ANÁLISIS DE HERRAMIENTAS ENDPOINT AND DETECTION RESPONSE (EDR) DE SOFTWARE LIBRE

JAVIER EDUARDO SEPULVEDA FUENTES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

ANÁLISIS DE HERRAMIENTAS ENDPOINT AND DETECTION RESPONSE (EDR) DE SOFTWARE LIBRE

JAVIER EDUARDO SEPULVEDA FUENTES

Monografía presentada como requisito parcial para optar al título de:
Especialista en seguridad informática

HERNANDO JOSE PEÑA HIDALGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 16/04/2021

Es preciso y coherente dedicar la superación de este peldaño más en el camino de la academia a mi padre, mi madre, mi hermana y especialmente a mi novia; pues son ellos mi núcleo familiar y quienes en todo momento estuvieron prestos y dispuestos a brindar todo tipo de apoyo para que el desarrollo tanto del presente trabajo de grado como el de todos los créditos de la especialización se pudieran llevar a buenos términos.

Dedico y agradezco también a Dios, por darme la sabiduría y la paciencia para poder llevar en armonía los diferentes ámbitos de mi vida y siempre permitirme distinguir de forma clara cuáles son las prioridades. También a Dios gracias por cada una de las habilidades que como ser humano me ha entregado para así afrontar con fundamentos los diferentes desafíos que se presentan en lo académico, laboral y personal.

Enfatizo mi dedicatoria a Natalia B., mi novia, porque fue ella quien, con determinación, incluso mucho antes de iniciar la especialización, direccionó acertadamente el ámbito educativo en mi vida siendo así la causante de todo lo que a partir de ello he conseguido.

AGRADECIMIENTOS

Agradezco a la UNAD – Universidad Nacional Abierta y a Distancia y particularmente a cada uno de los docentes de la especialización en seguridad informática, quienes, a través del acompañamiento en el desarrollo de cada uno de los cursos pertenecientes al programa, fortalecieron mis conocimientos en el área y brindaron su apoyo ante las dificultades presentadas.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ALERTA DE SEGURIDAD INFORMÁTICA: Mensaje emitido por una plataforma de seguridad informática debido a la ocurrencia de un evento que debe ser revisado

AMENAZA INFORMÁTICA: Agente externo o interno con capacidad de afectar el funcionamiento normal de un activo/servicio.

ANÁLISIS FORENSE: Uso de técnicas y herramientas informáticas con el fin de reconstruir un ataque realizado para así determinar las modificaciones hechas sobre el sistema y realizar las correcciones pertinentes que eviten que el mismo sea realizado nuevamente.

ATAQUE INFORMÁTICO: Acciones realizadas por un delincuente que comprometen la seguridad de un sistema y de la información.

BOTNET: Conjunto de computadores que han sido infectados y están bajo subordinación de un servidor malicioso.

COMANDO & CONTROL (C&C): Servidor malicioso que controla una botnet(sistemas infectados) a la cual le emite instrucciones para la realización de delitos informáticos (distribución de malware, denegación de servicio (DoS), denegación distribuida de servicio (DDoS), envío de spam, etc.

CONFIDENCIALIDAD: Propiedad de la información con la cual un recurso sólo puede ser accedido por quien se encuentre autorizado, así, "cada sistema automático o individuo sólo podrá usar los recursos que necesita para ejercer sus tareas"[1]

CSIRT[2]: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad informática). Equipo interdisciplinar creado con el propósito de ayudar en la respuesta a incidentes relacionados con la seguridad informática

DISPONIBILIDAD: Propiedad de la información por la cual un recurso puede ser accedido en el momento en que se requiera.

DENEGACIÓN DE SERVICIO (DoS): Ataque informático mediante el cual un sistema realiza peticiones recurrentes a un servidor con el fin de agotar sus recursos de cómputo y ocasionar indisponibilidad del servicio

[1] ROMERO CASTRO, Martha Irene, et al. En: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Alcoy, 2018, p 26

[2] NIST. National Institute of Standars and Technology. Handling an Incident. En: Computer Security Incident Handling Guide

DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDoS): Ataque informático mediante el cual varios sistemas realizan peticiones recurrentes a un servidor con el fin de agotar sus recursos de cómputo y ocasionar indisponibilidad del servicio

ENDPOINT: Es un dispositivo que envía y recibe datos a través de una red de telecomunicaciones en la que se encuentra conectado y se caracteriza por ser el punto final en dicha red. En estos dispositivos nacen y finalizan las transacciones informáticas.

EVENTO DE SEGURIDAD INFORMÁTICA: Situación que implica un cambio en el estado normal de un activo de información o sistema.

EXPLOIT: Como expresa BELCIC[3], un exploit es una porción de código diseñado para que al ejecutarse explote una vulnerabilidad determinada en un sistema. Los exploit dejan de ser funcionales cuando con actualizaciones y parches de seguridad dichas vulnerabilidades son corregidas

INCIDENTE DE SEGURIDAD: Según lo indica INCIBE[4], un incidente de seguridad consiste en la materialización de un riesgo que afecta uno o varios de los pilares de la seguridad de la información: Disponibilidad, Confidencialidad, Integridad.

INDICADOR DE COMPROMISO (IoC): Es una porción de información, que permite identificar la existencia de actividad anormal sobre un sistema. Un IoC, “simplemente es un artefacto que se deja en un sistema o red que significa que se ha materializado una amenaza o un ataque ya conocido”[5]

INTEGRIDAD: Propiedad con la cual se conoce que la información ha estado libre de modificaciones de personas no autorizadas, así, la integridad “consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente, el hecho de trabajar con información errónea puede ser tan nocivo para las actividades como perder la información”[6]

MALWARE: Código malicioso diseñado para causar inestabilidad en un sistema informático, robar información o suplantar identidad, entre otros; ya sea mediante la explotación de una vulnerabilidad o modificando la configuración del sistema informático.

---

[3] BELCIC, Ivan. ¿Qué es un exploit en seguridad informática? En: https://www.avg.com/es/signal/computer-security-exploits Marzo 2021

[4] INCIBE, Instituto Nacional de Ciberseguridad. Una guía de aproximación para el empresario. En: Glosario de términos de Ciberegurudad. León. 2017. p. 24

[5] FOWLER, Kevvie. Data Breach Preparation and Response: Breaches are Certain, Impact is Not. Cambridge, 2016.

[6] ROMERO CASTRO, Martha Irene, et al. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Alcoy, 2018. p. 26

MYPYMES[7]: Microempresas, pequeñas empresas y medianas empresas.

PROCESO DE RESPUESTA A INCIDENTES[8]: Conjunto de pasos ejecutados por un equipo de respuesta a incidentes para mitigar el impacto ocasionado por la ocurrencia de un incidente de seguridad

RIESGO INFORMÁTICO: Es el nivel de exposición de un sistema de información calculado con base en la probabilidad de ocurrencia de un incidente contra el impacto causado. Como lo indica ROMERO[9], el riesgo es el resultado de sumar el impacto producido por una amenaza y la probabilidad de que una vulnerabilidad permita que dicha amenaza tenga éxito.

[7] CONGRESO DE COLOMBIA. Ley 590 de 2000, Congreso de Colombia, establece los criterios para la clasificación de la micro, pequeña y mediana empresa.
[8] NIST, National Institute of Standars and Technology. Handling an Incident. En: Computer Security Incident Handling Guide
[9] ROMERO CASTRO, Martha Irene, et al. En: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Alcoy, 2018. p. 29

RESUMEN

El desarrollo de este proyecto establece un punto de partida para que principalmente las MiPymes que para el desarrollo de su funcionamiento y su actividad comercial tengan activos de información, puedan iniciar el análisis y posible implementación de una herramienta tecnológica basada en software libre que permita proteger parte de su infraestructura, específicamente los puntos finales (endpoints), de la creciente oleada de ataques informáticos que día a día amenazan con deteriorar e interrumpir sus actividades.

Una plataforma EDR (Endpoint and Detection Response) es una herramienta que apoya parte del proceso de gestión y respuesta a incidentes de seguridad de la información aportando información de valor de forma organizada y haciendo posible la ejecución de acciones según lo requerido, de acuerdo con cada una sus etapas. Se abordarán diferentes soluciones EDR ya existentes y ofrecidas al público por la comunidad open source, realizando un análisis sobre características como soporte ofrecido por la comunidad, requisitos de sistema, efectividad, entre otras, que al final darán sustento a la elección de una de ellas. Finalmente, con la plataforma EDR elegida, se analizará la implementación de la misma, identificando así su funcionamiento y elaborando la documentación que permita a cualquier persona o entidad replicar dicho proceso en su propia infraestructura tecnológica.

Debido a la naturaleza de las plataformas EDR, es fundamental abordar de forma paralela el tema de proceso de gestión y respuesta a incidentes de seguridad informática, entendiendo las acciones a realizar en cada una de sus etapas.

PALABRAS CLAVE: EDR, Incidente, evento, riesgo informático, vulnerabilidad, gestión de incidentes, malware.

ABSTRACT

The development of this project establishes a starting point so that mainly MSMEs that have information assets for the development of their operation and their commercial activity, can start the analysis and possible implementation of a technological tool based on open source that allows to protect part of your infrastructure, specifically the endpoints (endpoints), of the growing wave of computer attacks that every day threaten to deteriorate and interrupt your activities.

An EDR (Endpoint and Detection Response) platform is a tool that supports part of the management and response process to information security incidents by providing valuable information in an organized way and making it possible to carry out actions as required, according to each join its stages. Different EDR solutions already existing and offered to the public by the opensource community will be addressed, performing an analysis on characteristics such as support offered by the community, system requirements, effectiveness, among others, which in the end will support the choice of one of them. Finally, with the chosen EDR platform, its implementation will be analyzed, thus identifying its operation and preparing the documentation that allows any person or entity to replicate said process in their own technological infrastructure.

Due to the nature of EDR platforms, it is essential to address in parallel the issue of management process and response to computer security incidents, understanding the actions to be taken in each of its stages.

KEYWORDS: EDR, Incident, event, computer risk, vulnerability, incident management, malware.

INTRODUCCIÓN

Las plataformas EDR – Endpoint Detection and Response, son plataformas de seguridad informática que se encargan de brindar protección a los diferentes activos de información que hacen parte de la infraestructura tecnológica de una organización. Con una plataforma de este tipo, las empresas pueden disponer de un mecanismo efectivo que ayuda a prevenir que los sistemas informáticos sean vulnerados por amenazas conocidas, así como disponer de protección en tiempo real a través de análisis estático, dinámico, por comportamiento y, además, realizar acciones de contención como por ejemplo aislamiento de un sistema de la red informática, eliminación remota de archivos y administración remota de procesos. Adicionalmente, este tipo de herramienta permite en amplio grado la realización de tareas de investigación en los sistemas gestionados, logrando así la recopilación de información sobre actividad en archivos, procesos en ejecución, modificaciones en llaves de registro, entre otras. La importancia de contar con este tipo de plataformas consiste en que una vez una amenaza logra evadir los sistemas de seguridad perimetral y se infiltra en la red informática, puede ser detectada debido a su actividad y comportamiento en el sistema comprometido, permitiendo al equipo de respuesta a incidentes actuar de forma rápida para su contención y evitando su propagación a otros sistemas de información

Como punto de partida para el desarrollo del presente documento, se abordan conceptos generales acerca de la seguridad informática los cuales son el insumo principal para comprender de forma acertada la relación entre el tipo de plataforma tecnológica investigada (EDR) y los beneficios de su existencia dentro de la infraestructura tecnológica de las empresas independientemente de su tamaño, actividad comercial, sector económico u otros aspectos.

Posteriormente se abarcan aspectos generales sobre el proceso de respuesta a incidentes de seguridad informática el cual se constituye en la base del modo de operar de las herramientas tipo EDR. Se identifican las distintas fases que contiene este proceso tomando como base una metodología globalmente reconocida y se identifican algunas actividades que los profesionales de seguridad informática y en particular los miembros del equipo de respuesta a incidentes deben ejecutar dependiendo de la situación presentada.

Como parte final y con la intención de plasmar la teoría previamente analizada en un escenario práctico, se acudirá a distintas fuentes de información con el fin de investigar acerca de algunas herramientas EDR de código abierto para así, luego de comparar algunas de ellas en aspectos como funcionalidad, consumo de recursos de máquina, facilidad de administración, soporte del desarrollador o de la comunidad, entre otros, dar paso a la implementación y experimentación de diferentes casos de uso con una de ellas mediante lo que se denomina prueba de concepto

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

Con el paso del tiempo se ha evidenciado que la protección de la información en las compañías debe tenerse en cuenta como uno de los puntos clave si dentro de los objetivos de esta se encuentra el mantener su actividad con un alto grado de disponibilidad. Los ataques informáticos son una realidad y cuando una empresa es víctima de estos puede sufrir un impacto negativo de tal magnitud que, si no tiene un manejo apropiado del mismo, puede incluso verse obligada a cerrar su operación.

