraer los metadatos de estos. Tras esto, en el árbol de archivos aparecerán los recién analizados con la información obtenida a partir de sus metadatos. Este análisis de los metadatos **se puede realizar sobre páginas web**, de manera que se analizarían todos los documentos disponibles en esta. A partir de esos documentos descargados, se puede realizar un análisis para sacar información de la organización o, en nuestro caso, revisar que no se esté exfiltrando ninguna información que pueda haber sido usada para realizar un ataque o que sirva para esconder información privada de la organización. FOCA además realiza búsquedas en el contenido tratando de sacar más información (por ejemplo enlaces, correos o datos perdidos) de la que de por sí se encuentra en los metadatos.

Como podemos ver, esta aplicación cuenta con una funcionalidad bastante sencilla en lo que respecta al análisis de metadatos, pero es más que suficiente para realizar lo que se requiere de ella: analizar los metadatos de una gran variedad de documentos.

Entre las **ventajas** encontramos lo anteriormente comentado, además, cuenta con una **gran documentación** detrás, habiendo seminarios y libros destinados a funcionar como una guía para el uso de esta herramienta.

Como **punto negativo**, podemos mencionar que esta herramienta está más bien orientada a la realización de un rastreo de huellas para una **posterior prueba de penetración**, por lo que, aunque nos puede servir para realizar un análisis forense de la información almacenada en estos documentos, esta no sería su función principal.

Como conclusión, si en el proceso del análisis forense de la Infraestructura Crítica se requiere el análisis de documentos sospechosos o de posibles exfiltraciones de información a través de técnicas de ocultamiento en documentos, se puede hacer uso de esta herramienta, permitiendo descubrir información importante sobre la creación de estos documentos.

- **Libextractor**

Al igual que DDrescue, *libextractor* se trata de una iniciativa del proyecto GNU que engloba al comando *extract* y a la librería en C *extractor.h*. Es capaz de **interpretar los metadatos de más**

de cuarenta formatos distintos, incluyendo documentos, archivos multimedia, documentos comprimidos, documentos situados en páginas web y páginas web. Esta herramienta ha sido diseñada en un inicio para ejecutarse por comandos en sistemas GNU/Linux, pero actualmente ya está disponible para otras distribuciones Unix (incluyendo Mac OS) y Windows.

Este comando cuenta con las siguientes opciones: ***-b*** (muestra el resultado en formato BiBTeX), ***-g*** (salida adaptada a posibles concatenaciones de comandos), ***-h*** (ayuda), ***-i*** (lanza procesos complementaros en procesos separados), ***-l*** (usa las librerías que se indiquen a continuación), ***-L*** (lista los metadatos conocidos), ***-n*** (no usa los extractores por defecto, sino los indicados con *-l*), ***-p*** (muestra solamente los metadatos que coincidan con el tipo indicado), ***-v*** (indica la versión), ***-V*** (muestra el resultado con un texto más extendido) y ***-x*** (excluye metadatos con el tipo que se especifique a continuación).

Entre las **ventajas** que tiene esta herramienta de extracción de metadatos podemos encontrar que tiene una **gran variedad de formatos** analizables y que es muy **rápida** y con pocas dependencias.

Entre las **desventajas** contamos con que no son todos los formatos posibles y que la **búsqueda de los metadatos no es muy profunda**, de manera que se puede dejar algunos atrás.

Como conclusión, en el caso de tener la posibilidad de analizar el documento con FOCA, es preferible realizarlo, aunque si ese formato no está relacionado con la ofimática y no te lo reconoce, *libextractor* es una buena solución.

- **Foremost**

Para terminar con las herramientas de este apartado, pasamos a analizar el tipo de archivo, en vez de los metadatos de este. Recientemente se ha alertado de un tipo de ataque bastante común; el *spare phishing*[14][15] con documentos Excel falsos [42]. Este ataque consiste en enviar un correo realista a una persona de una empresa u organización e incluir un supuesto Excel con información para que sea descargado. El truco de este ataque es que el Excel no es tal, sino que es un ejecutable al que en el nombre le incluyeron un ".excel", y como las extensiones por defecto en Windows están desactivadas, el usuario piensa que es una tabla de datos normal y corriente.

Este es solamente un ejemplo posible de cómo se puede ocultar el formato de un documento. El ***file carving*** se encarga de **detectar** si tenemos **algún archivo malicioso escondido** en el medio de otros documentos legítimos o de **recuperar la información perdida sobre la extensión de un documento** que antes se encontraba en el dispositivo.

Foremost es una herramienta de comandos desarrollada para entornos GNU/Linux cuyo principal objetivo es la **recuperación de archivos a partir de información oculta en ellos**. Además, a través de la ejecución con la opción *-t*, permite identificar archivos del tipo indicado, facilitando el cribado de elementos ejecutables o de algún formato en particular que le interese al investigador forense. Por lo general, este comando funciona recibiendo como entrada una

[14] **Phishing:** El phishing consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales.
[15] **Spear-phishing:** Utiliza las técnicas del phishing pero se trata de un ataque dirigido lanzado contra un objetivo concreto. El hecho de que sea dirigido y no masivo implica una más rigurosa elaboración para lograr mayor credibilidad, y la utilización más sofisticada de ingeniería social.

imagen de volcado (*.dd*) y dentro de ella busca distintos archivos, pudiendo filtrar por el tipo o tratando de lograr un barrido rápido (solamente leería las cabeceras).

Como **puntos a favor** de esta herramienta contamos con que es una utilidad que estaría a caballo entre el **identificar archivos escondidos** bajo otro formato y que nos permitiría **recuperar archivos borrados** y teóricamente perdidos.

Como **punto negativo** tenemos que el **espacio de acción** de esta herramienta es **muy pequeño**, al tener una especialización muy concreta dentro de la identificación de información de archivos y no ser tan potente como las herramientas que veremos a continuación.

Como conclusión, *foremost* es una herramienta que seguramente no será la más necesaria dentro del ámbito de las Infraestructuras Críticas pero en el caso de requerir realizar un *file carving*, es una opción rápida, útil y gratuita.

6.10. Herramientas de recuperación de información eliminada

Como comenzamos a ver en el apartado anterior, en ocasiones en un análisis forense nos será necesario realizar un barrido de la memoria que teóricamente no está asignada o que está corrompida para poder recuperar así información perdida. Este proceso se realiza para recuperar evidencias que se han tratado de eliminar pero que al no haber sido sobrescritas en disco, aún son recuperables.

- **EASEus data recovery wizard**

La primera herramienta de recuperación de información eliminada que vamos a comentar es EASEus data recovery wizard, disponible para Windows y Mac OS y con una versión gratuita bastante limitada y dos licencias de pago que permiten recuperar la información sin límite de cantidad. El objetivo principal de esta herramienta es la **recuperación de información perdida** ya sea en el mismo dispositivo en el que se encuentra instalada, en un medio de almacenamiento externo (como un disco USB o una tarjeta SD), en una partición borrada o incluso en un disco formateado.

El programa funciona con **permisos de administrador**. Para comenzar a utilizarlo basta con seleccionar los formatos que se quieren localizar y la unidad a analizar. El programa tiene dos modos de búsqueda, uno más **en profundidad** (búsqueda bit a bit) y otro **más rápido**, dejando al usuario en una ventana de previsualización antes de guardar los datos, para así revisar que estos archivos recuperados no están corrompidos y son útiles.

Como **parte positiva**, esta herramienta cuenta con que tiene una **interfaz muy usable e intuitiva**, además entre los tipos de archivos identificables recoge la gran mayoría de los que nos pueden interesar en un análisis posterior y **soporta los principales sistemas de archivos**.

Como **contraparte negativa**, la versión gratuita se queda muy corta y el **barrido de la información es bastante lento**, aunque esto es una característica común a casi todas estas herramientas. Por último, al no utilizar un sistema de identificación de archivos mediante Hashes, **puede recuperar muchas veces el mismo archivo** (por ejemplo, un archivo que se haya movido de su ubicación inicial o que haya tenido varias copias en el dispositivo).

Por lo general, esta aplicación de recuperación de información borrada es **bastante útil** y puede ayudar a un forense a recuperar información que creía perdida o con la que no contaba.

- **Disk Drill Data Recovery Software**

Al igual que en el caso anterior, con Disk Drill nos encontramos con una herramienta de recuperación de información perdida bastante completa. Está disponible para sistemas Windows y Mac OS y **soporta una gran variedad de sistemas de archivos, incluyendo los discos catalogados como desconocidos** (RAW File Systems).

Disk drill cuenta gran variedad de archivos recuperables, siendo el proceso de recuperación muy sencillo. Las situaciones en las que es capaz de recuperar información son muy variadas: eliminado accidental, se ha vaciado la papelera de reciclaje, perdida de funcionalidad del disco duro, el formateo de unidad externa, una infección por *malware*, una partición perdida, un sistema de archivo desconocido o una tarjeta de memoria corrompida. Tras el análisis muestra un resumen de la información identificada al usuario y **permite su posterior almacenamiento en un disco distinto** al analizado dado que de coincidir origen y destino se podría dar una sobreescritura dañando así los datos recuperados.

Entre las **ventajas** de esta herramienta contamos con que soporta una **gran cantidad de formatos diferentes**, tiene una **alta tasa de recuperación** de la información y consta de una **interfaz muy intuitiva y directa**. Por el contrario, **no soporta el sistema de ficheros de teléfonos móviles** y la velocidad de recuperación es bastante mejorable.

Como conclusión, en este caso contamos con varias herramientas muy similares en prestaciones, seguramente la herramienta con estas características que destaca un poco más sobre las demás es EASEus, aunque la diferencia no es excesiva (detecta más formatos y es capaz de recuperar información en teléfonos móviles).

6.11. Herramientas de recuperación de contraseñas

En las grandes instituciones es común contar con una plantilla amplia, con distintas responsabilidades y permisos de acceso y con una gran variedad de aplicaciones y servicios. Por eso mismo, es común que en ocasiones las aplicaciones que menos uso tengan acaben siendo víctimas del olvido, de modo que al realizar un análisis forense, el investigador se dé cuenta de que esta continúa estando operativa pero nadie es capaz de darle un acceso a ella. Por eso mismo, nunca viene mal que un forense cuente en su conjunto de herramientas con alguna que le ayude a conseguir acceso a esas aplicaciones que puedan contener información útil para el caso.

- **RainbowCrack**

La primera de las herramientas que comentaremos aquí es RainbowCrack, la cual es un **cracker de contraseñas basado en tablas arcoíris**. Este sistema de búsqueda de contraseñas consiste en una aplicación alterna de funciones hash (también llamadas funciones resumen) y funciones de reducción, que tras una serie de repeticiones de este proceso genera un texto plano que se almacenará junto con la palabra inicial. Para buscar la contraseña que origina el hash, este sistema de búsqueda realiza el mismo proceso pero esta vez comenzando con la reducción, y tratando de localizar si alguna de las reducciones generadas da una coincidencia con la tabla. Este proceso se realiza para que las tablas de hashes no sean de un tamaño intratable pero que el tiempo destinado a descubrir el hash sea aceptable [43].