Según el informe del CCIT (Cámara Colombiana de Informática y Telecomunicaciones), en lo expuesto por su director ejecutivo, "El impacto que sufren las empresas colombianas luego de un ciberataque trasciende el coste económico por pérdidas de sus activos financieros y conlleva de manera colateral afectaciones a la productividad, daños reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y data sensible"[10]. Si bien, es cierto que el costo monetario de invertir en la adopción de herramientas para protección de la seguridad de la empresa es alto, el costo de no tenerlos cuando se es víctima de un ataque informático puede ser mucho mayor.

En el mismo informe como conclusión se menciona que "El 60% de las pequeñas y medianas empresas, no pueden sostener sus negocios más de seis meses luego de sufrir un ciberataque importante. Esto demuestra que los factores en torno a los Ciberataques a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías."[11] Cuando una empresa es víctima de un ataque informático, evidentemente tendrá una afectación económica, operativa y legal con la cual deberá lidiar durante algún tiempo, pero, si no dispone de las plataformas adecuadas para responder de forma óptima, la probabilidad de determinar el vector de ataque y los sistemas afectados con exactitud es muy baja, por lo cual, no se puede descartar que el mismo ataque recibido se presente nuevamente.

En la actualidad, tanto grandes empresas como pequeños comercios utilizan medios digitales para almacenar información (contable, proyectos, clientes, estrategias comerciales, etc.) y diferentes tecnologías para el desarrollo de su operación con lo cual los delincuentes informáticos tienen diversidad de objetivos para diseñar y ejecutar diferentes tipos de malware como virus, troyanos, ransomware, entre otros, de los cuales se hablará con detalle en el numeral 4.2.3, capaces de adentrarse en la infraestructura tecnológica y ocasionando afectación

[10] YOHAI, Alberto. TENDENCIAS CIBERCRIMEN COLOMBIA 2019 – 2020. Informe de las tendencias del cibercrimen en Colombia (2019-2020), 2019. p. 4
[11] Ibid., p. 31

de sistemas y pérdida o robo de información. Esta tendencia por parte de las organizaciones por el uso de tecnología en sus procesos se ha dado con lo que hoy en día se conoce como transformación digital, definida como "La transformación digital, es un concepto que involucra un proceso de explotación de tecnologías digitales que tiene la capacidad de crear nuevas formas de hacer las cosas."[12]. Como muestra de lo anterior, se puede observar en el Plan TIC 2018-2022 emitido por el Gobierno Nacional en relación con la evolución digital del país:

> En el más reciente estudio de caracterización de las MiPymes colombianas y su relación con las TIC, adelantado por el MinTIC en el 2017, se establecieron los niveles de apropiación de TIC en las empresas. Se encontró que la tenencia de diferentes herramientas o canales TIC, ha aumentado 10% en los último cuatro años, lo cual ha impulsado procesos de trasformación digital en las empresas. Del 2013 al 2017, el uso de páginas web pasó de 21% al 32%, las redes sociales del 27% al 45% y la tenencia de Internet del 61% al 74%.[13]

Si bien estas cifras corresponden al año 2017, son una muestra clara de su tendencia al aumento con lo que es muy probable que, a hoy, tres años después, el crecimiento de estas se haya dado en un mayor grado.

Las herramientas EDR son capaces de detectar y responder ante este tipo de amenazas, por ejemplo, si se habla de "Creeper", catalogado como el primer virus informático el cual aunque no fue creado con fines maliciosos, según lo expuesto por Loebenberger[14] presentaba un comportamiento típico de un virus, siendo entonces capaz de adentrarse en un sistema, ejecutar una tarea, propagarse a otros sistemas y eliminarse; una plataforma EDR detecta y está en la capacidad de aislar al sistema infectado y posteriormente a través de la misma, es posible extraer diferentes archivos de información para realizar la investigación forense y determinar vectores de ataque, modificaciones realizadas, conexiones intentadas así como diferentes indicadores de compromiso que permitirían una evolución de la postura de seguridad informática de la organización mediante la implementación de estos dentro de sus controles

Otro ejemplo a citar es el ataque de Ransomware "WannaCry", que como lo menciona Mattei[15], fue realizado a nivel mundial en mayo de 2017 logrando afectar a grandes compañías de diferentes sectores económicos como telecomunicaciones, automotriz, servicios financieros y de salud, entre otros, ante lo cual, muchas empresas vieron sus sistemas directamente afectados y otras optaron como medida de prevención apagar sus sistemas ocasionando en ambos

[12] Ministerio de Tecnologías de la Información y las Comunicaciones, Marco de la Transformación Digital para el Estado Colombiano, 2020. p. 13
[13] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Plan TIC 2018-2022 El Futuro Digital es de Todos. p. 40
[14] LOEBENBERGER, Daniel. Evolution! From Creeper to Storm: Presentation for the Seminar on "Malware". p. 2
[15] Estrada, Carlos. Estudio sobre el malware Ransomware. España. 2018. p. 79

casos indisponibilidad en los servicios ofrecidos y en el primero de ellos pérdida de información.

Para el caso concreto del país se puede deducir que los casos de Ransomware, aún son un gran dolor de cabeza para las compañías ya que, se ha observado que, "Colombia recibió el 30% de los ataques de Ransomware en Latinoamérica en el último año, seguido de Perú (16%), México (14%), Brasil (11%) y Argentina (9%). Las PYMES fueron el blanco preferido por los atacantes, pues conocen que los niveles de seguridad suelen ser más bajos en este tipo de compañías"[16]

Una plataforma EDR analiza constantemente el comportamiento de programas y procesos en los sistemas, está en la capacidad de detectar cuando se hace un cifrado masivo y recurrente de información, alertando y protegiendo de forma temprana y evitando que el causante de dicho comportamiento pueda replicarse a través de otros sistemas en la red informática.

Así como los ejemplos citados anteriormente, a diario se realizan miles de ataques informáticos en compañías de todo el mundo y es por esto que una plataforma EDR toma vital importancia para la protección de las organizaciones, pues cuando el sistema de seguridad perimetral falla, es insuficiente o si acaso la técnica utilizada por el delincuente informático es tan sofisticada que logra traspasar de forma desapercibida los controles de la empresa, sólo queda por detectar rápidamente y responder de la mejor forma ante tal incidente.

Ahora, y con relación a los ejemplos expuestos, puede surgir la pregunta de ¿Acaso este tipo de protección no la brinda un Antivirus? La respuesta a esto es, con base en lo mencionado por PETTERS[17]: Un antivirus en su forma esencial, se compone de una gran base de datos o firmas que se alimentan frecuentemente de acuerdo con las amenazas que este detecta en las distintas organizaciones a nivel mundial en donde se encuentre implementado y en otros casos, las generadas por grandes equipos de investigación de amenazas y ciber inteligencia. Un antivirus, detecta software malicioso y lo elimina, pero no está en la capacidad de detectar comportamientos sospechosos con lo cual las amenazas más comunes en la actualidad como por ejemplo las APTs (Advanced Persistent Threat), serían indetectables. Ahora, tal como lo menciona Cybriant[18], es válido decir que un Antivirus es un componente de una plataforma EDR y que esta última consiste en un conjunto de funciones de seguridad informática administradas de forma centralizada y que permiten una mayor protección, control y visibilidad de la

[16] CCIT, Cámara Colombiana de Informática y Telecomunicaciones. Informe Tendencias Cibercrimen Colombia 2019-2020. p. 19

[17] PETTERS, Jeff. Endpoint Detection and Response (EDR): Everything You Need to Know. En: www.varonis.com Junio 2020

[18] CYBRINT. Traditional Antivirus vs. EDR (Endpoint Detection and Response). En: https://cybriant.com

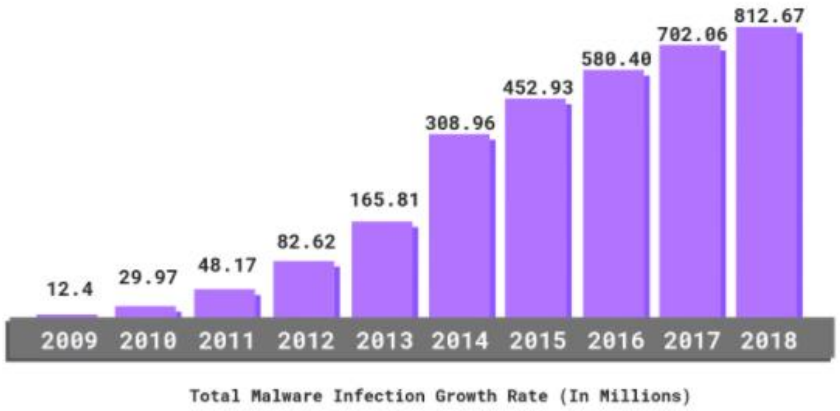
actividad realizada desde, hacia y dentro de los endpoints en la red informática de una organización.

1.2. FORMULACIÓN DEL PROBLEMA

Según lo informado por Puentes[19], las empresas día a día son objetivos de gran atracción para los delincuentes informáticos y el número de ataques informáticos perpetrados sobre estas es significativo y crece de forma acelerada, por lo cual, resulta conveniente que las organizaciones implementen una plataforma EDR que apoye los procesos de detección y respuesta a incidentes de seguridad informática.

En la siguiente figura se observa el crecimiento año tras año del crecimiento de muestras de malware desde el año 2019 de acuerdo con la estadística de una firma estadounidense consultora en ciberseguridad:

Figura 1. Crecimiento de Malware



Fuente: PURPLESEC LLC. 2020 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends [sitio web]. Virginia, Estados Unidos. PURPLESEC. [Consulta: 21 de noviembre de 2020]. Disponible en https://purplesec.us/resources/cyber-security-statistics/

El principal inconveniente y teniendo en cuenta que el enfoque de la presente monografía son las pequeñas y medianas empresas, se encuentra en la no disposición de recursos económicos dentro del presupuesto para la adquisición de una plataforma EDR y para los costos de su administración.

Entonces, ¿Deben las pequeñas y medianas empresas estar expuestas a las diferentes ciber amenazas que podrían afectar la continuidad del negocio debido a la falta de presupuesto?

[19] PUENTES,Juan. Empresas colombianas solo invierten 20% de presupuesto en ciberseguridad. En: larepublica.co Septiembre 2018

Es cierto que una plataforma EDR comercial tiene un costo elevado el cual puede variar dependiendo de factores como por ejemplo la cantidad de Endpoints a proteger, funcionalidades a implementar, soporte de fabricante, servicios de administración, entre otros, sin embargo, a través del desarrollo del presente escrito, se demostrará el cómo las herramientas EDR de software libre pueden ser una alternativa para las pequeñas y medianas organizaciones y cómo a través de ellas se consigue mejorar los índices de seguridad y la postura en seguridad informática frente a las amenazas que en todo momento están en constante evolución.

2. JUSTIFICACIÓN

Con base en el problema planteado, se hace importante brindar a la comunidad académica y profesional, una perspectiva bastante objetiva sobre algunas herramientas EDR open source, que permita mostrar su capacidad para detectar y contener las diferentes técnicas, tácticas y estrategias que a través de la informática son desarrolladas por los ciberdelincuentes.

Una plataforma EDR por lo general incluye diferentes módulos que aportan en gran medida a la protección de los puntos finales en una red, tanto servidores de información como equipos de usuario. Estos módulos funcionan como antimalware y anti-exploit, detectando comportamientos anómalos en un sistema informático y permitiendo su aislamiento de la red en caso de que se confirme que el mismo ha sido comprometido. Además, este tipo de plataformas permiten la realización de actividades post-incidente que son de gran valor para los equipos de investigación.

Con esta revisión bibliográfica, fácilmente las empresas podrán seleccionar e implementar una solución de tipo EDR en su infraestructura, haciendo frente a los diferentes tipos de ataques informáticos que se registran a diario, permitiendo tomar acciones a tiempo y evitando que un incidente desatado en un activo de información se extienda a través de la red.

De forma general algunos de los beneficios que podrían obtener las empresas al implementar una plataforma de este tipo son:

- Detección oportuna de dispositivos infectados mediante la observación de eventos de sistema, registros y procesos ejecutándose en los endpoint.
- Rápida contención de amenazas informáticas logrando detener la posible propagación de estas a otros dispositivos a través de la red, evitando así, que la afectación sea de gran impacto para la compañía.
- Permiten realizar actividades de investigación y recopilación de información detallada de los endpoint.
- Permiten a las organizaciones tener una visión general del estado de seguridad de sus endpoint y determinar los eventos que generan mayor riesgo con el fin de definir prioridades.
- Brindan la posibilidad de administrar fácilmente y de forma ágil determinadas funciones de los endpoint con el fin de generar acciones de contención y remediación.

Adicionalmente, existen diversas normas y estándares como por ejemplo COBIT, NIST, ISO, entre otros, que a través del tiempo han definido controles y estrategias con el fin de que las organizaciones dispongan de un marco de referencia para que teniendo en cuenta los diferentes frentes de su infraestructura tecnológica (Red,

Cloud, Endpoints, etc.) puedan prepararse ante la gran cantidad de amenazas a las que se encuentran expuestos.

Una herramienta EDR logra dar cumplimiento a muchos de los controles definidos por tales estándares. A continuación, se exponen los controles del estándar definido por el CIS (Center for Internet Security) relacionados a los endpoint para lo cuales las plataformas EDR pueden dar cumplimiento.

Tabla 1. Controles del estándar CIS relacionados a los Endpoint

CIS Subcontrol	Nombre	Descripción
8.1	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.
8.2	Ensure Anti-Malware Software and Signatures are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
8.4	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected
8.6	Centralize Anti-malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.
13.7	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.
13.8	Manage System's External Removable Media's Read/write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices
13.9	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest

Fuente: El autor

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Analizar diferentes Herramientas tipo Endpoint and Detection Response (EDR) de software libre para recomendar una propuesta de implementación en pequeñas organizaciones

3.2. OBJETIVOS ESPECÍFICOS

- Estudiar las características y funcionalidades de las herramientas EDR (particularmente proyectos open source), utilizadas en el fortalecimiento de la seguridad informática

- Analizar y comparar las diferentes soluciones EDR de tipo open source para identificar las ventajas y desventajas más significativas

- Analizar el proceso de instalación y afinamiento de una herramienta EDR de tipo open source para identificar la óptima configuración para su funcionamiento

- Documentar el proceso de instalación y configuración de una herramienta EDR Open source y su funcionamiento

4. MARCO REFERENCIAL

4.1. MARCO CONCEPTUAL

4.1.1. Endpoints. Según la definición dada por Palo Alto[20], los endpoint son sistemas informáticos que se comunican de ida y de vuelta con una red a la cual se encuentran conectados. Ejemplos de endpoint son: equipos de escritorio, portátiles, teléfonos inteligentes, servidores, dispositivos IoT (Internet de las cosas), entre otros. Según lo menciona el mismo autor, los dispositivos endpoint representan un punto de entrada y objetivo a vulnerar clave para los ciberdelincuentes ya que, cuando un ciberdelincuente logra comprometerlos desde allí logran la ejecución de código, explotación de vulnerabilidades, secuestro del sistema o de información, entre otras acciones. También, con la tendencia de las organizaciones por el teletrabajo se tienen usuarios que se conectan a los recursos internos de la compañía desde fuera de las instalaciones y desde cualquier lugar del mundo con lo que los endpoint son cada vez más susceptibles a ataques cibernéticos. La importancia de este tipo de dispositivos consiste en que dependiendo del tipo de endpoint pueden contener información sensible o ser fundamentales para los procesos y servicios de las organizaciones con lo cual algún evento de fuga de información o interrupción en su funcionamiento representará un impacto negativo de gran magnitud para la empresa.

4.1.2. Vulnerabilidades informáticas. Una vulnerabilidad en informática se traduce en una debilidad o un fallo en un sistema que hace que éste se encuentre expuesto a un ataque debido a un criterio de seguridad no considerado o una técnica de ataque nueva, poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información. Como lo menciona GÓMEZ[21], los orígenes de las vulnerabilidades en los sistemas informáticos se deben a fallos en sistemas físicos o lógicos, defectos de ubicación, instalación, configuración, mantenimiento, procedimientos mal definidos, entre otros.

> "La primera vulnerabilidad que puede suceder es que los diseñadores del sistema no sean capaces de prever todas las amenazas que existen o que pueden existir en el futuro, y como es imposible predecir el futuro, los sistemas siempre serán vulnerables. Otra vulnerabilidad, consecuencia de la anterior, es un mal diseño del protocolo, que en su momento parece ser lo suficientemente seguro; sin embargo, al ponerlo en práctica, se descubre ciertas debilidades que no eran tan evidentes al momento de su diseño"[22]

[20] Palo Alto Networks. What is an Endpoint? En: https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint 2020
[21] GÓMEZ VIEITES, Álvaro. Enciclopedia de la Seguridad Informática. Madrid. 2014.
[22] BARCA URBINA, Gabriel. Introducción a la seguridad informática. México D.F. 2016. p. 30

4.1.3. Incidente de seguridad. Como lo informa el NIST[23], un incidente de seguridad de la información hace referencia a la violación de las políticas de seguridad definidas.

> **"**Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.**"**

4.1.4. Informática forense. Es un proceso de investigación que se realiza sobre los sistemas informáticos con el fin de detectar y recopilar toda evidencia que sirva como soporte ante un proceso judicial. En este proceso de investigación, "se hace necesaria la aplicación de técnicas científicas y analíticas especializadas que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Entre las técnicas mencionadas se incluyen reconstruir el sistema informático, examinar datos residuales y explicar las características técnicas del uso aplicado a los datos y bienes informáticos."[24]

4.1.5. IoC (Indicador de compromiso). Según lo informa AUDEA[25] los Indicadores de Compromiso (IoC's), son un mecanismo altamente efectivo y de bajo costo para que las organizaciones puedan detectar de forma anticipada amenazas. Un IoC puede describir desde actividad maliciosa en un sistema identificando los elementos participantes, hasta incidentes de seguridad a través de patrones de comportamiento y otras características que pueden ser actualizadas. Los IoC's se comparten entre diferentes entidades y equipos de gestión de incidentes con el fin de que puedan ser implementados en las diferentes plataformas de seguridad como Firewalls, sistemas de detección y prevención de intrusos (IDS / IPS), plataformas de protección de endpoints, entre otros. Según lo evidenciado por JUMBO[26] cuando un sistema se encuentra comprometido, se encuentran evidencias como ficheros creados, entradas de registro modificadas, procesos o servicios nuevos, conexiones a direcciones IP o dominios sospechosos, que pueden constituirse en nuevos IoC's

---

[23] NIST, National Institute of Standards and Technology. Recommendations of the National Institute of Standards and Technology. En: Computer Security Incident Handling Guide. Estados Unidos. 2012. p. 6

[24] INCIBE, Instituto Nacional de Ciberseguridad. Una guía de aproximación para el empresario. En: Glosario de términos de Ciberegurudad. León. 2017. p. 24

[25] AUDEA. Indicadores de Compromiso en la gestión de riesgos. En: https://www.audea.com/indicadores-compromiso-la-gestion-riesgos/ 2018

[26] JUMBO, Tatiana. Metodología para el análisis de malware en un ambiente controlado. Cuenca, Ecuador. 2017 p. 49

4.2. MARCO TEÓRICO

4.2.1. Plataformas endpoint detection and response. Las herramientas EDR - Endpoint Detection and Response (Detección y respuesta en puntos finales) son soluciones de seguridad informática que permiten proteger los endpoints en una red (por lo general servidores y estaciones de trabajo), de amenazas informáticas las cuales con el paso del tiempo son más sofisticadas y de difícil detección.

Los ataques e infecciones informáticas no son nada nuevo y junto a los primeros ejemplares de ellos también surgieron los primeros software de Anti-Virus (AV) los cuales en su funcionamiento básico según Botte[27], operan mediante escaneos recurrentes y la comparación de los archivos de un sistema contra una base de firmas que se actualiza constantemente. Esta base de firmas se compone de datos que a nivel mundial el fabricante de la herramienta logra reunir e incluso datos compartidos de forma colaborativa con terceros para así determinar si algún archivo analizado coincide con dicha base de firmas generando así una alerta o un bloqueo según como se encuentre configurado.

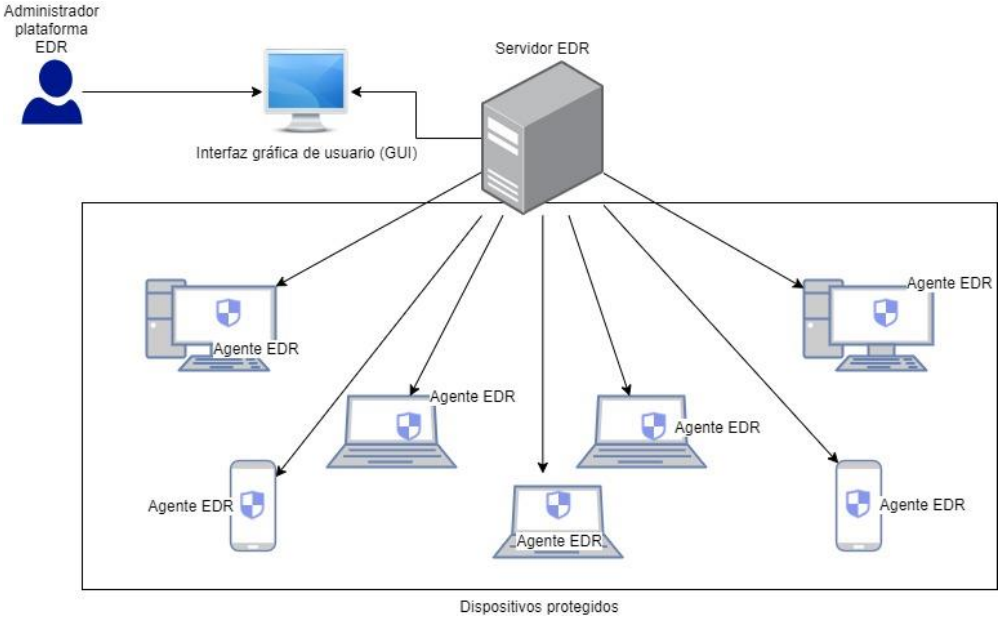
A diferencia del software Anti-Virus, los EDR además de tener estas mismas capacidades para detectar si un archivo es o no malicioso, tienen funcionalidades como detección de amenazas con base en comportamiento, monitoreo de servicios y procesos, protección con base en IoC's, módulos anti-exploit, entro otros. De acuerdo con lo señalado por Gattie[28] una plataforma EDR está en la capacidad de detectar ataques Zero-day, ataques de ransomware y ataques de malware sin archivos, lo cual un Anti-Virus convencional no podría. Para la protección con base en IoC's, las plataformas EDR están en capacidad de realizar analítica teniendo en cuenta IoC's definidos por el administrador de la herramienta y/o IoC's que son recopilados por la plataforma EDR a través de conexiones e integraciones con servicios de inteligencia en la nube.

Por lo general, la arquitectura básica de ese tipo de soluciones consta de una consola(servidor) de gestión y agentes (software) que se despliegan en los dispositivos a proteger. Desde esta consola se realizan actividades como visualizar el estado de los dispositivos protegidos (Endpoints – Puntos finales), definición y actualización de IoC's, toma de acciones sobre los dispositivos gestionados y otras tareas que ayudan en el proceso de investigación para dar respuesta a un incidente de seguridad informática.

[27] BOTTE, Antoine. Antivirus, epp and edr what differences? Vanves. 2020

[28] GATTIE, Ian. Why Endpoint Detection and Response (EDR) is Superior to Your Current Antivirus (AV) Tools. En: https://avaloncybersecurity.com/ New York. 2018.