En el caso de RainbowCrack, las principales **características** que posee son las siguientes:

- **Algoritmos de resumen disponibles** para el descifrado. LM, NTLM, MD5, SHA1 y SHA256.
- **Sistemas Operativos**: Windows y Linux.
- Genera **tablas para contraseñas alfanuméricas en minúsculas, alfanuméricas mixtas y ASCII** (caracteres imprimibles).
- **Permite modificar la longitud** de la cadena de aplicaciones de las funciones.
- **Aceleración por GPU** (NVIDIA y AMD).

El funcionamiento es muy sencillo, basta con cargar el hash, indicar el archivo donde se encuentran las tablas y el programa comenzará a ejecutarse. El tiempo necesario para conseguir la contraseña varía de la complejidad de esta y de lo grandes que sean las tablas, al igual que sucede con el resultado. Cabe destacar que esta aplicación **no garantiza dar la contraseña**, y aún dándola, al tratarse de funciones resumen, existe la posibilidad de que sea otra contraseña pero que produzca el mismo resultado (lo que se conoce como una colisión), aun así, esta nueva contraseña debería funcionar de la misma manera que la original al compartir hash.

Entre las **ventajas** que tiene esta herramienta destacan la **rapidez** de evaluación de contraseñas respecto a la fuerza bruta, además el **menor tamaño de las tablas** respecto a las grandes bases de datos usadas para algunos ataques de diccionario hace que esta herramienta se pueda utilizar de manera portable.

Como **desventajas** destacables contamos con que esta herramienta **no es infalible**, ya que ante contraseñas que tengan un resumen que no aparezca dentro de la lista (o más bien, que ningún hash del proceso antes dicho lo haga), además en muchos sistemas se comienza a introducir el uso de rellenos que se añaden al final de la contraseña y que se guardan con el hash, de manera que cuesta más descubrir la contraseña al no estar preparado el algoritmo para este proceso.

Como conclusión, RainbowCrack es una herramienta muy útil, permitiendo descubrir contraseñas perdidas en servicios y aplicaciones que no apliquen medidas de seguridad al guardado de las contraseñas más allá de la aplicación de resúmenes para el almacenado. Además, es una herramienta que ya está integrada en la distribución Kali Linux, altamente utilizada para auditorías y análisis forenses, por lo que de disponer de este sistema operativo, el perito ya contaría con ella por defecto.

- **John the Ripper**

Cambiando de modelo de actuación, John the Ripper es una herramienta **de recuperación de contraseñas basada en fuerza bruta** aunque también permite la **búsqueda por diccionarios**, La principal finalidad de esta herramienta es el **auditar la seguridad de las contraseñas a partir de sus resúmenes**, trabajando con formatos como DES, BSDI, MD5, BF, AFS y LM.

Al ser una herramienta de comandos su funcionamiento es muy sencillo e intuitivo, siendo solamente necesario pasarle como argumento el archivo donde se encuentran las contraseñas resumidas. Además, permite incluir otras opciones para optimizar o variar su funcionamiento [44][45]. Algunos de los **sistemas que pueden verse vulnerados** con esta herramienta son: distribuciones **UNIX**, **Mac OS**, **Windows**, **WordPress**, **bases de datos SQL** y LDAP, contraseñas de **redes WiFi** WPA-PSK, el sistema de **autenticado en red de Windows**, claves privadas de **SSH** o de **monederos de criptomonedas**, documentos y **archivos comprimidos** con contraseña y más servicios y sistemas que utilicen el mismo sistema de protección de las contraseñas que los aquí nombrados. Cabe destacar que aunque John the Ripper no cuenta con una versión para Windows, uno de sus desarrolladores también ha creado otra aplicación con

muchas características en común para Windows que además cuenta con una GUI (*Graphical User Interface*, Interfaz Gráfica de Usuario) [46].

Entre las **ventajas** de esta herramienta podemos encontrar que permite la **aceleración por GPU**, se puede parar y reanudar la búsqueda en otro momento y ofrece una buena **versatilidad**, permitiendo modificar su modelo de actuación si el usuario así lo prefiere.

Por la contra, su principal **desventaja** está implícita en su objetivo; no busca descubrir contraseñas, sino evaluar la robustez de estas, de manera que de tener **una contraseña medianamente robusta se le hará muy complicado encontrarla**.

Como conclusión, hay muchas herramientas que pueden servir para la evaluación de las contraseñas. Que sean seguras para el usuario y que sean eficaces, no tantas. Por eso mismo, esta herramienta puede servir como un buen primer filtro para detectar posibles contraseñas perdidas pero que pude quedarse pequeña si se da el caso de que en esa organización la seguridad de las contraseñas se lleva correctamente.

- **HashCat**

Cuando se trata con recuperadores de contraseñas, lo normal es que surjan tres nombres: RainbowCrack (o también Ophcrack), John the Ripper y Cain & Abel. De las dos primeras acabamos de hablar, pero como la tercera opción mencionada lleva sin ser continuado desde 2014 hemos decidido hacer uso de uno de sus herederos en la materia; HashCat.
HashCat es uno de los **recuperadores de contraseñas más rápidos del mercado**, trabajando con un sistema de **reglas a nivel de núcleo** y la posibilidad de hacer **uso de las GPUs para acelerar el procesamiento** de Hashes. Además, otras características también destacables es que es un sistema capaz de **procesar varios Hashes a la vez**, actuar utilizando distintos elementos del mismo sistema (dos GPUs, la GPU y el procesador, …), permite parar la búsqueda y reanudarla más adelante, tiene **distintos modos** de actuación (por diccionario, fuerza bruta, asociación y distintas mezclas entre ellos y otros) y además es **capaz de trabajar con más de trescientos tipos de hash distintos**.
Como podemos ver, las ventajas de esta herramienta son muy numerosas, partiendo de que es multiplataforma, es adaptable al hardware disponible para así reducir el coste temporal, permite el uso de tablas o diccionarios si el usuario así lo prefiere y es capaz de trabajar con una gran cantidad de algoritmos distintos. Como contraparte, contamos con que es una herramienta que solamente está **disponible a través de comandos**, lo cual le puede dificultar el uso a un usuario que no tenga tanta experiencia con ese tipo de herramientas (aunque esto sea poco común en informáticos forenses).
Como conclusión, HashCat es seguramente la mejor herramienta del mercado en lo que a recuperación de contraseñas se refiere. Recientemente, el creador de esta herramienta ha afirmado que han sido capaces de recorrer todo el espectro de contraseñas de ocho caracteres en dos horas y media [47]. **Rápida, potente y gratuita**, por ahora, la mejor herramienta disponible para esta finalidad.

6.12. Herramientas de gestión de incidencias

En el caso de las Infraestructuras Críticas, siempre viene bien que quede un registro de la incidencia y que se haga un aviso lo más rápido posible para que se evalúe la gravedad de la incidencia; aún más, si tenemos en cuenta que no todos los trabajadores tienen por qué saber sobre informática ni más concretamente sobre ciberseguridad. Por ello, además de las

herramientas de análisis forense antes comentadas vamos a añadir dos herramientas de **seguimiento y gestión de incidentes**, cuyo principal objetivo será el generar **registros de posibles actividades indebidas** y poner al tanto a los encargados y a los expertos en la materia para que sean estos los que clasifiquen la peligrosidad de la situación encontrada.

- **GLPI**

La primera herramienta para analizar es la francesa **GLPI** (*Gestionnaire Libre de Parc Informatique*), cuya función es la de **gestionar servicios en tecnologías de la información**. Esta herramienta se instalaría en un servidor web de la organización y sería accesible desde los distintos equipos de la red interna a través de los navegadores web.

GLPI está **especializada en la administración de elementos de las organizaciones**, estando entre los activos administrables equipos, elementos de red, dispositivos periféricos, softwares o teléfonos. También aporta una parte de soporte y gestión en la que puedes hacer un **seguimiento de las distintas incidencias**, encontrar información sobre estas y gestionar qué elementos personalizables (presupuestos, proveedores, certificados, etc.) se pueden vincular con la herramienta. Por último, se incluye una parte de gestión de las herramientas utilizables y de los elementos de la aplicación, como son los usuarios, grupos o diccionarios.

Como **parte positiva** podemos encontrarnos con que esta es una herramienta de código abierto, de manera que el propio usuario puede **personalizar algunas de las funcionalidades** tratando de adaptarla lo mejor posible al esquema de su organización. También podemos contar como ventajas el que es una herramienta **muy completa** (permite monitorizar varios niveles de elementos de la organización) y que al ser una **aplicación del servidor**, no consume espacio en los distintos elementos de la red.

Por el contrario, al ser una herramienta centralizada, esta puede dar **problemas de escalabilidad** tanto en el almacenamiento de los registros y logs como en la administración de las incidencias por parte del administrador.

Como conclusión, esta herramienta cuenta con la parte positiva de ser de código abierto y personalizable, pero que puede desbocarse si se deja sin cuidar, por lo que en el caso de que los administradores de los servicios sean capaces de manejar la información resultante de la herramienta, esta sería una **solución muy útil**.

- **BOSSDesk**

Como **alternativa comercial** a GLPI contamos con **BOSSDesk**, el cual también realiza una **gestión de las incidencias por parte de los usuarios** y que está orientado a medianas y grandes empresas e incluso al sector público. Aunque es una herramienta muy completa, a nosotros lo que más nos interesará de ella es su parte de respuesta a problemas e incidentes.

Cuando un usuario detecta un funcionamiento incorrecto o un evento sospechoso, este debe comunicarlo para que se gestione y quede un registro de la incidencia, pudiendo **clasificarla según niveles de criticidad**. En cada incidencia abierta, se pueden incluir flujos de trabajo esperables habiendo también rutinas y calendarios de tareas. Cada una de estas notificaciones se denominan *tickets*, siendo el sistema de gestión aquí descrito un **sistema de *ticketing***.

Un problema es la causa de uno o más incidentes, por ello, además de permitir gestionar los incidentes por separado, BOSSDesk nos permite agruparlos y realizar un análisis conjunto del problema, realizando también un seguimiento del ciclo de vida de este. El programa permite al

gestor de las incidencias organizar las peticiones de gestión de manera que se quedan agrupados en un problema del cual dependerán para darse por terminados. En esta agrupación, se pueden incluir descripciones en detalle, incluir tareas, programaciones temporales y marcadores de resolución. También se pueden enlazar distintos problemas que estén correlacionados y realizar cambios en el proceso de resolución de los estos.

Como **puntos positivos** de esta herramienta contamos con la ya comentada funcionalidad de **agrupar las incidencias según el motivo** de estas y la posibilidad de tratar por separado las incidencias del posible problema que escondan detrás. También permite **realizar un seguimiento del estado** de la incidencia, por lo que facilita la resolución de esta.

Como **lado negativo**, paradójicamente, tenemos que esta es una **herramienta muy completa**, de manera que tiene muchas más funcionalidades de las que aquí buscamos, complicando la usabilidad en el caso de que prefiramos ceñirnos a ese único objetivo.