Figura 2. Arquitectura de una plataforma EDR



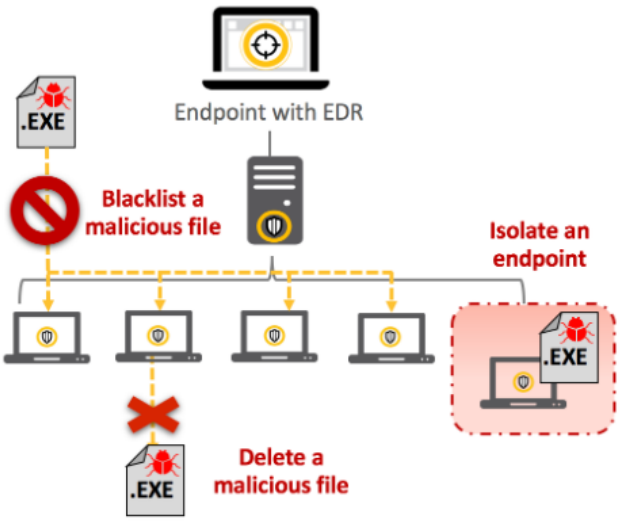
Fuente: El autor

Este tipo de soluciones de seguridad informática, a diferencia de los programas de antivirus convencionales, tiene un enfoque hacia el tratamiento de incidentes de seguridad que se puedan presentar en los dispositivos por lo que además de proteger a los dispositivos contra amenazas informáticas puede realizar actividades de reportes, análisis en tiempo real, análisis forense e incluso, como lo menciona Cynet[29]aislamiento de la red en caso de detectar un sistema comprometido con el fin de evitar la etapa conocida como “Movimiento lateral” en el ciclo de vida del malware.

En la siguiente figura se observan algunas de las acciones que puede realizar un EDR cuando se encuentra instalado en un sistema: Bloquear un archivo malicioso, detectar y crear un IoC al detectar un archivo malicioso, aislar un sistema que ha sido comprometido.

[29] CYNET. Endpoint protection and EDR. En: www.cynet.com New York

Figura 3. Actividad de un EDR



Fuente: Cyber Security Information Portal. Multilayered Defense for Endpoint. [sitio web]. Hong Kong. [Consulta: 21 de noviembre de 2020]. Disponible en: https://www.cybersecurity.hk/en/expert-2018-07-25-endpoint.php

Existen diferentes alternativas para las empresas a la hora de pensar en la implementación de una solución de tipo EDR en su infraestructura de seguridad. Diferentes gigantes y proveedores de plataformas de seguridad como FireEye, Symantec, Checkpoint, Rapid7, Palo Alto Networks, entre otros, ofrecen soluciones EDR que por lo general son de alto costo.

Más adelante, en el capítulo 5, se revisarán diferentes alternativas de soluciones EDR de código libre que si bien, no cumplen al cien por ciento las funcionalidades que se pueden obtener con una solución de pago, son una excelente alternativa a tener en cuenta cuando dentro de las compañías por diversas razones no se destinan los recursos necesarios para la protección de los activos de información

4.2.2. Proceso de gestión y respuesta a incidentes. El proceso de gestión y respuesta a incidentes de seguridad informática tiene por objetivo dar tratamiento de forma procedimental y organizada a la materialización de un riesgo buscando minimizar el impacto producido por el mismo. “Los incidentes de seguridad son situaciones que pueden causar un gran daño en nuestros entornos (sistemas de información, personas, negocios, etc.); por este motivo es importante tener la capacidad, en primer lugar, de prevenirlos, y en segundo, de detectarlos y de responder adecuadamente a ellos.”[30] De forma general, este proceso involucra diferentes etapas las cuales permiten tener un panorama general acerca de los factores que intervienen antes, durante y después de la presentación de un

[30] INCIBE, Instituto Nacional de Ciberseguridad. ¿Qué camino debo seguir para gestionar correctamente un incidente de seguridad en mi empresa? España, 2014.

incidente. Contar con un proceso de gestión de incidentes en las organizaciones ayuda a identificar con rapidez la materialización de un riesgo y a tomar las acciones apropiadas para darle el mejor tratamiento.

El proceso de gestión de incidentes se compone de varias etapas (Preparación, Identificación, Contención, Erradicación, Recuperación, Lecciones aprendidas) las cuales a su vez se componen de diferentes actividades que permiten dar tratamiento a un incidente desde incluso antes de su inicio (Proactivamente) hasta su final.

El proceso de respuesta a incidentes, de acuerdo con lo mencionado por Optaris[31] debe definirse a la medida de cada organización teniendo en cuenta factores como la misión, el tamaño, el sector económico, su objeto social, entre otros. Lo anterior, se sustenta por ejemplo en el hecho de que tiene mayor probabilidad de ser blanco de un ataque una entidad financiera en lugar de una ONG dedicada a la protección de la población infantil. Luego de definido el proceso de respuesta a incidentes, este debe madurar con el paso del tiempo a la vez que aumenta su eficacia tanto en asertividad como en tiempo de respuesta.

Internacionalmente existen diferentes metodologías/normativas aceptadas que definen el proceso de respuesta a incidentes dentro de las organizaciones (ISO 27035, NIST 800-61, SANS, entre otras). A continuación, se muestra el proceso establecido por el instituto SANS para la respuesta a incidentes, el cual será tomado como base para la explicación de las diferentes etapas:

Figura 4. Proceso de respuesta a Incidentes - SANS

Fuente: SANS Institute. Information Security Reading Room. Malware 101 - Viruses [documento electrónico]. [Consulta: 22 de noviembre de 2020]. Disponible en: https://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848

4.2.2.1. Preparación. Esta fase inicial permite que el equipo de respuesta a incidentes CSIRT se encuentre capacitado y en condiciones para dar respuesta a un incidente de seguridad. En esta fase el equipo CSIRT adquiere el conocimiento

[31] OPTARIS. Guía de planificación de respuesta a incidentes para 2019. En: www.optaris.com. Buenos Aires. 2017.

sobre las herramientas dispuestas para la protección y monitoreo de los activos de información y define contactos y procedimientos a activar en caso de presentación de un incidente.

Algunas actividades iniciales en esta etapa según lo indica SANS[32] son:

- **Definición de herramientas**: Se definen las herramientas, plataformas tecnológicas y mecanismos que permitirán detectar la ocurrencia de un incidente de seguridad.
- **Valoración de activos**: Se define el nivel de criticidad de los activos de información.
- **Definición de indicadores de compromiso**: Se establecen los criterios a monitorear por las herramientas para definir en qué condiciones la ocurrencia de un evento será clasificada como incidente de seguridad.

La Preparación es una etapa de suma importancia ya que determina el nivel de capacidad de respuesta por parte del CSIRT para dar respuesta a cualquier posible afectación que se pueda dar sobre los sistemas de información, ya sea desde un evento fortuito como un desastre natural o un corte de energía o ataques dirigidos, efectuados por delincuentes informáticos.

En esta fase, Kral[33] propones las siguientes actividades como puntos clave para tener un CSIRT correctamente preparado:

- **Establecer políticas de seguridad**: Definir dentro de la organización reglas que limiten la actividad de los empleados y que definan las consecuencias que acarrearían su incumplimiento. Por ejemplo: Acceso no autorizado a sistemas informáticos, uso inadecuado del ancho de banda, envío de información clasificada, entre otros. Lo anterior se puede controlar mediante la implementación de banners de inicio de sesión, cláusulas en el contrato de trabajo y acuerdos de confidencialidad, respectivamente.

- **Definir un plan de actuación**: El CSIRT debe establecer un flujo de acciones a realizar, una vez confirmado el incidente. De este modo, surgen diferentes estrategias que el CSIRT empleará, dependiendo de variables como por ejemplo la cantidad de usuarios afectados, el tipo de servicio afectado, la criticidad del servicio afectado, entre otros. Además, mediante la creación de los diferentes flujos, el CSIRT puede notar y establecer la forma de contacto con otras áreas, de las cuales dependerían las acciones a tomar.

[32] KRAL, Patrick. Incident Handler's Handbook. En: SANS Institute Information Security Reading Room. 2011. p. 2
[33] KRAL, Patrick. Incident Handler's Handbook. En: SANS Institute Information Security Reading Room. 2011. p. 3

- **Establecer un plan de comunicación**: Se debe definir una base de datos de contactos a través de la cual se logre determinar con exactitud las personas a las que se les debería contactar para lograr mitigar el incidente. De no contarse con esta base de datos, el tiempo de afectación incrementará considerablemente y así mismo el impacto ocasionado sobre la compañía.

- **Documentar**: Es de gran utilidad que todos los procesos llevados a cabo por el equipo de respuesta a incidentes tales como extracción de logs, generación/restauración de backups, reinicio de servicios, reinicio de máquinas, ejecución de comandos, etc., queden documentados. Esta documentación puede ser utilizada posteriormente como evidencia ante un proceso judicial y a su vez, se convierte en una base de conocimiento que ayudará al CSIRT a la definición de controles a implementar.

- **Equipo multidisciplinario**: El CSIRT debe ser conformado no solo por personas involucradas con la informática. Dados los diferentes contextos en los que se puede presentar un incidente de seguridad informática, la participación de funcionarios de áreas como finanzas, derecho, recursos humanos, etc., puede resultar en aportes significativos que permitan dar respuesta a un incidente con mayor rapidez.

- **Definir un conjunto de herramientas (Jump-Bag)**: Como lo comenta KRAL[34], esta actividad consiste en poner a disposición del CSIRT un conjunto de herramientas software/hardware, que puedan ser de utilidad para la gestión del incidente de seguridad.

- **Entrenamiento**: Cada miembro del CSIRT debe recibir capacitación acerca del proceso de manejo de incidentes y de forma específica debe conocer con exactitud su campo de acción o su participación en el mismo. Es importante realizar de forma periódica, simulacros de ataques informáticos que permitan identificar debilidades y fortalezas dentro del CSIRT.

4.2.2.2. Identificación. En esta fase se analizan las alertas generadas por las herramientas de seguridad y se determina la ocurrencia o no de un incidente de seguridad. Se revisan dispositivos implementados dentro de la infraestructura tecnológica de la organización que controlan y monitorean la actividad de la red y la actividad en los sistemas de información, con el fin de determinar la presentación o no de un incidente de seguridad informática. Se analiza cualquier actividad sospechosa a través de la red y/o sistemas con el fin de determinar con exactitud si un riesgo se ha materializado, en cuyo caso se activará el procedimiento correspondiente de acuerdo con lo definido en la etapa de Preparación.

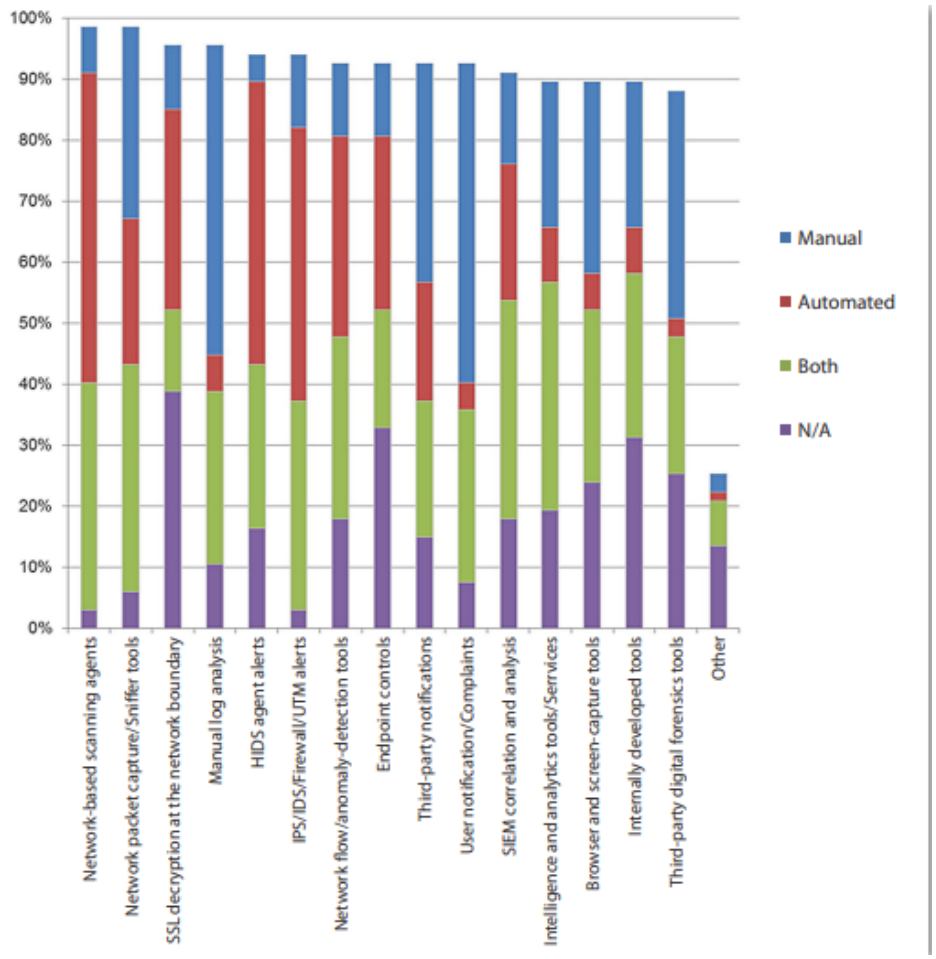
[34] KRAL, Patrick. The Incident Handlers Handbook. EEUU. 2011. p. 4

Algunas fuentes de información pueden ser:

- Plataformas EDR
- Herramientas de Antivirus
- Firewalls
- Plataformas IPS/IDS
- Plataformas de correlación (SIEM)
- Herramientas de monitoreo de servidores de archivo y bases de datos (FAM/DAM)

En la siguiente figura se aprecia el porcentaje de uso de diferentes herramientas de seguridad que las organizaciones utilizan para la detección de sistemas en estado de compromiso

Figura 5. Métodos de detección



Fuente: SANS. Incident Response: How to Fight Back. [Documento electrónico]. [Consulta: 23 de noviembre de 2020]. Disponible en: https://csbweb01.uncw.edu/people/cummingsj/classes/mis534/articles/ch3_ir_sanssurvey.pdf

Es importante en esta etapa que se notifique a todos los miembros del CSIRT quienes cumplirán los roles definidos en la anterior etapa para cada integrante. Luego de confirmada la ocurrencia del incidente informático, se abre un gran número de posibilidades de cómo tal hecho se pudo haber dado, ante lo cual, es importante tener diferentes perspectivas acerca de los acontecimientos; aquí la importancia de que el CSIRT esté compuesto por profesionales de diferentes disciplinas.