Como **conclusión**, esta herramienta es una de las más completas del mercado, lo cual puede ser una desventaja en el caso de que solamente nos interese la funcionalidad aquí analizada pero que a su vez podría ser la herramienta ideal si en la organización también se busca una solución de gestión de incidencias de escritorio completa.

6.13. Herramientas CCN-CERT

Como ya hemos visto en los capítulos de *El estado del arte* y *La ciberseguridad en las Infraestructuras Críticas en España*, a través del CCN se pone a nuestra disposición una gran variedad de documentos e información para comprender mejor la situación de las Infraestructuras Críticas y para saber cómo actuar en lo que a la defense de estas se refiere. Por ello, no es de extrañar que en este capítulo volvamos a contar con una sección dedicada a las herramientas de esta organización. Actualmente el **CCN-CERT** cuenta con **veintitrés soluciones** que intervienen en distintas fases de la solución de incidencias, y abarcan desde herramientas de gestión y coordinación en ciberincidencias hasta herramientas de auditoría. Entre todas ellas, hay siete que serían aplicables en alguno de los once apartados antes descritos.

Como apunte antes de comenzar con el análisis, con la excepción de REYES y LUCÍA, la información referente a las soluciones aquí comentadas está clasificada, por lo que solamente se puede acceder a la descripción que se aporta de ellas ya sea en la página del CCN con la descripción de las distintas soluciones [48] o en algún caso, en las páginas web de los colaboradores en el desarrollo de la solución [49].

- **ADA**

La primera solución que comentaremos es **ADA**. Esta es una herramienta de **análisis avanzado de malware**, que surge de la **integración de** las soluciones previas de **análisis estático** (MARÍA) y **análisis dinámico** (MARTA). Además de servir como unificación de estas dos herramientas, también aporta **nuevas funcionalidades**:

- **Interfaz unificada**. Como acabamos de comentar, ADA permite gestionar las funcionalidades de MARÍA y MARTA desde una misma interfaz.
- **Histórico de análisis**. Permite la consulta de los resultados en ambos tipos de análisis además de realizar un seguimiento de las amenazas que se van detectando.

- **Generación de informes automáticos y personalizables**. Tras realizar un seguimiento de los resultados de los análisis, es posible exportar estos creando un informe ejecutivo o técnico.
- **Diseñado desde el *front-end***. El diseño de la herramienta está centrado en la usabilidad, tratando de simplificar las investigaciones realizadas.
- **Entorno de análisis aislado**. Se aplican dos niveles de aislamiento: por un lado el análisis se realiza en entornos de *sandbox* y además, el resultado de estos queda aislado del resto de usuarios y miembros de la organización.
- **Interacción completa con las máquinas virtuales**. Integración completa de los entornos de análisis que permite acceder a estos de manera sencilla desde la propia solución.

Una vez vista la descripción de la herramienta, realicemos la pregunta clave **¿Dónde puedo integrar esta solución dentro del proceso de análisis forense?** El objetivo de ADA es detectar posibles softwares maliciosos escondidos dentro del sistema a analizar, por lo que en este caso, la respuesta es sencilla, al encajar perfectamente con las herramientas expuestas en el apartado ***6.7. Herramientas de detección de malware***.

- **CARMEN**

La protección de las instalaciones ante actividades ilícitas no se queda en el análisis de aplicaciones maliciosas, sino que también se nos presenta una solución de **identificación de APTs**. A través de CARMEN podemos realizar una **adquisición, procesamiento y análisis de eventos** que puedan ser indicios de anomalías en el correcto funcionamiento del sistema, de movimientos laterales o de exfiltraciones.

La base de CARMEN es el **procesamiento del tráfico de la red interna**, revisando tanto los tráficos con el exterior como posibles movimientos laterales. Este análisis se realiza de manera pasiva, analizando los tráficos y los registros que dejan los accesos en red. Con esto, se busca proteger la información más crítica de la organización, evitando así los posibles daños económicos y de reputación que generaría que estos pasasen a ser de dominio público.

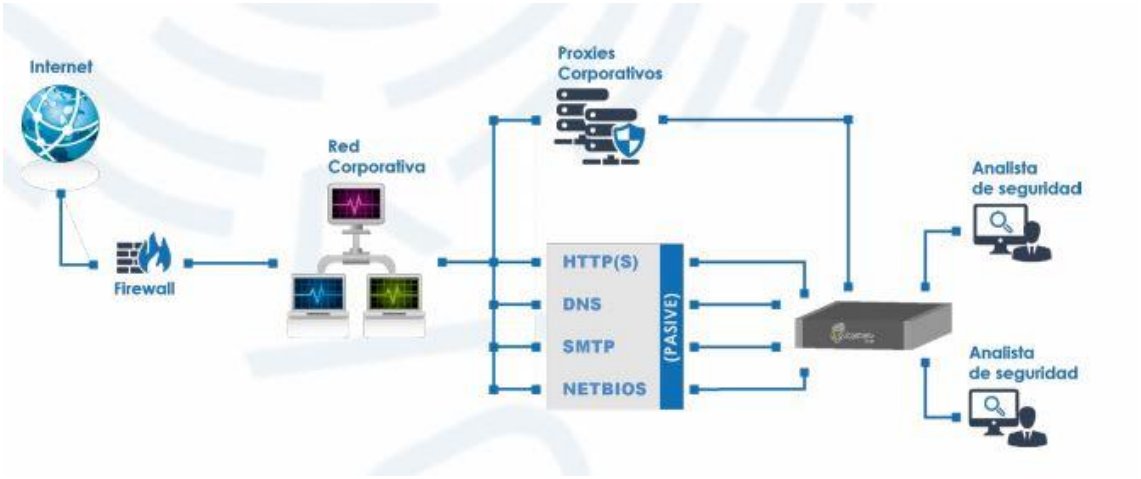

Figura 7. Esquema del funcionamiento de CARMEN. Fuente: Ficha técnica de CARMEN (https://www.ccn-cert.cni.es/soluciones-seguridad/carmen.html).

Esta es una de las soluciones más transversales entre las propuestas en el CCN-CERT, ya que se integra con GLORIA (gestión de amenazas e incidentes), LUCÍA (gestión de ciberincidentes) y REYES (intercambio de información en ciberamenazas). A su vez, si tratamos de clasificarla

dentro de los apartados antes descritos, CARMEN se situaría entre las presentadas en el ***6.8. Herramientas de detección de intrusiones***, siendo catalogable como un NIDS. Aun así, esta solución cuenta con más funcionalidades, quedándosele corta la clasificación en uno solo.

- **CLAUDIA**

Como acabamos de comentar, CLAUDIA es una solución integrada con la recién analizada CARMEN. El objetivo de esta herramienta es servir de ***endpoint*** **para la recogida de información**. Las características principales de CLAUDIA son:

1. **Base de Datos de la gestión de configuración** (CMDB por sus siglas en inglés) **integrada**, en la que se actualizan automáticamente los activos de red presentes.
2. **Configuración centralizada en los dispositivos terminales**.
3. **Ejecución de los sensores bajo demanda**. Permite la consulta de claves de registro, de existencia de ficheros, permite la realización remota de volcados de memoria, la ejecución remota de herramientas de triaje y la ejecución de reglas YARA en toda la red (de estas reglas ya hemos hablado en el apartado 6.7).
4. **Recogida de eventos de usuario de Windows** y del monitor del sistema de Windows (*Sysmon*).

Esta solución, aunque forma parte de CARMEN, puede catalogarse en el grupo de las herramientas vistas en el punto ***6.7. Herramientas de detección de malware***, compartiendo algunas de las características de funcionamiento de YARA, herramienta con la que comparte reglas de análisis.

- **GLORIA**

GLORIA por su parte es una plataforma de **gestión de incidentes y amenazas cibernéticas**. Al igual que sucedió con la herramienta IBM QRadar, está basada en un **sistema SIEM**, realizando un análisis, almacenamiento e interpretación de aquellos datos sacados durante el proceso de monitorización del sistema. El objetivo de esta solución es utilizar esa información para **encontrar posibles relaciones entre los eventos analizados**.

Con GLORIA se optimiza en el procesamiento centralizado de grandes volúmenes de información de eventos de seguridad, siendo esta mejora escalable en el caso de que se estén analizando datos de distintas fuentes. Con esta información, se realiza una **correlación en origen**, repartiendo así el trabajo de manera distribuida y **mandando alertas** solamente en aquellos casos **en los que se han establecido correlaciones**.

Su funcionamiento está basado en **cuatro módulos**:

1. **Módulo de vigilancia, monitorización y recolección** (ARGOS). Realiza una **monitorización de los elementos tecnológicos** de donde recoge los eventos de seguridad. Este módulo está basado en tecnologías IDS, sistemas de análisis automáticos de vulnerabilidades, analizadores de tráficos y otros detectores de actividad en red.
2. **Módulo de inteligencia mediante correlación de eventos** (TRITÓN). En este módulo se realizan **tareas de inteligencia** a través de las que se detallan y parametrizan los distintos eventos obtenidos en el primer módulo.
3. **Módulo de gestión del servicio** (EMAS). De manera centralizada, se **recogen las incidencias y alertas generadas** en el segundo módulo.

4. **Módulo de *Dashboarding*** (HERA). Se realiza una automatización, orquestación y optimización de los tiempos de respuesta a través de la integración de distintos sistemas de análisis de eventos. De esta manera, se **automatiza tanto como sea posible el proceso de análisis** acelerando la respuesta a los incidentes.

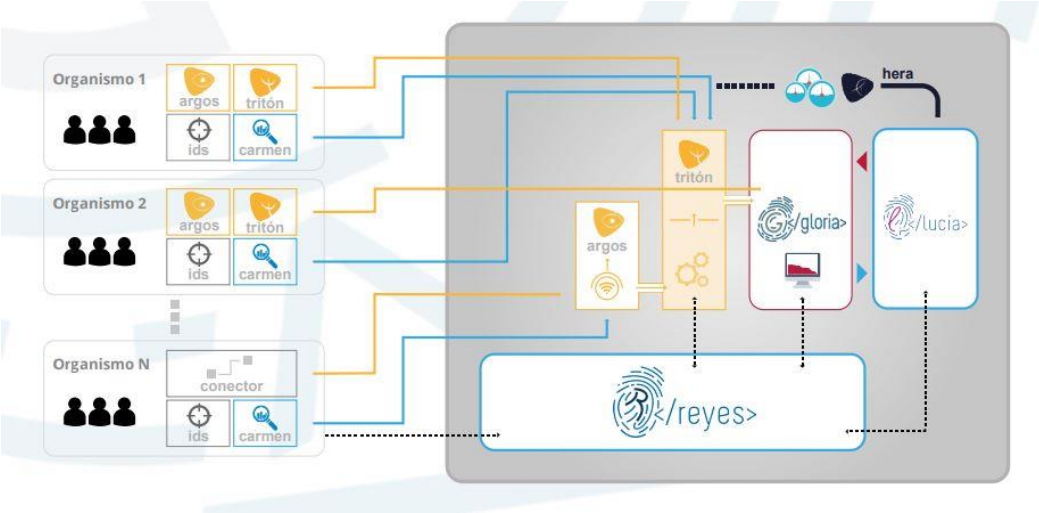

Figura 8. Esquema de la arquitectura de GLORIA. Fuente: https://www.ccn-cert.cni.es/soluciones-seguridad/gloria.html, Ficha Técnica.