En esta fase es conveniente realizar la clasificación y categorización del evento presentado. La clasificación define si el evento corresponde a un falso positivo ante lo cual se documentará y se dará cierre al mismo, en caso contrario, se declarará la presentación de un incidente de seguridad informática. En este último caso, se asignará una categoría (Malware, Phishing, DoS, DDoS, XSS, SQL Injection, etc.) al incidente presentado la cual determinará su tratamiento.

Dentro de la fase de identificación se debe encontrar la respuesta a los siguientes interrogantes, que como lo menciona Bandos[35] ayudarán a interpretar con mayor claridad la situación presentada y dará una ruta a seguir para encontrar la solución:

- ¿**Quién** es el autor del ataque? ¿Es un individuo o una agrupación? ¿es un ataque dirigido?

- ¿**Por qué** se realizó el ataque? ¿El atacante busca un beneficio económico? ¿Se busca interrumpir y afectar la credibilidad de la organización? ¿Corresponde a hacktivismo?

- ¿**Qué** resultó afectado luego del ataque? ¿**Cuál** fue el objetivo principal del atacante? ¿**Cuáles** activos de información fueron intervenidos o manipulados por el atacante?

- ¿**Cómo** se realizó el ataque?: Se busca plasmar en una línea de tiempo la actividad ejecutada por el atacante. ¿Cuál fue su metodología? ¿A qué tipo de ataque pertenece? ¿Logro acceso no autorizado a la red de la organización a través de vulnerabilidades de los sistemas o acaso mediante ingeniería social obtuvo información importante?

- ¿**Dónde** se originó el ataque? ¿El atacante es alguien externo o interno a la organización? ¿Geográficamente el atacante tuvo que estar cerca o dentro de la organización? ¿Todo el ataque pudo ser ejecutado de forma remota?

- ¿**Cuándo** se inició el ataque y cuánto tiempo duró? ¿Cuánto tiempo estuvo el intruso dentro de los sistemas?

[35] BANDOS, Tim. THE FIVE WS OF INCIDENT RESPONSE. Boston. 2016

Figura 6. The five Ws (and one H)

Fuente: Information Age. The five Ws (and one H) of effective incident response. [Sitio web]. Londres. [Consulta: 23 de noviembre de 2020]. Disponible en: https://www.information-age.com/five-ws-and-one-h-effective-incident-response-123461486/

Como parte final de esta etapa, se entrega una valoración del riesgo para la cual se tiene en cuenta el impacto del incidente. Esta variable determina la prioridad con la cual se debe dar atención al incidente y el tiempo en el cual debe ser resuelto. Existen varias formas de determinar esta variable las cuales dependen de la metodología para el análisis de riesgo establecida en la organización.

4.2.2.3. Contención. Una vez el equipo CSIRT ha determinado el compromiso en un sistema, se despliegan acciones con el fin de mitigar los efectos del ataque, tanto en el sistema comprometido como en dispositivos cercanos en la red. En esta fase de contención, se pretende reducir al mínimo el impacto ocasionado sobre la organización, por lo cual, con el fin de lograr una rápida actuación ante los hechos, es recomendable contar con una lista de actividades que el equipo CSIRT podría ejecutar. Como lo señala Torres[36]Algunas de estas actividades pueden ser:

- Aislamiento de un sistema informático o de un segmento de red
- Análisis estáticos sobre sistemas informáticos con el fin de detectar malware y ejecutar las acciones de remediación
- Apagado de sistemas de información
- Actualización de sistemas
- Puesta en operación de sistemas de respaldo (Contingencia o alta disponibilidad)

Es importante tener en cuenta que, en esta fase, además de buscar la no expansión del daño a través de la infraestructura de la organización, se deben preservar los sistemas comprometidos como evidencias y material que servirá para un posterior

[36] TORRES, Alissa. Incident Response: How to Fight Back. [Documento electrónico]. Disponible en https://csbweb01.uncw.edu/people/cummingsj/classes/mis534/articles/ch3_ir_sanssurvey.pdf 2014 p. 17

análisis forense. Se deben tomar imágenes forenses para su posterior análisis con herramientas como Forensic Tool Kit (FTK), EnCase. Autopsy, entre otras

4.2.2.4. Erradicación. Luego de ser contenido, se inician las acciones para eliminar los efectos ocasionados por el ataque en el sistema y cualquier cambio que la actividad maliciosa pueda haber ocasionado. Se inspeccionan detalladamente los registros del sistema con el fin de determinar si queda rastro alguno del atacante. De forma adicional, en esta fase se debe hacer un esfuerzo por mejorar la seguridad de los sistemas o infraestructura vulnerada para evitar que el atacante consiga infiltrarse nuevamente por lo menos usando el mismo medio.

Dentro de esta fase se realizan acciones como:

- Restauración de copias de seguridad o imágenes de disco con un punto de restauración justamente anterior al primer momento en que el atacante se infiltró en los sistemas.
- Análisis y limpieza de los sistemas de archivos con herramientas que puedan inspeccionar todo tipo de archivos, llaves de registro, procesos y servicios.
- Aplicación de actualizaciones y parches de seguridad en los sistemas.

4.2.2.5. Recuperación. Luego de que los sistemas han sido limpiados, con esta etapa de recuperación se busca nuevamente retronarlos a su ambiente normal de operación revirtiendo las acciones realizadas anteriormente para su contención. Luego de esto, se debe mantener un monitoreo constante de los sistemas que permita saber si su comportamiento es acorde a los esperado o por si lo contrario están presentando de nuevo un comportamiento sospechoso lo que podría indicar que algún componente del sistema sigue aún comprometido y podría nuevamente detener la operación de este.

Como lo sugiere Kral[37], algunas acciones recomendadas para ejecutar durante esta fase son:

- Realizar pruebas sobre los sistemas que permitan identificar si su respuesta es o no acorde a lo esperado.
- Establecer el tiempo que sería necesario mantener el monitoreo para decidir si la recuperación ha sido o no exitosa.
- Tener definido un Umbral de datos que permita definir cuando un sistema está funcionando dentro o fueras de los valores normales (Tiempos de respuesta, consumo de recursos, Temperatura, etc)

4.2.2.6. Lecciones aprendidas. Se recopila y organiza la documentación generada durante cada una de las fases anteriores con el fin de generar acciones de mejora que contribuyan a evitar la ocurrencia nuevamente del mismo incidente u otros

[37] KRAL, Patrick. The Incident Handlers Handbook. EEUU. 2011. p. 8

similares. Como entregable surge un informe que detalla paso a paso la ocurrencia del incidente y el manejo dado por el equipo CSIRT desde su detección, análisis y respuesta.

Este documento se convierte en una fuente de información de suma importancia que incluso servirá como medio de capacitación para toda la organización o específicamente para nuevos miembros del equipo CSIRT.

Junto al informe detallado es conveniente elaborar una presentación para exponer ante los altos directivos de la organización de forma entendible la situación presentada, la afectación causada y las acciones tomadas para solucionarlo. El mensaje debe ser contundente y debe transmitir con claridad la importancia de la implementación de nuevos controles, herramientas y procesos que mitiguen de raíz los riesgos que se han identificado.

Según lo expresa Karl[38], es recomendable que dicha presentación contenga por lo menos la siguiente información:

- Momento inicial en que se detectó el incidente
- El alcance de la afectación
- Acciones tomadas por el CSIRT para contener y erradicar
- Acciones realizadas por el CSIRT para la recuperación
- Áreas con las cuales el CSIRT interactuó para llevar a cabo las acciones en cada una de las fases
- Acciones que, durante el proceso de respuesta a incidentes, el CSIRT identificó que necesitan mejoras
- Un estimado de costos generados por la atención del incidente (Tiempo extra laborado, contrato de proveedores, tiempo de indisponibilidad de algún servicio, etc)

4.2.3. Malware y amenazas informáticas. Las amenazas informáticas pueden ser entes externos o internos a las organizaciones que tienen como fin el aprovechamiento de vulnerabilidades de los sistemas y así lograr fines específicos como robo de información, secuestro de datos y sistemas, suplantación, robo de identidad, indisponibilidad de servicios, entre otros. Para lograr esto, los delincuentes informáticos utilizan diferentes métodos y desarrollan su propio "software" para así adentrarse de manera ilegítima dentro de la infraestructura tecnológica de las empresas. A continuación, se listan algunas categorías de amenazas informática comunes:

4.2.3.1. Malware. Por malware se entiende todo código malicioso que ha sido desarrollado con el fin de traspasar el esquema de seguridad de los sistemas

[38] Ibid., p. 9

poniendo en riesgo la confidencialidad, integridad y disponibilidad de estos. Según lo indica MONAPPA[39] el malware es distribuido por los ciberdelincuentes a través de diferentes vectores de ataque como correo electrónico, sitios web, oculto dentro de otro software aparentemente legítimo, entre otros y una vez alojado en el sistema víctima se ejecuta y se replica a través de la red. Se acuerdo con lo señalado por el mismo autor, este tipo de software maligno se puede presentar como ejecutables, scripts, porciones de código, entre otros. Según lo menciona AVG[40] existen diferentes tipos de malware como virus, troyanos, spyware, gusanos, ransomware, adware, botnet, entre otros, cuya razón de existencia generalmente se basa en la obtención de fines económicos o como mecanismo de protesta.

4.2.3.2. Ingeniería social. Es el acto en el cual un atacante pretende engañar a la víctima conduciéndola a realizar alguna acción a partir de falsa información. De acuerdo con lo indicado por OWASP[41], la ingeniería social es un conjunto de técnicas psicológicas y habilidades sociales, como por ejemplo la persuasión, la influencia y la sugestión con las que un atacante busca directa o indirectamente que una víctima revele información confidencial sin ser consciente del riesgo que esto conlleva. Este mismo autor también señala que los ataques de Ingeniería social son altamente efectivos y fáciles de realizar ya que no necesariamente se requiere de medios tecnológicos y además se realizan directamente sobre un recurso humano el cual es considerado como el eslabón más débil cuando se habla de seguridad de la información.

4.2.3.3. Exploit. Según lo afirmado por Cisco[42], un exploit consiste en un fragmento de código desarrollado específicamente para la explotación de una vulnerabilidad en un sistema. Básicamente es la ejecución de código que un atacante ha diseñado con el fin de aprovechar un "hueco" de seguridad y así adentrarse en un sistema.

4.2.3.4. Botnet. Es un grupo de sistemas que luego de ser infectados empiezan a ser parte de la red del atacante y ejecutan órdenes recibidas desde un servidor de comando y control (c2c). "Cada equipo infectado con este tipo de malware se denomina computadora zombi, porque queda a merced del cibercriminal. Es él quien tiene el control del equipo, usándolo para diferentes tipos de actividades delictivas."[43]

---

[39] MONAPPA, K, A. En: Learning Malware Analysis. Birmingham, Reino Unido. 2018. p 7

[40] AVG. ¿Qué es el malware? Cómo funciona el malware y cómo eliminarlo?. En: https://www.avg.com/es/signal/what-is-malware. 2020

[41] OWASP, The Open Web Application Security Project. En: Ingeniería Social, Hacking Psicológico. OWASP Latam Tour. República Dominicana. 2016.

[42] CISCO, What Is an Exploit? En: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html

[43] PEREZ, Ignacio. ¿Qué es una botnet? Conoce al control remoto de los ciberdelincuentes. En: https://www.welivesecurity.com/la-es/2014/08/06/botnets-control-remoto-ciberdelincuentes/ 2014

4.2.3.5. Phishing. Según lo define Forcepoint[44], el phishing consiste en el uso de comunicaciones electrónicas de forma fraudulenta con el fin de engañar a usuarios y extraer información confidencial. En este tipo de ataque, el ciberdelincuente pone a disposición de la víctima por ejemplo un portal falso en internet o un formulario de ingreso de datos falso, diseñado a semejanza de un sitio genuino, con el fin de engañar al usuario quien al no contar con las medidas pertinentes terminará ingresando la información.

4.3. MARCO LEGAL

En la legislación colombiana, las acciones delictivas que se desarrollen desde, hacia o directamente sobre sistemas informáticos o de telecomunicaciones son penalizados a través de la Ley 1273 de 2009[45]. Esta ley abarca diferentes eventos que pueden representar la situación de alguna organización cuando está bajo un incidente de seguridad y es en el momento de la investigación y recopilación de evidencias en donde el contar con una Plataforma EDR toma vital importancia, pues permite conocer información detallada de procesos, servicios, archivos, usuarios, direcciones de red y mucha más información involucrada que conducirá a la adjudicación de los hechos a un sujeto.

Para una situación de Acceso abusivo a un sistema informático, una plataforma EDR permite conocer el usuario que ha sido comprometido, fecha y hora exacta del acceso, tiempo total de actividad, origen del acceso y dependiendo de si la plataforma EDR está configurada para ello, es posible evidenciar la actividad realizada por el atacante sobre el sistema infectado.

Si ahora, se habla de un escenario de Obstaculización ilegítima de sistema informático o red de telecomunicación, puede asociarse perfectamente a un ataque de DoS (denegación de servicio) en el cual un servicio o sistema de la organización está bajo un estado de indisponibilidad debido a una sobrecarga de procesos ocasionada por el actuar de un delincuente informático (múltiples peticiones, peticiones malformadas, peticiones desde muchos clientes, etc.). En este caso, una plataforma EDR puede identificar el comportamiento anormal de la red y el sistema afectado para que rápidamente se pueda iniciar la etapa de respuesta. Además, durante las actividades de investigación, la plataforma EDR proporcionará información de bastante utilidad para determina el vector de ataque.

4.4. ANTECEDENTES

Así como la tendencia de los ciberdelincuentes consiste en crear y diseñar día a día nuevas alternativas para perpetrar la seguridad de las organizaciones,

[44] FORCEPOINT. What is Phishing? Phishing Attacks and Prevention Explored. En: https://www.forcepoint.com/es/cyber-edu/phishing-attack

[45] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009. Bogotá. 2009

afortunadamente también surgen comunidades e individuos cuyo interés por defender la infraestructura tecnológica de las empresas los llevan a investigar y desarrollar herramientas capaces de detectar y responder a tal actividad maliciosa. Es así como a través de la web se encuentra variedad de informes y proyectos académicos enfocados en el estudio y testeo de plataformas de seguridad informática que permiten a la sociedad disponer de una pila de oportunidades con las cuales hacer frente a la ciberdelincuencia es posible,

Muestra de lo anterior lo evidencia el Trabajo final de Master en seguridad de la información y de las comunicaciones, elaborado por Bello[46], en el cual, conceptualiza acerca de las plataformas EDR, muestra su arquitectura e indica el estado actual de este tipo de soluciones en la industria tecnológica. También, expone acerca de diferentes plataformas EDR de código abierto eligiendo algunas de ellas para la realización de prueba de concepto. Por último, realiza un análisis de resultados con la información obtenida en las PoC definiendo cuatro ítems de evaluación: Habilidad para detectar incidentes, contención de incidentes, soportar la investigación del incidente y proporción de mecanismos para remediación de los endpoint afectados.

También se observa en el desarrollo del trabajo de grado para Master en ciencias de Ciberseguridad elaborado por Liggett[47] la importancia de las plataformas EDR en las empresas. En este, el autor inicialmente introduce conceptos relacionados con amenazas informáticas. Posteriormente abarca parte del proceso de gestión y respuesta a incidentes y relaciona algunas de sus etapas con el funcionamiento de las plataformas EDR. Como punto final, el autor expone su perspectiva futurista para las EDR, introduciendo el concepto de XDR como la tecnología que posiblemente remplace o mejor, complemente el funcionamiento actual de los EDR y menciona las capacidades de estos en ambientes con dispositivos BYOT e IoT.

[46] BELLO VIEDA, Jaime Andrés. Soluciones Endpoint Detection and Response Open-Source. Estado del arte, propuesta de medición, análisis y evaluación para determinar su implementación y aplicabilidad en ambientes empresariales. España, 2019

[47] LIGGETT Terry. Evolution of endpoint detection and response platforms. New York. 2018

5. ANÁLISIS DE HERRAMIENTAS TIPO ENDPOINT AND DETECTION RESPONSE (EDR) OPEN SOURCE

Las herramientas open source son una gran alternativa para que las empresas integren diferentes plataformas de seguridad dentro de su infraestructura tecnológica cuando el factor económico es un limitante. Así, es habitual encontrar sistemas como Firewalls, IPSs, IDSs, SIEMs, entre otros, desarrollados y soportados por proyectos y comunidades de código abierto, implementados y gestionados en diferentes organizaciones.

Haciendo un recorrido por la web se logran identificar para cada tipo de plataforma algunas herramientas open source las cuales se relacionan en la siguiente tabla

Tabla 2. Plataformas de seguridad open source

SIEM	Firewall	IPS / IDS
Apache Metron	Pfsense	Snort
AlienVault OSSIM	OPNSense	Suricata
Wazuh	IPFire	OSSEC
ELK Stack	SmoothWall	Security Onion
SIEMonster	Untangle Firewall	Bro Network Security Monitor

Fuente: El autor

También, realizando la búsqueda acerca de soluciones EDR ofrecidas por la comunidad open source, se encontraron diferentes alternativas. Sobre estas, se ha realizado una investigación a fondo con el fin de compararlas y elegir una de ellas para su posterior implementación.

Si bien, es notorio que con una solución EDR de código abierto no se logran resultados tan eficaces como con plataformas EDR de pago, también es notorio que el costo que una empresa tendría que asumir para adquirirla es alto; y no es que sea una mala inversión con el fin de salvaguardar la información teniendo en cuenta que en la actualidad este es el activo de mayor valor para las organizaciones; sin embargo, y siguiendo el enfoque del problema planteado para el desarrollo de esta monografía, las pequeñas y medianas empresas puede que no dispongan de mayor presupuesto para realizar este tipo de inversiones. Por esto, se puede asegurar que la implementación de una herramienta EDR de tipo open source, aportará un significativo apoyo para las pequeñas y medianas empresas en la protección de la información y la respuesta a incidentes de seguridad informática que se puedan presentar.

En la opinión de Rodríguez[48], con las diferentes plataformas Open source que existen, es posible la implementación de un potente SOC

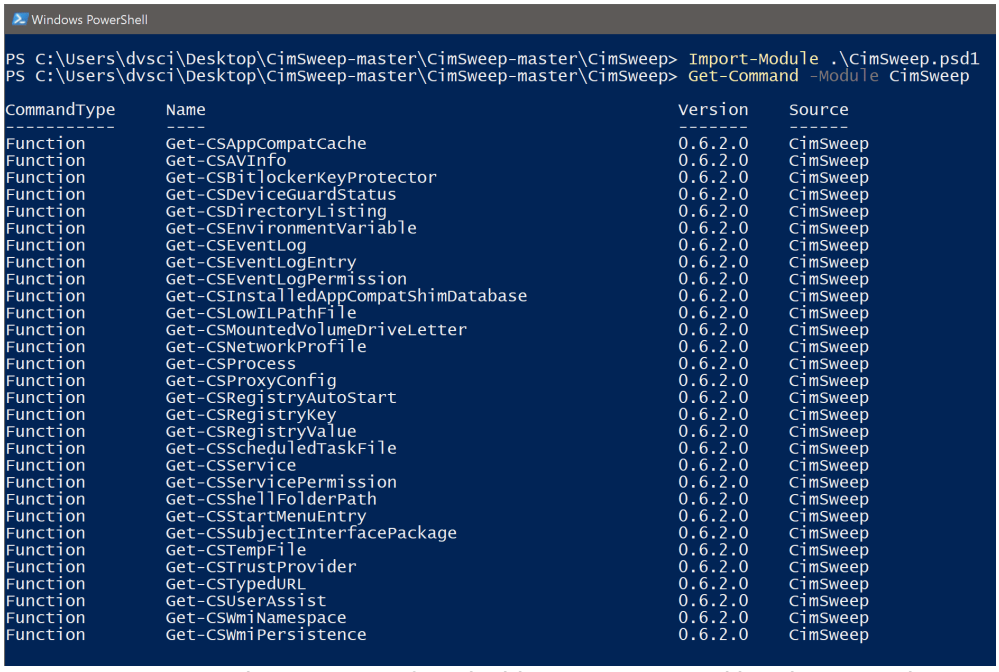
5.1. INVESTIGACIÓN Y ANÁLISIS DE HERRAMIENTAS OPEN SOURCE

5.1.1. CimSweep. Es un conjunto de herramientas basadas en CIM y WMI, que funcionan a través de PowerShell, tiene la particularidad de no requerir la instalación de un agente en los sistemas a analizar, pues trabaja con los cmdlets CIM. Es una potente herramienta que permite realizar actividades para detección y respuesta de incidentes en sistemas operativos Windows.

Actualmente se encuentra en la versión 0.6.1.1 (08 de junio de 2017), requiere como mínimo la versión 3.0 de powershell.

Se muestra en la siguiente figura una porción de las funciones incluidas en la herramienta a través de las cuales es posible extraer información importante de los sistemas administrados, lo cual, resulta de bastante utilidad en actividades de detección de amenazas e investigación

Figura 7. EDR CIMSweep



Fuente: GRAEBER, Matt. CimSweep: perform incident response and hunting operations remotely. [sitio web]. 2018. [Consulta: 25 de noviembre de 2020]. Disponible en: https://securityonline.info/cimsweep-perform-incident-response-and-hunting-operations-remotely/

[48] RODRÍGUEZ, Guillermo. En: Como implementar un potente SOC con herramientas Open Source. DragonJARCON Conferencia. Manizales, 2020

5.1.1.1. Requisitos de la plataforma. Para el uso de esta plataforma se identificaron los siguientes requerimientos:

- En el sistema de análisis (en el cual se ejecutará el CIM) se requiere Power Shell versión 3 o posterior.
- Se requiere ejecución de Power Shell en el sistema de análisis, con usuario que tenga permisos de administrador en los endpoints.
- Lo endpoints sólo pueden tener como sistema operativo Windows, a partir de XP.