- **LUCIA**

LUCÍA es la **herramienta de gestión de incidencias** que nos proporciona el CCN-CERT. Desde ella se permite realizar la notificación de una incidencia propia y que los distintos miembros adscritos se coordinen entre ellos para tratar de acelerar la resolución de las alertas generadas a través del Sistema de Alertas Tempranas (SAT).

Estas notificaciones se gestionan a través de un **sistema de *ticketing***, en el que hay dos tipos de *tickets*; los propios y los SAT. Ambos tipos se recogen cuando se notifican, se incluyen en una cola y ahí se agrupan por temática o por tipo. En la notificación, se añade una serie de datos, los cuales indican desde elementos identificadores hasta el rango de direcciones IP de los elementos que se han visto comprometidos por el evento notificado.

Cuando se realiza la gestión de un *ticket*, se genera otro del **tipo Incidencia**, el cual incluye información procedente del *ticket* original que ha sido tratado e información añadida como es el caso del **nivel de Peligrosidad** y la **Situación del *ticket***. Además, según el organismo de origen de la Incidencia y las características de esta, se especifica si se debe realizar una notificación a la Agencia Española de Protección de Datos (AEPD), al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) o al Centro Criptológico Nacional (CCN).

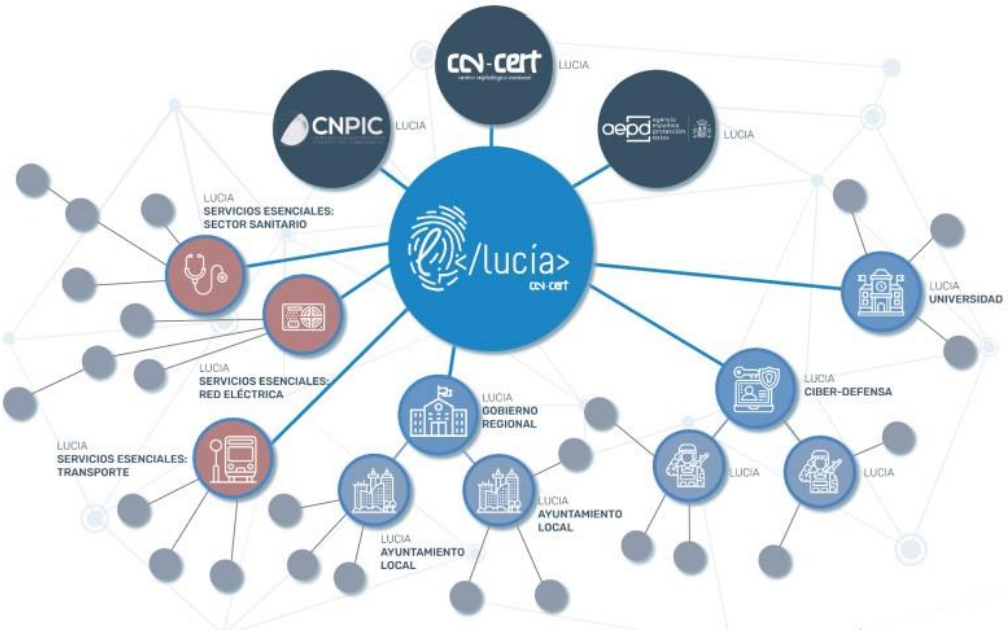

Figura 9. Esquema de la arquitectura de LUCÍA. Fuente: https://www.ccn-cert.cni.es/soluciones-seguridad/lucia.html. Sistema LUCIA y actualizaciones, Presentación Lucía.

El resto de **las funcionalidades** de LUCÍA **dependerán de la calificación del organismo**, permitiendo todos los organismos editar, buscar, enlazar y borrar *tickets*, siendo posible también para los organismos federados la creación y asignación de *tickets*. De cara a la resolución de los *tickets*, el organismo que recibe la asignación puede rechazarlo (o abandonarlo de ser del tipo Incidencia) o resolverlo (cerrándolo).

Al igual que en las soluciones anteriores, también vamos a tratar de clasificar esta herramienta entre los tipos antes analizados. En esta ocasión, esta se puede encuadrar dentro del apartado ***6.13. Herramientas de gestión de incidencia***.

- **MÓNICA**

MONICA es un **sistema automatizado de gestión de eventos e información de seguridad**. El objetivo de esta solución es **detectar una amenaza antes de que logre hacerse con información o se logre reproducir**, adelantándose así al ataque. Este tipo de soluciones recibe el nombre de **sistemas SIEM**, dividiendo sus funcionalidades entre el análisis de eventos en tiempo real (SEM) y la gestión y almacenamiento de registros (SIM).

Sus principales **características** son:

- **Rápida toma de decisiones contextualizadas**. Realiza un **análisis y contextualización centralizado de los datos recogidos** desde las distintas fuentes a las que tiene acceso: fuentes técnicas, investigaciones, información abierta y oculta, redes sociales, fuentes internas y terceros. Este proceso lo logra realizar **hasta un 32% más rápido**, estableciendo además un triaje de los incidentes y reduciendo los falsos positivos.
- **Obtención de una imagen completa y real del riesgo**. Según el momento en el que se gestiona el incidente, se pueden dividir estos análisis en tres estadios: **análisis sobre el registro** de información de los eventos acontecidos, **análisis en tiempo real** del flujo de eventos acontecidos y la **acción preventiva** a través del estudio del historial de incidentes y la aplicación de algoritmos para el establecimiento de bandas de normalidad, tendencias y puntos débiles del sistema.

- **Visibilidad completa de la Infraestructura Tecnológica** (IT). Aplicación de distintos agentes para lograr una **mayor visibilidad de las posibles amenazas**. Estos agentes están divididos en tres **tipos**: agentes **intranet** (dispositivos de seguridad lógica, servidores web, sistemas internos, hosts, etc.), de agentes **extranet** (portales web de clientes y proveedores), aplicaciones *cloud-store* y aplicaciones no corporativas) y agentes **ambiente** (redes sociales, páginas web, sistemas de información no TIC y dispositivos de seguridad física).
- **Uso de técnicas de detección avanzadas para descubrir amenazas**. Uso de herramientas de aprendizaje autonómico, de ciberinteligencia y de análisis del comportamiento del usuario para **identificar amenazas hasta 10 veces antes** y resolviéndolas un 63% más rápido.
- **Simplificación de la monitorización y gestión de incidentes**. Acceso a la plataforma a través de una **interfaz web *responsive*** y generación automatizada y personalizada de informes.

MONICA está diseñada para ser aplicada junto con GLORIA, de manera que estas actúan de manera complementaria en sus objetivos. Visto esto, podemos incluir a MONICA dentro del apartado ***6.5. Herramientas de monitorización del sistema y usuarios en tiempo real***.

- **REYES**

La última herramienta que analizaremos es el analizador de ciberincidencias REYES. Esta herramienta está basada en la **tecnología MISP** (*Malware Information Sharing Platform*), es decir, se nutre de la información disponible en sus distintas fuentes para lograr un mayor conocimiento de las posibles amenazas logrando así agilizar el proceso de prevención y respuesta ante estas.

Sus principales **características** son:

- **Uso de múltiples fuentes**. Para realizar la búsqueda de información sobre las ciberamenazas, se usan **fuetes integradas de carácter privado** (MISP y CIF) **y fuentes públicas especializadas** (RiskIQ, VirusTotal, Whois, Censys y Shodan). En estas fuentes se puede realizar la búsqueda por dominio, IP, URL o Hash, dependiendo de la fuente que se elija.
- **Representación en grafo de asociaciones o de inteligencias**. Según los filtros de búsqueda indicados, el programa **muestra los resultados obtenidos a través de un grafo de asociación o de inteligencia**, siendo posible pivotar entre los distintos indicadores presentados. Al realizar doble clic en un elemento, se despliega una descripción desde donde se añade información de este.
- **Priorización de la información**. Antes de mostrar la información, se realiza un **proceso de filtrado y clasificación para mostrar la información disponible según su prioridad**. Esta información se puede obtener a través de distintos listados que varían su presentación según el elemento buscado.
- **Uso de información de acceso restringido**. A partir del núcleo de información MISP, se puede obtener de manera exclusiva **información proveniente de distintos organismos internacionales**.
- **Fácil exportación**. Desde prácticamente todas las interfaces donde se muestra información detallada se aporta una **opción para descargar esta información**. El formato de la descarga depende de la interfaz desde la que se realiza y de la información seleccionada para ser descargada.

Al igual que pasó con otras herramientas de este apartado, REYES forma una solución bastante completa, estando integrada con una serie de detectores de amenazas en red que le aportan información para su análisis posterior, aun así, como su principal función no es la detección de eventos sino el análisis de estos para establecer relaciones que puedan denotar amenazas, podríamos encuadrar a esta herramienta en el apartado ***6.7. Herramientas de detección de malware***.

6.14. Paquetes de herramientas forenses

Para terminar con las herramientas forenses, vamos a comentar una serie de distribuciones y herramientas que incluyen diversas funcionalidades, englobando no sólo varias de las aquí expuestas sino también otras que puedan ser de utilidad según el contexto del análisis. Las herramientas de este apartado a su vez se dividirán en dos clases; las **distribuciones**, que corresponden con las tres primeras herramientas, y los **paquetes de herramientas**, que serán las cuatro siguientes. Muchos investigadores forenses seguramente ya contarán en su *toolkit* con alguna de ellas, por ello, vamos a comentar cuales son sus herramientas que mejor se adaptan en nuestra clasificación y con cuales se pueden complementar.

- **Kali**

Para comenzar, vamos a presentar una distribución que está presente en casi todos los libros que trate de auditoría informática: Kali Linux. Esta distribución está **basada en Debian** y surge como respuesta a la necesidad de una **distribución ligera que pueda realizar test de penetración y auditorías de seguridad**. Aunque esta temática no coincide con la que nosotros estamos tratando en este trabajo, también cuenta con **herramientas de *reversing* y análisis forense**. Estos tipos de herramientas son:

1. **Recolectores de información**. Las herramientas de este apartado nos permiten realizar una **evaluación de los sistemas y redes** del entorno a analizar. Aunque lo más común es que se usen para evaluar qué servicios vulnerables hay o que información sensible se envía de manera insegura, muchas de estas herramientas también pueden ser utilizadas para **identificar flujos de información o servicios ilegítimos**. Algunas de las herramientas que encontramos aquí: *nmap*, *Wireshark* y *Xplico*.
2. **Explotación de contraseñas**. Las herramientas de este apartado están diseñadas para **explotar posibles debilidades en las contraseñas de los usuarios y servicios**. Aunque el fin es el mismo, no todas las herramientas son iguales, dado que estas pueden estar especializadas según el servicio a atacar, el tipo de contraseña o el algoritmo de ataque. Algunas de las herramientas que encontramos aquí: *ashcat*, *John the Ripper* y *RainbowCrack*.
3. **Ingeniería Inversa**. La técnica de la ingeniería inversa (o *reversing*) es utilizada para **analizar el código de una aplicación a partir un ejecutable**. En las pruebas de penetración se utiliza esta técnica para tratar de localizar vulnerabilidades escondidas en el código, pero para el análisis forense esta técnica nos puede servir para identificar código malicioso dentro de una aplicación. Algunas de las herramientas que encontramos aquí: *apktool*, *dex2jar* y *JD-GUI*.
4. **Rastreo y redireccionamiento en red**. Las herramientas aquí englobadas tratan de obtener información de la red para hacer una suplantación de identidad o un *Man in The Middle*. Dentro del análisis forense, también se pueden utilizar para **identificar posibles exfiltraciones de información**. Algunas de las herramientas que encontramos aquí: *Bettercap*, *rtpbreak* y *Wireshark*.

5. **Forense**. Por último, también tenemos un grupo de herramientas que tienen el objetivo principal de **realizar un rastreo de pistas** que puedan ayudar a descubrir el origen y el procedimiento realizado **en la explotación de una vulnerabilidad**. Algunas de las herramientas que encontramos aquí: *bulk-extractor*, *DFF* y *iPhone Backup Analyzer*.

En términos generales, si se tiene que definir cuál es la principal finalidad de Kali Linux, no hay duda de que la respuesta será realizar pruebas de penetración. Pero esto no es incompatible con el análisis forense; muchas de las herramientas de toma de información pueden servir para ambas finalidades y al también incluir herramientas de *reversing* y de análisis forense, esta distribución es muy buena opción para usarla como la base del *toolkit* personal. Además, la gran cantidad de información que hay disponible sobre esta distribución y la igualmente gran comunidad que tiene, facilita el mantenerse al día sobre las nuevas técnicas y herramientas disponibles.

Para saber más sobre esta distribución o descargarla, esto se puede realizar a través de su **página web oficial** [50] y de la página donde se explica más en detalle cada una de las herramientas disponibles por defecto [51].

- **Santoku**

Santoku es una distribución orientada para el **análisis forense de teléfonos inteligentes**. Aunque tiene muchas herramientas orientadas a Android, desde esta distribución también podemos analizar imágenes de dispositivos iOS y Windows, contando con aplicaciones especializadas según el sistema en cuestión.

Esta distribución permite realizar tanto auditorías como investigaciones forenses, teniendo herramientas de *reversing*, monitores de red, de pruebas de penetración y de análisis forense. Dentro de estas funcionalidades contamos con una novedad, el análisis de **archivos Smali**, pero ¿Qué es esto del Smali? Las aplicaciones Android contienen documentos ejecutables de extensión *.dex*, pero estos documentos son prácticamente ilegibles para los investigadores al tratarse de código binario. Por eso, Santoku nos ofrece las herramientas *baksmali*/*smali*, las cuales **desensamblan/ensamblan estos archivos en un formato de bajo nivel más accesible para el ojo humano**; el resultado de ese desembalaje es el documento *.smali* [52]. Para saber más de Smali, se recomienda revisar el repositorio del creador de este lenguaje [53].

Pasemos ahora a ver una tabla con las herramientas disponibles:

Desarrollo	Forense	Pentesting	Reversing	Análisis de red
Android SDK Manager	AF Logical OSE	Burp Suite	Androguard	Chaosreader
Android Studio	Android Brute Force Encryptation	Ettercap	AntiLVL	Dnschef
AXMLPrinter 2	ExifTool	Nmap	APKTool	DSniff
Eclipse	iOS Backup Analyzer 2	SSLStrip	Baksmali	Mitmproxy
Fastboot	Libimobiledevice	W3af	Bulb Security SPF	Tcpdump
Heimdall	Scalpel	ZAP	Dex2jar	Wifite
SBF Flash	SleuthKit	Zenmap	Drozer	Wireshark
	Yaffey		Jasmin	
			JD-GUI	
			Procyon	
			Radare2	
			Smali	

Tabla 1. Herramientas por defecto en la distribución Santoku.

Entre estas herramientas encontramos algunas que se **encuadran entre las categorías antes vistas**: *The SleuthKit* (clonado), *Wireshark* (monitorización de red), *Androguard* (detección de malware), *ExifTool* (análisis de archivos), *Scalpel* (recuperación de datos) y *Android Brute Force Encryptation* (recuperación de contraseñas). Estas herramientas son complementadas con otras centradas en la **recuperación de archivos y registros especiales en entornos móvil**. A su vez, podemos instalar otras herramientas como *Odin* (volcado de ROM) y *Snort*/*OSSEC* (detección de intrusiones). En este caso, al tratarse de una distribución que suele ser externa, no sería muy aprovechable el uso de herramientas de gestión de incidencias.

Para saber más sobre esta distribución o descargarla, esto se puede realizar a través de su **página web oficial** [54].

- **Caine**

Como última distribución orientada al análisis forense contamos con **CAINE** (*Computer Aided INvestigative Enviroment*), una distribución **basada en Linux y de código abierto** cuyo principal objetivo es proporcionar un **entorno intuitivo para las investigaciones forenses**. Si Kali Linux es un estándar para los que se están inicializando en el *pentesting* (y también para muchos usuarios avanzados), Caine es su equivalente forense.

Esta distribución cuenta con dos tipos de herramientas: las **herramientas vía script**, que son una serie de archivos ejecutables, generalmente **en Python**, que realizan tareas forenses, y las herramientas propiamente dichas. A su vez, entre todas estas, contamos con herramientas con multitud de funcionalidades:

1. **Herramientas de clonado y de volcado de memoria volátil**. Al igual que las demás distribuciones, en esta también contamos con herramientas que nos permiten realizar **clonados bit a bit de la información** en otro dispositivo (*dcfldd* y *AIR*) y herramientas de **volcado de memoria volátil** (*Autotimeliner*). Además cuenta con *The Sleuth Kit* y *Autopsy*, con las que puede realizar análisis de la información extraída o clonada.
2. **Herramienta de análisis del sistema y de registros de aplicaciones web**. En este grupo encontramos una serie de herramientas que nos permiten **extraer información sobre el estado del sistema**, comprobando si ha habido alguna actividad sospechosa recientemente ya sea a través del **análisis de archivos del sistema** (*log2timeline* y *reglookup*), de archivos de **log de bases de datos** (*SQLJuicer*), de la **papelera de reciclaje** (*rifiuti2*) o de **navegadores web** (*Pasco* y *Galleta*).
3. **Herramientas de análisis de red**. No podía faltar en una distribución forense las herramientas de **escaneo y monitorización del tráfico web**, ya sean más completas como *Wireshark* y *nmap* o más específicas como *tcpflow* o *tcpdump*.
4. **Análisis de archivos**. Caine también incluye herramientas que permiten realizar **análisis de los metadatos** (*AFF* y *AtomicParsley*), realizar ***file carving*** (*Scalpel*) y **análisis estenográficos**[16] (*stegbreak* y *steghide*).
5. **Recuperador de contraseñas**. Dentro de este apartado contamos con la posibilidad de realizar **análisis de los hashes** de las contraseñas del sistema y de aplicaciones (*Bkhave* y *hashdb*) o para analizar hashes en general (*Hashcat* y *MD5deep*). También tiene otras herramientas que permiten la **sobreescritura de contraseñas** (*Chntpw* y *Polkit*).

[16] **Estenografía:** Práctica de ocultar información secreta dentro de otro archivo o mensaje y transferirla a través de un canal oculto, para que no se sospeche de ella hasta que se extrae en su destino.

6. **Recuperación de información borrada**. Por último, también cuenta con herramientas de **recuperación de archivos** a través del análisis de cabeceras y pies (*foremost* y *fatback*) y la recuperación de **memoria estropeada** (*testdisk* y *ddrescue*).

Estas herramientas no son todas las disponibles, sino que forman una breve selección para indicar algunas de las funcionalidades que nos han parecido más relevantes y alguna de las herramientas que se presentan en esta distribución. Pero, además, esta distribución también **permite que el usuario instale otras herramientas** como pueden ser descompiladores o analizadores del código **para así completar las funcionalidades** aquí comentadas.

Para saber más sobre esta distribución o descargarla, esto se puede realizar a través de su **página web oficial** [55].

- **Paquetes de herramientas**

En este último subapartado contamos con una serie de paquetes de herramientas con una gran variedad de funcionalidades. Estos paquetes en lo que consisten es en proporcionar una **interfaz unificada para** que, a través de una serie de comandos o elementos accionables, el usuario pueda **ejecutar distintas tareas**, acaparando por lo general un mayor espectro de tareas que las herramientas comunes.

Los paquetes que hemos destacado son los siguientes:

1. **Autopsy.** Este paquete de herramientas proporciona una **interfaz gráfica a las herramientas englobadas dentro de *The Sleuth Kit***. Los **usos** de Autopsy son varios, **desde peritajes judiciales hasta recuperar fotos** de una tarjeta dañada. Está disponible de manera gratuita para sistemas Windows, Linux e iOS, tanto para 64-bit como para 32-bit [56].
2. **OSForensics.** Orientado a la **realización de peritajes informáticos**, OSForensics es un paquete de herramientas que permite la **ejecución de distintas funcionalidades clasificadas usando un sistema de árbol jerarquías**, en el que las herramientas a utilizar se encuentran en las hojas de este árbol. Está disponible para sistemas Windows a partir de Windows Vista y Windows Server 2000 tanto para 64-bit como para 32-bit, también es instalable en dispositivos extraíbles de al menos 500MB. El precio varía según el tipo de licencia, estando accesibles de manera gratuita las versiones que ya no cuentan con soporte [57].
3. **Nirsoft.** En este caso, contamos con un paquete de herramientas que proporciona una serie de ejecutables que son descargables tanto de manera individual como a través de un paquete completo. Estos programas se caracterizan por ser **pequeños ejecutables de una funcionalidad muy concreta**, estando divididos a la hora de descargarlos en distintas páginas según la utilidad más general (recuperar contraseñas, herramientas de red, análisis de correos, …). Estas herramientas están disponibles para sistemas operativos Windows de 64-bit y 32-bit [58].
4. **PowerForensics.** El objetivo principal de PowerForensics es proporcionar un conjunto de **herramientas en Windows para el análisis forense de discos duros, con un esquema de archivos NTFS o FAT**. Está disponible para su descarga tanto en la página web de PowerShell como desde GitHub [59].
5. **Sysinternals.** Este paquete de herramientas desarrollado por una filial de Microsoft busca proporcionar una serie de herramientas para **realizar acciones avanzadas del sistema y leer información técnica**. Está disponible de manera integrada al sistema

operativo y para utilizar de manera externa, siendo invocables las utilidades a través de PowerShell [60].

En la siguiente tabla podemos ver **cuántos de los tipos de herramientas** en los que hemos dividido este apartado **pueden englobar alguna de las funcionalidades presentes** en cada uno de los cinco paquetes de herramientas comentados.