5.1.1.2. Ventajas. A continuación, las ventajas identificadas de esta plataforma:

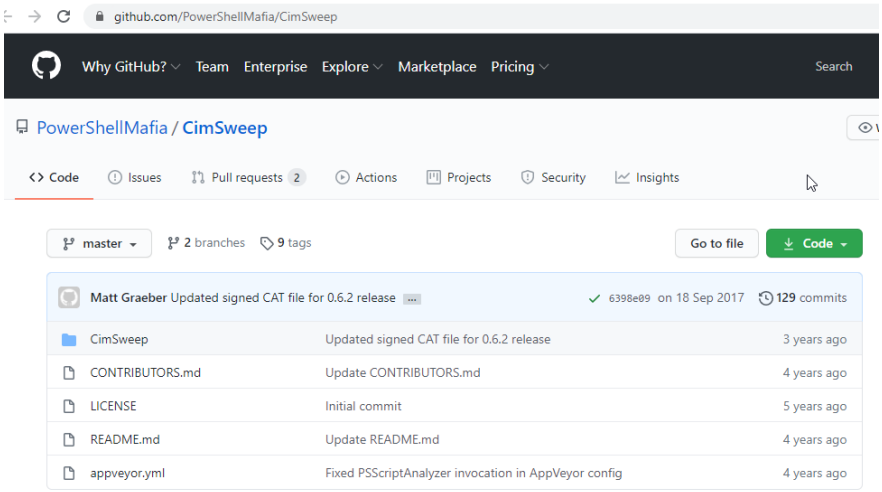
- No requiere instalación de agente en los sistemas endpoint
- Permita recopilar información de los sistemas de forma rápida
- El uso de recursos en cada sistema es mínimo
- Su instalación es sencilla, sólo se requiere la ejecución de una instrucción de instalación de módulo a través de Power Shell

5.1.1.3. Desventajas: A continuación, las desventajas identificadas de esta plataforma:

- Sólo funciona para endpoints con sistema operativo Windows
- Requiere un conocimiento medio en PowerShell y scripting
- No dispone de una interfaz gráfica para administración
- Requiere de otras utilidades para poder realizar acciones como aislamiento de sistemas

A continuación, el repositorio oficial de la herramienta en github en donde se encontrará información acerca del proyecto y documentación para su implementación:

Figura 8. Repositorio de CimSeep en github



Fuente: CimSweep. [Sitio web]. Proyecto CimSweep. [Consulta: 29 de noviembre de 2020]. Disponible en https://github.com/PowerShellMafia/CimSweep

5.1.2. GRR Rapid Response. Es una herramienta para respuesta a incidentes de seguridad. Está desarrollada en Python tanto para el agente el cual se debe implementar en cada uno de los sistemas sobre los cuales se quiere supervisar como para el servidor desde el cual se realiza la administración de la plataforma

Una vez desplegado el servidor, desde este se pueden realizar o programar diferentes acciones sobre los sistemas a través de los agentes como por ejemplo investigación a través de consulta de información de archivos, procesos, eventos; o toma de acciones como eliminación de archivos o aislamiento del sistema. Al realizar la implementación del servidor, se cuenta con los componentes:

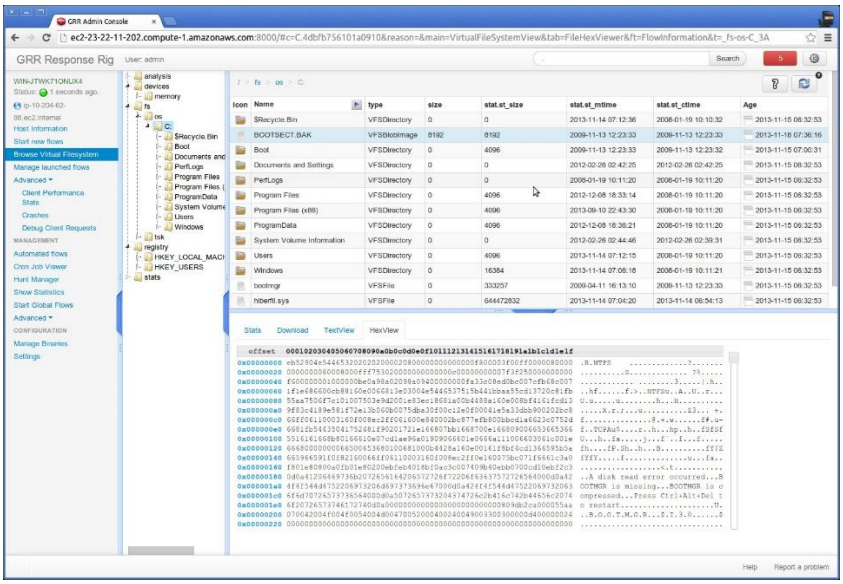
- Datastore: Se encarga del almacenamiento de información y administrar la comunicación entre los diferentes componentes.
- Front End Servers: Se encargan de capturar las solicitudes de los clientes para que puedan ser procesadas por el servidor GRR
- Worker: Se encargan de procesar la data capturada por los Front End. Es un componente que puede escalar de acuerdo con los requerimientos del entorno.
- Web UI: Es la aplicación central que permite al administrador de la plataforma realizar las actividades de respuesta a incidentes en los sistemas cliente.

Figura 9. EDR GRR - Rapid Response logo

Fuente: GRR RAPID RESPONSE. [imagen]. [Consulta: 23 de noviembre de 2020]. Disponible en: https://raw.githubusercontent.com/google/grr/gh-pages/img/grr_logo_real_sm.png

En la siguiente figura se observa la interfaz de la consola de administración de esta plataforma

Figura 10. Google GRR. Rapid response dashboard



Fuente: DARKNET ORG. Google Rapid Response (GRR) – Remote Live Forensics For Incident Response. [sitio web]. 2016. [Consulta: 23 de noviembre de 2020]. Disponible en: https://www.darknet.org.uk/2016/04/google-rapid-response-grr-remote-live-forensics-for-incident-response/

5.1.2.1. Requisitos de la plataforma. De acuerdo con la documentación, los requisitos para la implementación del servidor de GRR varían según la cantidad de sistemas cliente que se quieran administrar, así como según el enfoque para el cual se vaya a utilizar la herramienta (consultas e informes, recuperación de archivos, contención de sistemas, etc.). Por ejemplo, para un caso de uso con 15000 sistemas cliente, se recomienda un servidor con al menos 128GB de RAM y procesador de 16 núcleos.

La instalación del servidor GRR recomendada corresponde al sistema operativo Ubuntu Xenial. Wl motor de base de datos utilizado por la plataforma es mysql.

5.1.2.2. Ventajas. A continuación, las ventajas identificadas de esta plataforma:

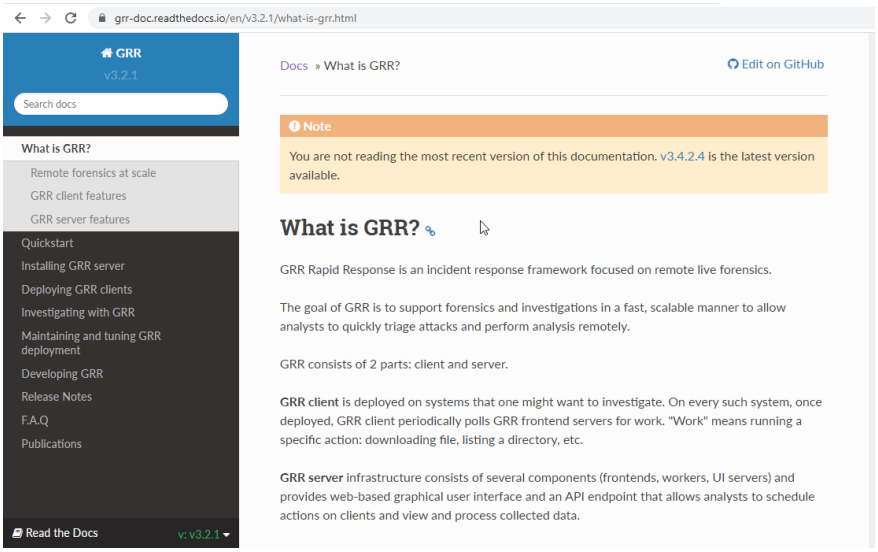
- Tiempo de respuesta muy bajo
- Dispone de Interfaz gráfica para la administración
- Tiene soporte para Endpoints con sistemas operativos Windows, Linux, Mac,
- Tiene una sólida documentación y soporte de la comunidad Open Source.

5.1.2.3. Desventajas. A continuación, las desventajas identificadas de esta plataforma:

- El proceso de instalación es extenso y dispendioso
- Los recursos de hardware requeridos para la implementación son elevados
- Es óptimo para grandes entornos. No es buena alternativa para pequeñas empresas
- Es invasivo, pues requiere la instalación de agentes en los endpoint a proteger

A continuación, el repositorio oficial de la herramienta en donde se encontrará información acerca del proyecto y documentación para su implementación.

Figura 11. Repositorio en Sitio oficial de GRR



Fuente: GRR Rapid Response. [Sitio web]. GRR Rapid Responde Documentation. [Consulta: 29 de noviembre de 2020]. Disponible en: https://grr-doc.readthedocs.io/en/v3.2.1/what-is-grr.html

5.1.3. TheHive. Es una plataforma para respuesta a incidentes de seguridad bastante popular por su eficiencia y usada en gran medida por CSIRTs, SOCs, entre otras áreas dedicadas al tratamiento e investigación de eventos de seguridad informática. Tiene un amplio desarrollo y se integra fácilmente con otras herramientas que permiten monitorear y responder rápidamente ante la ocurrencia de eventos de seguridad, tomando acción sobre los dispositivos administrados. Esta plataforma está en constante evolución, cuenta con una sólida documentación y

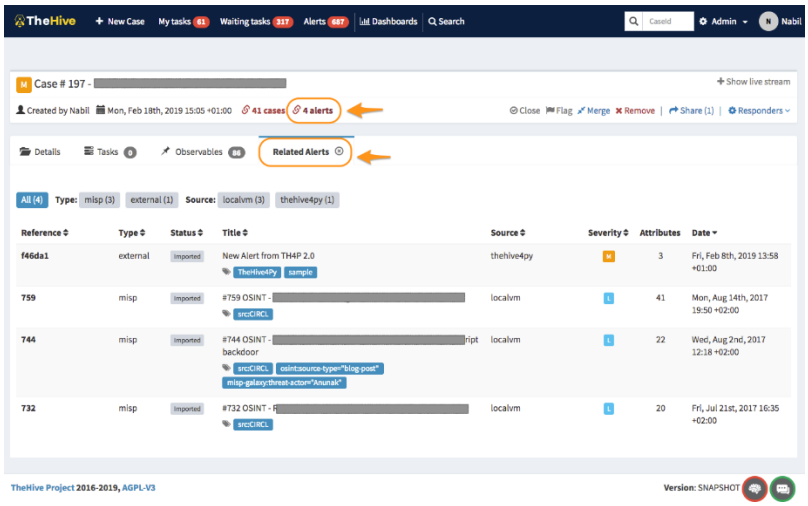
frecuentemente dispone de actualizaciones. Esta plataforma utiliza elasticsearch para el almacenamiento de la data y se vale de Cortex, plataforma también Open Source como motor de análisis por lo que permite una poderosa correlación de la información conseguida y así mismo una rápida detección de anomalías.

Figura 12 The Hive Project Logo

Fuente: THE HIVE PROJECT. [sitio web]. 2019. [Consulta: 21 de diciembre de 2020] Disponible en https://blog.thehive-project.org/tag/dashboards/

En la siguiente figura se observa uno de los dashboards de la plataforma

Figura 13. The Hive Dashboard



Fuente: THE HIVE PROJECT. Dashboards. [sitio web]. 2019. [Consulta: 21 de diciembre de 2020] Disponible en https://blog.thehive-project.org/tag/dashboards/

5.1.3.1. Requisitos de la plataforma. De acuerdo con la documentación, en cuanto a los requisitos para la implementación de The Hive, se recomienda el aprovisionamiento de una máquina virtual con 8vCPU, 8 GB of RAM and 60 GB of disk. Para el despliegue se cuenta con diferentes alternativas: RPM, DEB, DOCKER, entre otros.

5.1.3.2. Ventajas. A continuación, las ventajas identificadas de esta plataforma:

- Tiempo de respuesta muy bajo
- Dispone de Interfaz gráfica para la administración.
- Uso de elasticsearch como motor de analítica.

- Tiene una sólida documentación y soporte de la comunidad Open Source.

5.1.3.3. Desventajas. A continuación, las desventajas identificadas de esta plataforma:

- Está orientado al manejo y respuesta de incidentes en general y no se enfoca en Endpoints.
- Requiere de otros componentes para lograr la gestión de los endpoint

A continuación, el sitio web y repositorio oficial de la herramienta en donde se encontrará información acerca del proyecto y documentación para su implementación.