	Autopsy	**OSForensics**	**Nirsoft**	**PowerForensics**	**Sysinternals**
Clonado	✓	✓		✓	✓
Volcado de memoria	✓	✓			
Monitorización del sistema	✓	✓	✓	✓	✓
Análisis de red [17]	✓		✓	✓	✓
Análisis de código malicioso	✓	✓			
Detección de instrucciones					
Análisis de archivos	✓	✓	✓	✓	✓
Recuperación de datos	✓	✓	✓		
Recuperación de contraseñas	✓	✓	✓		✓

Tabla 2. Tipos de funcionalidades forenses disponibles en los paquetes de herramientas analizados.

Como podemos ver, ninguna de estas herramientas podría servirnos de manera completa por sí sola, y a su vez, **no todos los paquetes de herramientas realizan las mismas tareas aunque tengan herramientas de los mismos tipos**. Por ejemplificar esto, una herramienta que sea capaz de leer los registros de Windows sirve para monitorizar el sistema, pero también sucede lo mismo con las que son capaces de gestionar los archivos de log de las distintas aplicaciones y servicios, siendo estas tareas distintas pero englobadas en el mismo apartado.

Como **conclusión**, en este apartado contamos con varias distribuciones y paquetes de herramientas que ofrecen en un mismo lugar **una mayor variedad de funcionalidades** que una herramienta de por sí no suele proporcionar, aún así, **ninguna de ellas está completa en sí misma**, siendo en algunos contextos necesario el complementarlas con otras herramientas más específicas.

[17] El análisis de red hace referencia a las herramientas que realizan evaluaciones sobre las conexiones de red, no solamente a herramientas de monitorización.

7. Conclusiones

No documentes el problema; arréglalo.
Atli Björgvin Oddsson.

Cuando comenzamos con este trabajo, nos planteamos la cuestión de qué herramientas podrían ayudarnos en un análisis forense dentro del contexto de las infraestructuras críticas. Para poder responder a esto, lo primero fue comprender dicho contexto. Las Infraestructuras Criticas son un caso aparte dentro de las distintas organizaciones que conforman el panorama nacional, abarcando los sectores más críticos para el correcto funcionamiento de un país o región. Por ende, su contexto y regulación también están recogidos como un caso a parte que debemos estudiar con más detenimiento. Además, esta criticidad hace que puedan ser foco de atacantes más poderosos, tanto en número, como en conocimientos, como en capacidades, exponiéndonos así a las amenazas más peligrosas de la actualidad: las APTs.

Por eso mismo, el análisis de los eventos de estas infraestructuras no es un asunto baladí, siendo muy importante el saber identificar en cada momento las señales de que algo no está sucediendo correctamente, para así parar la amenaza lo más pronto posible, reduciendo daños, gastos y esfuerzos. En este aspecto, el valor añadido que aporta este trabajo reside en esta misma búsqueda y recolección de herramientas, ya que una de las partes del principal objetivo de este trabajo es justamente el presentar herramientas para este análisis, siendo las *Herramientas de monitorización del sistema en tiempo real* y las *Herramientas de detección de intrusiones* las principales para esta finalidad. Además, si este análisis detecta una anomalía o una intrusión, el investigador debe tratar de encontrar el origen alterando lo mínimo posible el estado de las pruebas y el sistema afectado, por eso también hemos visto conveniente incluir *Herramientas de clonado* y *Herramientas de volcado de memoria volátil*. Una vez los entornos de investigación han sido aislados, el resto de las herramientas (y también las de detección ya comentadas) ayudan a la resolución de la incidencia, encargándose cada una de buscar pista en su función específica.

Este proceso de análisis puede funcionar tanto para el peritaje forense de un individual, como para la evaluación e la seguridad en una empresa, como en el caso de las Infraestructuras Críticas. Por ello, para focalizar más sobre estas últimas, también hemos buscado y comentado aquellas herramientas que los organismos rectores de la ciberseguridad nacional han puesto a disposición de estas infraestructuras.

Dicho todo esto y como conclusión, respecto a los objetivos marcados al comienzo del trabajo, considero que hemos sido capaces de alcanzarlos dentro de nuestras capacidades. Muchas herramientas de monitorización, recolección de información y análisis forense están orientadas a grandes empresas. Otras, como es el caso de las herramientas del CCN-CERT, están orientadas a sectores críticos. Por esto mismo, a lo largo de la realización del trabajo nos hemos encontrado con varios impedimentos para lograr una mayor documentación tanto de herramientas aquí presentes como de otras que nos hemos visto obligados a descartar al no tener suficiente información que aportar.

En definitiva, la realización de este trabajo me ha permitido, a título personal, entrar en contacto con todas estas herramientas y aprender mucho sobre el proceso de toma de evidencias y su posterior análisis, por lo que, independientemente de lo que suceda posteriormente, en el momento en el que redacto estas líneas puedo considerarme satisfecho con el conocimiento adquirido a lo largo de este proceso de elaboración del trabajo de fin de carrera y con el resultado de este.

7.1. Trabajos futuros

A lo largo de este trabajo hemos tratado de resolver un problema presente en casi todos los ámbitos de la informática: la **paradoja de la elección** que se nos presenta ante la multitud de herramientas intercambiables entre sí dependiendo del contexto de uso. Desde aquí, hemos utilizado la perspectiva de las Infraestructuras Críticas para realizar una **selección de las herramientas de informática forense** que mejor podían cuadrar según las necesidades del investigador en cada momento. Pero la velocidad a la que avanza la tecnología puede hacer que estas aplicaciones acaben siendo superadas de aquí a unos pocos años o incluso meses; basta con la aparición de un nuevo paradigma para que estas herramientas caigan en desuso.

Por eso, desde aquí proponemos una herramienta que funcione como un **configurador de *toolkits***. Esta herramienta comenzaría solicitando el **tipo de organización** a la que irían dirigidas las herramientas, habiendo las opciones de individual, micropyme, PYME, gran empresa, sistema crítico. La siguiente etapa mostraría tres preguntas seguidas. La primera pregunta sería el **sistema operativo** desde el que se organizará el análisis forense; las opciones en este caso serían las tres grandes familias de sistemas operativos (a saber, Windows, Linux y Mac OS) y la opción de multiplataforma. A la vez, se mostraría la opción en la que se elegiría el **tipo de herramienta** a buscar, siendo las opciones las ya vistas y analizadas en el capítulo 6. Por último, se pediría un **precio máximo** a gastar, habiendo distintos márgenes en función de la primera pregunta (no es lo mismo la capacidad económica y los requisitos de una gran empresa que en el caso de un autónomo).

La aplicación mostraría una **selección ordenada** de las herramientas que cumplan las condiciones, dándole al usuario un **enlace a la página web oficial** de la herramienta para que desde ahí realicen el pago o, en el caso de que sea gratuita, la descargue directamente. La diferencia de esta aplicación respecto al trabajo actual es la posibilidad no solo de indicar las características de las herramientas, sino también darle al usuario un acceso directo a ellas; además, al ser una aplicación informática, podría **actualizar su lista de herramientas** según estas vayan apareciendo en páginas de referencia más genéricas, como pueden ser el catálogo de herramientas del INCIBE [61] o el catálogo de herramientas del NIST [21].

8. Glosario de término

Las definiciones aquí presentes son sacadas de la página web de Panda Security [62] y del glosario de Kaspersky [63]. Estas fuentes fueron elegidas al haber sido tomadas como referencia para la elaboración del glosario de términos de ciberseguridad del INCIBE. Otra fuente también usada como referencia ha sido el Glosario de Ciberseguridad del NICCS [64].

- **Análisis forense:** Procesos y técnicas especializados para reunir, conservar y analizar datos relacionados con el sistema (evidencias digitales) con fines de investigación. (Traducida de NICCS)
- **APT:** (*Advanced Persistent Threat*, Amenaza Persistente Avanzada). Este ataque se aplica a ataques concretados, sigilosos y continuos contra organizaciones específicas – en contraste con los incidentes especulativos, aislados y oportunistas que constituyen la mayor parte de la actividad de los ciberdelincuentes. Por lo general, estos ataques están dirigidos por entidades gubernamentales, quienes hacen uso de malwares altamente sofisticados para violar la seguridad de una organización concreta. (Traducida de Kaspersky)
- **Backdoor:** Se trata de un programa que se introduce en el ordenador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario. (Panda Security)
- **Backup:** La copia de datos en forma de *backup* ayuda a la recuperación de la información en el caso de que esta se pierda o dañe. Es recomendable realizar copias de seguridad periódicas de todos los datos importantes y mantener estas en un medio externo o en la nube. (Traducida de Kaspersky)
- **Ciberamenaza:** En el contexto de la ciberseguridad, una circunstancia o evento que tiene el potencial de explotar las vulnerabilidades y de tener un potencial dañino (generar circunstancias adversas) en la organización, sus activos (incluyendo la información y los sistemas de información), sus miembros, otras organizaciones o la sociedad. (Traducida de NICCS)

- **Ciberincidencia:** En el ámbito de la ciberseguridad, ocurrencia que tiene el potencial de provocar consecuencias adversas para un sistema de información o para la información que este procesa, almacena o transmite y que puede requerir un plan de acción para mitigar las posibles consecuencias. (Traducida de NICCS)
- **Cookies:** Es un fichero de texto que, en ocasiones, se envía a un usuario cuando éste visita una página Web. Su objetivo es registrar la visita del usuario y guardar cierta información al respecto. (Panda Security)
- **Cracker:** Es una persona interesada en saltarse la seguridad de un sistema informático. (Panda Security)
- **Darknet:** Red de superposición (es decir, una red construida sobre otra red, en este caso, Internet) que no es detectable por métodos normales y solo se puede acceder haciendo uso de software especializado como Tor. Las Darknets están diseñadas para preservar la privacidad de quienes las usan. (Traducida de Kaspersky)
- **Driver:** Es un programa, conocido como controlador, que permite la gestión de los dispositivos conectados al ordenador (generalmente, periféricos como impresoras, unidades de CD-ROM, etc). (Panda Security)
- **Estenografía:** Práctica de ocultar información secreta dentro de otro archivo o mensaje y transferirla a través de un canal oculto, para que no se sospeche de ella hasta que se extrae en su destino. (Traducida de Kaspersky)
- **Falso positivo:** Aplicado en el campo de la detección de malware, un falso positivo se produce cuando el programa marca por error un archivo inocente como infectado. Esto puede parecer bastante inofensivo, pero los falsos positivos pueden ser una verdadera molestia. (Traducida de Kaspersky)
- **Honeypot:** Los *honeypots* son ordenadores señuelos utilizados para atraer la atención de los ciberatacantes. Estos ordenadores están segregados del sistema principal, proporcionando una manera de desviar a los atacantes que entraron a la red o monitorizar sus actividades. (Traducida de Kaspersky)

- **Intrusión:** Violación intencionada de las políticas de seguridad de un sistema. (Traducida de NICCS)
- **Archivo de Log:** Documento o archivo electrónico que registra todas las acciones y eventos de un sistema en orden cronológico, así como los mensajes de error y otras incidencias. Se utilizan para analizar el funcionamiento de un objeto, ya sea un equipo, servidor, recurso web, sistema operativo o aplicación independiente. (Traducida de Kaspersky)
- **Machine Learning:** Rama de la inteligencia artificial que consiste en utilizar conjuntos de datos para entrenar algoritmos. Al analizar las soluciones que se dan a un gran número de problemas similares, los sistemas informáticos comienzan a identificar patrones y ofrecer soluciones a tales problemas. (Traducida de Kaspersky)
- **Malware / Código malicioso:** Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos. MALicious softWARE. (Panda Security)
- **Phishing:** El phishing consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. El caso más típico de phishing es el envío de correos electrónicos que se hacen pasar por procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falseada. (Panda Security)
- **Ransomware:** El *malware* de rescate, o *ransomware*, es un tipo de programa maligno diseñado para chantajear a las víctimas a cambio de dinero, bloqueando el acceso a su ordenador o encriptando la información almacenada en él. (Traducida de Kaspersky)
- **Reversing:** Proceso de estudio de un programa final utilizando métodos especiales. El *reversing* o ingeniería inversa, abarca una amplia gama de áreas, incluyendo la decompilación y desmontaje de archivos ejecutables y bibliotecas, y el análisis de datos del sistema. (Traducida de Kaspersky)

- **Rootkit:** Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los propios normalmente). Este tipo de software no es malicioso en sí mismo, pero es utilizado por los piratas informáticos para esconder evidencias y utilidades en los sistemas previamente comprometidos. Existen ejemplares de malware que emplean rootkits con la finalidad de ocultar su presencia en el sistema en el que se instalan. (Panda Security)
- **Sandbox:** En el contexto de la seguridad informática, un *sandbox* proporciona un entorno estrictamente controlado en el que programas o scripts semiconfiables pueden ejecutarse de forma segura en memoria (o con acceso limitado al disco duro local). (Traducida de Kaspersky)
- **Spear-phishing:** Utiliza las técnicas del phishing pero se trata de un ataque dirigido lanzado contra un objetivo concreto. El autor que origina este tipo de ataque, nunca recurrirá al spam para conseguir una avalancha masiva de datos personales de los usuarios. El hecho de que sea dirigido y no masivo implica una más rigurosa elaboración para lograr mayor credibilidad, y la utilización más sofisticada de ingeniería social. (Panda Security)

9. Bibliografía y Referencias

A continuación listaremos los documentos que nos sirvieron de referencia para la elaboración de este trabajo. Todos los enlaces indicados a continuación están disponibles a fecha de 07/07/2021:

- BOE.es - Ámbitos de la Seguridad Nacional: Ciberseguridad, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=397_Ambitos_de_la_Seguridad_Nacional_Ciberseguridad
- Página web del CSIRT. Sección de miembros, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.csirt.es/index.php/es/miembros
- Guías CCN-STIC:
    - Guía de Seguridad de las TIC: CCN-STIC 801 – Esquema Nacional de Seguridad. Responsabilidades y Funciones, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html
    - Guía de Seguridad de las TIC: CCN-STIC 804 – ENS. Guía de implantación, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html
    - Guía de Seguridad de las TIC: CCN-STIC 811 – Interconexión en el ENS, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/521-ccn-stic-811-interconexion-en-el-ens/file.html
    - Guía de Seguridad: CCN-STIC 815 – Esquema Nacional de Seguridad. Métricas e Indicadores, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/525-ccn-stic-815-indicadores-y-metricas-en-el-ens/file.html
    - Guía de Seguridad: CCN-STIC 817 – Esquema Nacional de Seguridad. Gestión de ciberincidentes, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html
    - Guía de Seguridad: CCN-STIC 818 – Herramientas de seguridad en el ENS, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/527-ccn-stic-818-herramientas-de-seguridad-en-el-ens/file.html

Referencias:

[1] Los diez principales hackers más relevantes (infames) de todos los tiempos, 2021. *www.kaspersky.es* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.kaspersky.es/resource-center/threats/top-ten-greatest-hackers

[2] Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país, sin fecha. *BBC News Mundo* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.bbc.com/mundo/noticias-39800133

[3] CORREAS, Por Marta, sin fecha. Ciberguerra fría y geopolítica: ¿con qué armas proteger el endpoint? | WatchGuard Technologies. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.watchguard.com/es/wgrd-news/blog/ciberguerra-fria-y-geopolitica-con-que-armas-proteger-el-endpoint-0

[4] El virus que tomó control de mil máquinas y les ordenó autodestruirse, 2015. *BBC News Mundo* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

[5] ANÁLISIS | El ciberataque al oleoducto Colonial Pipe en EEUU, 2021. *Newtral* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.newtral.es/ciberataque-oleoducto-colonial-line-eeuu-estados-unidos/20210518/

[6] Informe Anual de Seguridad Nacional 2019 (dsn.gob.es). Figura 9-5, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.dsn.gob.es/sites/dsn/files/MASTER%20IASN2019%20WEB_0.pdf

[7] EUR-Lex - 52004DC0702 - EN - EUR-Lex, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52004DC0702

[8] Informe Anual de Seguridad Nacional 2019 (dsn.gob.es). Página 127, sin fecha [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.dsn.gob.es/sites/dsn/files/MASTER%20IASN2019%20WEB_0.pdf

[9] Guía nacional de notificación y gestión de ciberincidentes, sin fecha. . P. 55. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

[10] ¿Qué es una APT? – Kaspersky Daily, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.kaspersky.es/blog/que-es-una-apt/966/

[11] List of intelligence gathering disciplines | Project Gutenberg Self-Publishing - eBooks | Read eBooks online, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: http://www.self.gutenberg.org/articles/eng/List_of_intelligence_gathering_disciplines?View=embedded%27%27

[12] Five Styles of Advanced Threat Defense, sin fecha. *Gartner* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.gartner.com/en/documents/2576720/five-styles-of-advanced-threat-defense

[13] A. Villalón Huerta, *Amenazas Persistentes Avanzadas*. Nau Llibres, 2016, pp. 215. ISBN: 9788416926091.

[14] S. M. Milajerdi, R. Gjomemo, B. Eshete, R. Sekar and V. N. Venkatakrishnan, *HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows*, 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 1137-1152, doi: 10.1109/SP.2019.00026.

[15] SEGURIDAD, Redacción Muy, sin fecha. Kaspersky Lab destapa la «Operación NetTraveler». *MuySeguridad. Seguridad informática.* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.muyseguridad.net/2013/06/05/kaspersky-nettraveler/

[16] The Epic Turla (snake/Uroburos) attacks, 2021. *latam.kaspersky.com* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://latam.kaspersky.com/resource-center/threats/the-epic-turla--snake-uroburos-attacks

[17] P. Vila Avendaño, *Técnicas de Análisis Forense Informático para Peritos Judiciales profesionales*. 0xWord, 2018, pp. 239. ISBN: 9788469777008.

[18] ¿Qué Es Un Hash Y Cómo Funciona?, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

[19] J. Garrido Caballero, J.L. G. Rambla y Chema Alonso. *Análisis Forense Digital en entornos Windows*. Informática 64, 2009, pp. 219. ISBN: 9788461334322.

[20] Guía de Seguridad: CCN-STIC 818 – Herramientas de seguridad en el ENS, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/527-ccn-stic-818-herramientas-de-seguridad-en-el-ens/file.html

[21] Computer Forensics Tools & Techniques Catalog - Tool Search, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://toolcatalog.nist.gov/search/index.php

[22] I just used Capterra to find software!, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.capterra.com/

[23] SourceForge - Download, Develop and Publish Free Open Source Software, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://sourceforge.net/

[24] SECURITY, T. W. C., 2021. *thimbleweed/All-In-USB* [en línea]. PHP. [Accedido 7 julio 2021]. Recuperado a partir de: https://github.com/thimbleweed/All-In-USB

[25] *volatilityfoundation/volatility*, 2021. [en línea]. Python. Volatility Foundation. [Accedido 7 julio 2021]. Recuperado a partir de: https://github.com/volatilityfoundation/volatility

[26] GARCÍA, Jose, 2021. La Universidad de Minnesota ha sido baneada del desarrollo de Linux por introducir vulnerabilidades a propósito. *Xataka* [en línea]. 22 abril 2021. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.xataka.com/aplicaciones/universidad-minnesota-ha-sido-baneada-desarrollo-linux-introducir-vulnerabilidades-a-proposito

[27] MAHESAN, Thanursan, 2020. Comparison of Memory Acquisition Software for Windows. *Medium* [en línea]. 27 diciembre 2020. [Accedido 7 julio 2021]. Recuperado a partir de: https://thanursan.medium.com/comparison-of-memory-acquisition-software-for-windows-e8c6d981db23

[28] WinPcap - Home, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.winpcap.org/default.htm

[29] Man page of TCPDUMP, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.tcpdump.org/manpages/tcpdump.1.html

[30] Man page of PCAP-FILTER, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.tcpdump.org/manpages/pcap-filter.7.html

[31] Wireshark · Display Filter Reference: Index, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.wireshark.org/docs/dfref/

[32] Wireshark User's Guide: Version 3.5.0, sin fecha. . P. 333. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.wireshark.org/download/docs/user-guide.pdf

[33] Fiddler | Web Debugging Proxy and Troubleshooting Solutions, sin fecha. *Telerik.com* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.telerik.com/fiddler

[34] NetworkMiner - The NSM and Network Forensics Analysis Tool 🔨, sin fecha. *Netresec* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.netresec.com/?page=networkminer

[35] Running YARA from the command-line — yara 4.1.0 documentation, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://yara.readthedocs.io/en/stable/commandline.html

[36] Snort - Network Intrusion Detection & Prevention System, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.snort.org/#documents

[37] Releases · snort3/snort3, sin fecha. *GitHub* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://github.com/snort3/snort3/releases

[38] ET OPEN Ruleset Download Instructions, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://rules.emergingthreats.net/OPEN_download_instructions.html

[39] Oinkmaster, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: http://oinkmaster.sourceforge.net/download.shtml

[40] WHITE, Joshua, FITSIMMONS, Thomas y MATTHEWS, Jeanna, 2013. *Quantitative Analysis of Intrusion Detection Systems: Snort and Suricata*. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.researchgate.net/profile/Joshua-White-26/publication/236146583_Quantitative_Analysis_of_Intrusion_Detection_Systems_Snort_and_Suricata/links/02e7e51945be7912a7000000/Quantitative-Analysis-of-Intrusion-Detection-Systems-Snort-and-Suricata.pdf

[41] Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview

[42] Un ataque de «phishing» por correo electrónico utilizando ni más ni menos que código Morse, sin fecha. *Microsiervos* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.microsiervos.com/archivo/seguridad/new-phishing-attack-uses-morse-code-to-hide-malicious-urls.html

[43] Rainbow tables: qué son y cómo funcionan las tablas arco iris, sin fecha. *IONOS Digitalguide* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.ionos.es/digitalguide/servidores/seguridad/rainbow-tables/

[44] Linux Certif - Man john(8), sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.linuxcertif.com/man/8/john/

[45] Más sobre John The Ripper | Manual de seguridad informática - I, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.fpgenred.es/Seguridad-Informatica-I/ms_sobre_john_the_ripper.html

[46] Hash Suite - A program to audit security of password hashes, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://hashsuite.openwall.net/

[47] PASTOR, Javier, 2019. El fin de la contraseña de ocho caracteres: HashCat puede crackearlas en menos de 2,5 horas. *Xataka* [en línea]. 15 febrero 2019. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.xataka.com/seguridad/no-basta-contrasenas-ocho-caracteres-hashcat-puede-crackearlas-2-5-horas

[48] Soluciones, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.ccn-cert.cni.es/soluciones-seguridad.html
[49] MÓNICA NGSIEM: la nueva herramienta del CCN desarrollada por ICA Sistemas y Seguridad, sin fecha. *Web Corporativa* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.grupoica.com/-/monica_ngsiem_ccn_ica_sistemas_y_seguridad
[50] Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution, sin fecha. *Kali Linux* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.kali.org/
[51] Kali Linux Tools Listing, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://tools.kali.org/tools-listing
[52] Introducción al lenguaje de Smali, 2018. *Blog de iordic* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://iordic.github.io/android/smali/reversing/apk/coding/2018/10/08/introduccion-a-smali.html
[53] GRUVER, Ben, 2021. *JesusFreke/smali* [en línea]. Java. [Accedido 7 julio 2021]. Recuperado a partir de: https://github.com/JesusFreke/smali
[54] Welcome · Santoku Linux, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://santoku-linux.com/
[55] CAINE Live USB/DVD - computer forensics digital forensics, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.caine-live.net/
[56] Autopsy | Digital Forensics, sin fecha. *Autopsy* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.autopsy.com/
[57] PassMark OSForensics - Digital Investigation, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.osforensics.com/osforensics.html
[58] freeware utilities: password recovery, system utilities, desktop utilities - For Windows, sin fecha. *NirSoft* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.nirsoft.net/
[59] PowerForensics, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://powerforensics.readthedocs.io/en/latest/
[60] MARKRUSS, sin fecha. Windows Sysinternals - Windows Sysinternals. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://docs.microsoft.com/en-us/sysinternals/
[61] Buscador de soluciones, sin fecha. *INCIBE* [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/buscador-soluciones
[62] Glosario técnico sobre Virus, Spyware, Troyanos y amenazas de Internet-Información sobre Seguridad-Panda Security, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://www.pandasecurity.com/es/security-info/glossary/
[63] Glossary, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://encyclopedia.kaspersky.com/glossary/
[64] Cybersecurity Glossary | National Initiative for Cybersecurity Careers and Studies, sin fecha. [en línea]. [Accedido 7 julio 2021]. Recuperado a partir de: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

ANEXO 1. Tablas de herramientas

NOMBRE	TIPO	ENTORNO	MODO DE EMPLEO	USO	LICENCIA -MIENTO	ACCESO
Upcopy	Clonado	Windows	comandos	Externa	Gratuita	UPCOPY (dmares.com), http://www.dmares.com/maresware/html/upcopy.htm
FTK Imager	Clonado y volcado de RAM	Multiplata-forma	GUI	Instalable	Gratuita	FTK Imager version 4.2.1 | AccessData, https://accessdata.com/product-download/ftk-imager-version-4-2-1
DDrescue	Clonado	Linux	comandos o GUI	Integrada	Gratuita	Ddrescue - GNU Project - Free Software Foundation (FSF), https://www.gnu.org/software/ddrescue/ddrescue_es.html
Dumpit	Volcado de RAM	Windows	comandos	Externa	Desde 0€ hasta 2.154,50€	Utilities | MoonSols, https://moonsols.com/resources.html
Volatility	Análisis de RAM	Multiplata-forma	comandos o GUI	Instalable	Gratuita	The Volatility Foundation - Open Source Memory Forensics, https://www.volatilityfoundation.org/
Manet RAM Capture	Volcado de RAM	Windows	GUI	Externa	Gratuita	MAGNET RAM Capture | Magnet Forensics, https://www.magnetforensics.com/resources/magnet-ram-capture/
Belkasoft Live RAM Capturer	Volcado de RAM	Windows	GUI	Externa	Precio variable, desde 0€	Belkasoft RAM Capturer: Volatile Memory Acquisition Tool, https://belkasoft.com/ram-capturer
Intella W4	Análisis del sistema	Windows y plataformas Web	GUI	Instalable	732,11 € (895 USD)	W4 - Who | What | When | Where (vound-software.com), https://www.vound-software.com/w4
IBM QRadar SIEM	Análisis del sistema	Windows	GUI	Instalable	772 €/mes	IBM QRadar SIEM - Visión general - España | IBM, https://www.ibm.com/es-es/products/qradar-siem
Magnet Axiom	Análisis del sistema	Windows	GUI	Instalable	Precio variable, sin versión gratuita	Magnet AXIOM | Digital Investigation Platform | Magnet Forensics, https://www.magnetforensics.com/products/magnet-axiom/

Tabla 3. Resumen de las herramientas forenses analizadas (1/3).

NOMBRE	TIPO	ENTORNO	MODO DE EMPLEO	USO	LICENCIA-MIENTO	ACCESO
Windows Registry Recovery	Análisis del sistema en tiempo real	Windows	GUI	Portable	Gratuito, 30€ o 150€	MiTeC Homepage, https://www.mitec.cz/wrr.html
TCPDump/ Windump	Análisis del tráfico de la red	Multiplata-forma	comandos	Instalable	Gratuito	TCPDUMP/LIBPCAP public repository, https://www.tcpdump.org/
Wireshark	Análisis del tráfico de la red	Multiplata-forma	comandos o GUI	Instalable	Gratuita	Wireshark · Go Deep., https://www.wireshark.org/
FOCA	Análisis de metadatos	Multiplata-forma	GUI	Instalable	Gratuita	GitHub - ElevenPaths/FOCA, https://github.com/ElevenPaths/FOCA
libextractor	Análisis de metadatos	Multiplata-forma	comandos	Integrada	Gratuita	Libextractor - GNU Project - Free Software Foundation, https://www.gnu.org/software/libextractor/
Foremost	file carving	Linux	comandos	Integrada	Gratuita	foremost(1) - Linux man page (die.net), https://linux.die.net/man/1/foremost
YARA	detección de malware	Multiplata-forma	comandos	Integrada	Gratuita	Welcome to YARA's documentation! — yara 4.1.0 documentation, https://yara.readthedocs.io/en/v4.1.0/index.html
rkhunter/ chkrootkit	detección de malware	Linux	comandos	Integrada	Gratuita	The Rootkit Hunter project (sourceforge.net), http://rkhunter.sourceforge.net/ Chkrootkit -- locally checks for signs of a rootkit, http://www.chkrootkit.org/
IDA hex-rays	detección de malware	Multiplata-forma	GUI	Instalable	Desde 0€ hasta 3220,53€ al año	ida-pro – Hex Rays (hex-rays.com), https://hex-rays.com/ida-pro/
hijackthis	detección de malware	Windows	GUI	Portable	Gratuita	HijackThis 2.9.0.6 - Español | InfoSpyware, https://www.infospyware.com/antimalware/hijackthis/

Tabla 4. Resumen de las herramientas forenses analizadas (2/3).

NOMBRE	TIPO	ENTORNO	MODO DE EMPLEO	USO	LICENCIA-MIENTO	ACCESO
EASE us data RW	recuperación de archivos borrados	Windows y Mac OS	GUI	Instalable o Portable (según la licencia)	Gratuita, 66,69€ o 139,90€ al año	Free Download Data Recovery Software of 2021 for File Recovery - EaseUS® Data Recovery Wizard Free. https://www.easeus.com/datarecoverywizard/free-data-recovery-software.htm
Disk Drill Data RS	recuperación de archivos borrados	Windows y Mac OS	GUI	Instalable	Gratuita, 72,67€ o 407,47€	Data Recovery Software Wizard & Rest. ore Deleted Data from Windows PC (bitrecover.com), https://www.bitrecover.com/data-recovery-software/
SNORT	NIDS y HIDS	Multipla-taforma	comandos	Instalable	Gratuita	Snort - Network Intrusion Detection & Prevention System, https://www.snort.org/
Suricata	NIDS y HIDS	Multipla-taforma	comandos o GUI	Instalable	Gratuita	Suricata | Open Source IDS / IPS / NSM engine (suricata-ids.org), https://suricata-ids.org/
OSSEC	NIDS y HIDS	Multipla-taforma	comandos o GUI	Instalable	Gratuita con versión corporativa	Get OSSEC - OSSEC, https://www.ossec.net/ossec-downloads/
Rainbow Crack	Explotación de contraseñas	Windows y Linux	comandos o GUI	Instalable o Portable (según la licencia)	Gratuita	RainbowCrack - Crack Hashes with Rainbow Tables (project-rainbowcrack.com), https://project-rainbowcrack.com/index.htm
HashCat	Explotación de contraseñas	Multipla-taforma	comandos	Instalable	Gratuita	hashcat - advanced password recovery, https://hashcat.net/hashcat/
John the ripper	Explotación de contraseñas	Linux y Mac OS	comandos	Instalable	Desde 0€ hasta 152,58€	John the Ripper password cracker (openwall.com), https://www.openwall.com/john/
GLPI	Gestión de incidencias	Multipla-taforma	GUI	Instalable en Servidor	Gratuita o corporativa por 19€/mes	Inicio - GLPI Project (glpi-project.org), https://glpi-project.org/es/
BOSS Desk	Gestión de incidencias	Multipla-taforma	GUI	Instalable	Desde 15,69€ al mes	Award Winning Help Desk for Cloud and On-Premise (boss-solutions.com), https://www.boss-solutions.com/bossdesk.html

Tabla 5. Resumen de las herramientas forenses analizadas (3/3).

	TIPO DE HERRAMIENTA	ACCESO
ADA	Herramientas de detección de malware	https://www.ccn-cert.cni.es/soluciones-seguridad/ada.html
CARMEN	Herramientas de detección de intrusiones	https://www.ccn-cert.cni.es/soluciones-seguridad/carmen.html
CLAUDIA	Herramientas de detección de malware	https://www.ccn-cert.cni.es/soluciones-seguridad/claudia.html
GLORIA	Herramientas de monitorización del sistema y usuarios en tiempo real	https://www.ccn-cert.cni.es/soluciones-seguridad/gloria.html
LUCÍA	Herramientas de gestión de incidencias	https://www.ccn-cert.cni.es/soluciones-seguridad/lucia.html
MONICA	Herramientas de monitorización del sistema y usuarios en tiempo real	https://www.ccn-cert.cni.es/soluciones-seguridad/monica.html
REYES	Herramientas de detección de malware	https://www.ccn-cert.cni.es/herramientas-ciberseguridad-2/reyes.html

Tabla 6. Resumen de las herramientas del CCN-CERT englobables en la clasificación vista en este trabajo.