Figura 14. Repositorio en sitio web de The Hive

Fuente: The Hive Project. A 4-IN-1 SECURITY INCIDENT RESPONSE PLATFORM [Sitio web]. [Consulta: 29 de noviembre de 2020]. Disponible en: https://thehive-project.org/

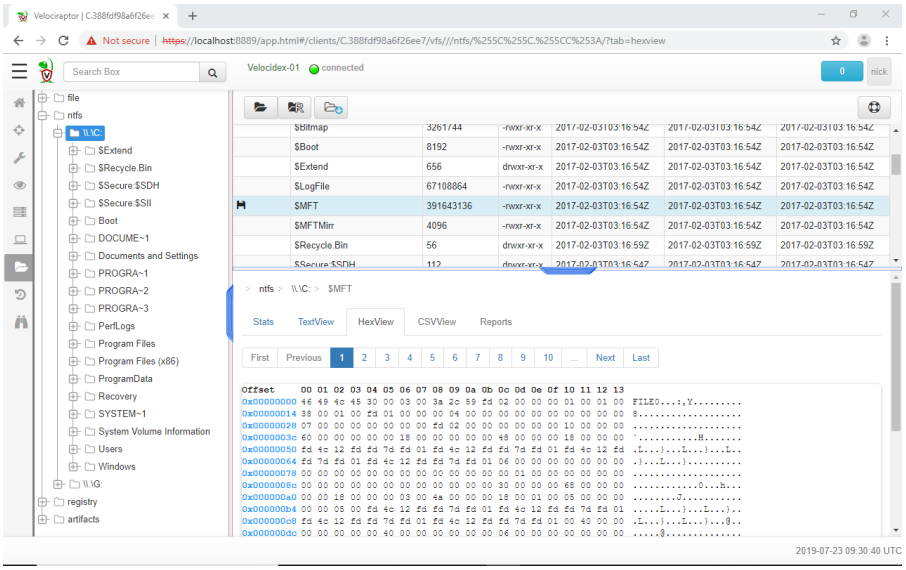
5.1.4. Velociraptor. Es una plataforma avanzada para monitoreo y protección de Endpoints que permite la recopilación de información forense y la ejecución de acciones de respuesta en los mismos ante la ocurrencia de incidentes de seguridad. con esta herramienta se obtiene gran visibilidad de situaciones que pueden desencadenar un incidente de seguridad tales como propagación de malware a través de la red, uso de dispositivos USB para extracción de información y se logra un constante monitoreo de la actividad en los endpoints logrando la correlación de diferentes eventos en diferentes periodos de tiempo.

Figura 15 Velociraptor EDR Logo

Fuente: VELOCIRAPTOR. Velocidex sitio web oficial. [sitio web]. 2020. [Consulta: 21 de diciembre de 2020]. Disponible en: https://www.velocidex.com/

En la siguiente figura se observa la interfaz de usuario de la plataforma en la ejecución de una de sus funciones:

Figura 16. Velociraptor Interfaz de usuario



Fuente: VELOCIRAPTOR. Examine remote files. [sitio web]. 2020. [Consulta: 21 de diciembre de 2020]. Disponible en: https://www.velocidex.com/

5.1.4.1. Requisitos de la plataforma. De acuerdo con la documentación, se encuentran tres tipos de implementación y dependiendo de cual se elija, los requerimientos de hardware pueden variar:

- **Standalone**: Se instala la herramienta en un solo servidor que a la vez hace de cliente. Posteriormente se pueden desplegar otros clientes.
- **Cloud**: Se despliega la herramienta en un entorno cloud (Google Cloud, Azure, AWS, entre otros).

- **Triage Mode**: Se despliega la herramienta en un servidor y se despliegan agentes en los endpoint a monitorear.

La instalación típica inicia con el modo Standalone para lo cual, en cuanto a requisitos de hardware, lo recomendado es contar con 4GB de Memoria, 2 core VM y el espacio en disco depende de la cantidad de endpoints a gestionar y de la cantidad de tiempo que se desee almacenar la información

5.1.4.2. Ventajas. A continuación, las ventajas identificadas de esta plataforma:

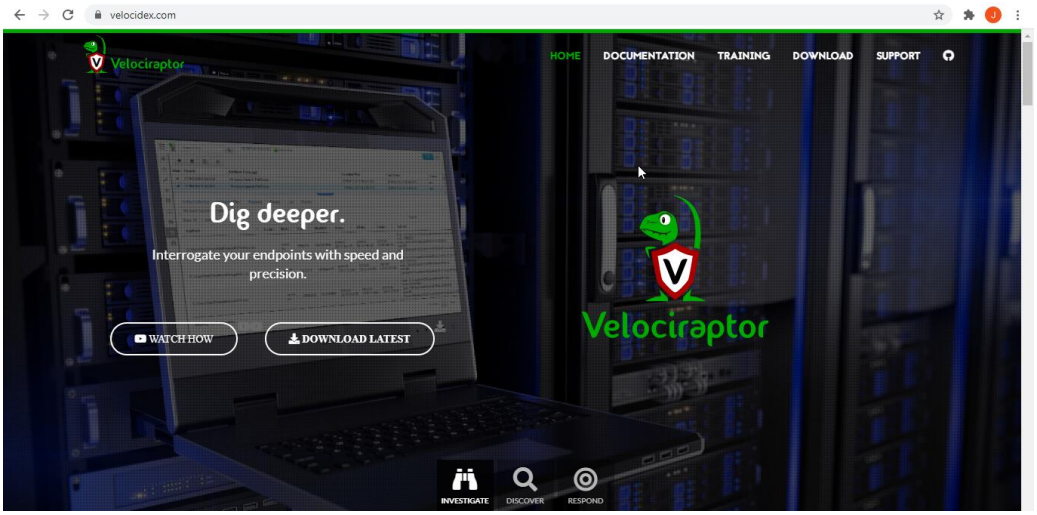
- Tiempo de respuesta muy bajo
- Dispone de Interfaz gráfica para la administración.
- De fácil implementación
- Está enfocado hacia sistemas endpoint
- Tiene una sólida documentación y soporte de la comunidad Open Source.

5.1.4.3. Desventajas. A continuación, las desventajas identificadas de esta plataforma:

- Lanzó su primera versión (Alpha) en agosto de 2018 lo cual transmite la sensación de ser una plataforma inestable o inmadura

A continuación, el sitio web y repositorio oficial de la herramienta en donde se encontrará información acerca del proyecto y documentación para su implementación.

Figura 17. Repositorio en sitio web te Velociraptor



Fuente: VELOCIRAPTOR. Velocidex sitio web oficial. [sitio web]. 2020. [Consulta: 21 de diciembre de 2020]. Disponible en: https://www.velocidex.com/

5.2. ANÁLISIS COMPARATIVO DE LAS PLATAFORMAS EDR

En la siguiente tabla se cuantifica las características dadas en el punto anterior bajo la siguiente definición: 1 = Malo/Bajo, 2 = Medio, 3= Bueno/Alto

La plataforma que obtuvo la mejor puntuación promedio fue elegida para implementación

Tabla 3. Análisis comparativo de plataformas EDR

Característica	Descripción	CimSweep	GRR Rapid Response	The Hive	Velociraptor
Implementación	Facilidad en la implementación	3	1	1	2
Administración	Facilidad en la administración de la plataforma EDR	2	2	2	3
Soporte	Soporte ofrecido por la comunidad open source	2	3	3	3
Recursos de sistema	Es liviano en consumo de recursos de CPU, RAM, Espacio en disco	3	2	2	3
Afinidad a MIPYMES	Ideal para implementar en MiPymes teniendo en cuenta la cantidad de endpoints a supervisar	2	1	2	3
GUI	Dispone de Interfaz gráfica para administración y es amigable	1	2	3	3
Bases de conocimiento	Dispone de amplia documentación	1	3	3	2
PROMEDIO		**2,0**	**2,0**	**2,3**	**2,7**

Fuente: El autor

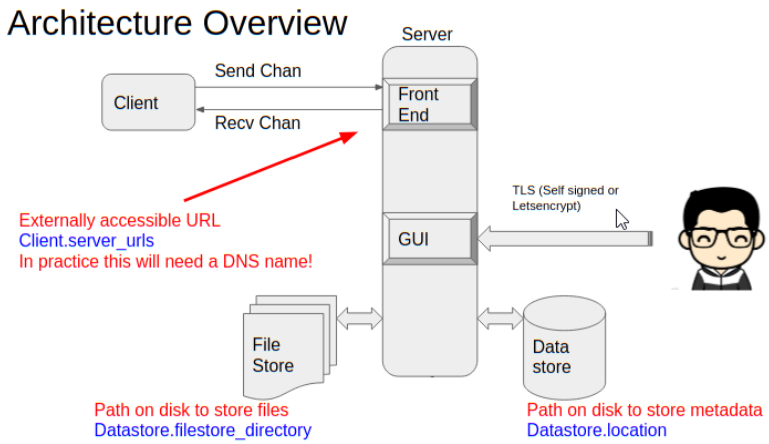
La plataforma EDR a implementar y testear es Velociraptor la cual obtuvo un puntaje de 2,7 sobre un máximo de 3.0

Vale la pena aclarar que los puntajes asignados a las plataformas en cada una de las características son totalmente subjetivos y se han asignado con base en lo que el autor de esta revisión bibliográfica ha podido evidenciar en diferentes canales de información en la web como foros, videoconferencias, canales de streaming, entre otros.

6. IMPLEMENTACIÓN Y PRUEBA DE LA PLATAFORMA VELOCIRAPTOR

Se implementó la plataforma EDR inicialmente en el modo Standalone con lo cual el servidor, también hizo las veces de cliente. Luego, se realizó la modificación en los archivos de configuración con el fin de integrar otros clientes. La siguiente figura es una vista general de la arquitectura de la plataforma Velociraptor:

Figura 18. Arquitectura Velociraptor



Fuente: VELOCIRAPTOR. Velocidex sitio web oficial. [sitio web]. 2020. [Consulta: 21 de diciembre de 2020]. Disponible en: https://www.velocidex.com/docs/getting-started/stand_alone/

A continuación, se describe el entorno en el cual se realizó la implementación de la plataforma Velociraptor versión 0.5.3 y la realización de pruebas sobre su funcionamiento

- Servidor EDR: Centos 8.2
- Cliente0: Centos 8.2
- Cliente1: Windows 10
- Cliente2: Windows 7

6.1. CONCEPTOS IMPORTANTES EN VELOCIRAPTOR

6.1.1. Cliente: En velociraptor, un cliente es simplemente un endpoint que tiene en ejecución un agente de velociraptor.

6.1.2. VQL: Velociraptor, como herramienta rápida para detección y respuesta de incidentes informáticos actúa en los endpoints a través de un lenguaje propio denominado VQL (Velociraptor Query Language), con el cual, se realizan consultas a los endpoints sobre su estado y se extrae información para análisis forense.

A continuación, se muestra la sintaxis básica de una consulta con VQL:

Figura 19. Sentencia VQL

Fuente: VELOCIRAPTOR. Velocidex sitio web oficial. [sitio web]. 2020. [Consulta: 21 de diciembre de 2020]. Disponible en: https://www.velocidex.com/docs/vql_reference/

Se puede observar que la sintaxis es muy similar al lenguaje SQL empleado en bases de datos, sin embargo, sólo soporta operaciones básicas y a diferencia de SQL, VQL funciona para bases de datos dinámicas. La sintaxis mostrada anteriormente permite identificar que una consulta de VQL conlleva uno valores de "columna" los cuales hacen referencia a los valores que serán mostrados de la información devuelta por el parámetro "plugin"

6.1.3. Artefactos. Los artefactos no son más que conjuntos de sentencias VQL empaquetados los cuales permiten realizar consultas mucho más estructuradas sobre los clientes. Velociraptor tiene definidos una gran cantidad de artefactos clasificados por sistema operativo y en su mayoría categorizados según el propósito: Información del registro de sistema, aplicaciones, detección de malware, remediación, entre otros. Algunos ejemplos son:

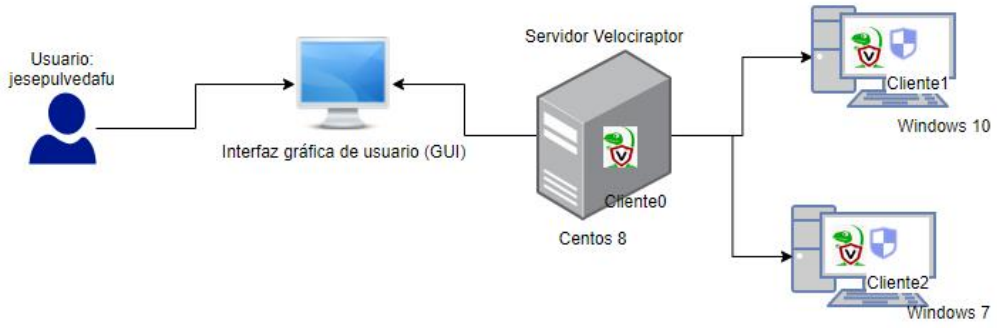
- Generic.Applications.Office.Keywords: Realiza búsqueda de archivos con extensiones de Micosoft Office
- Generic.Client.Info: Recolecta información básica de un cliente
- Generic.Client.Stats: Muestra información estadística acerca de los recursos de cómputo de un cliente
- Network.ExternalIpAddress: Detecta la dirección IP externa de un cliente
- Windows.Memory.Acquisition: Extrae una imagen completa de la memoria del cliente
- Windows.Search.FileFinder: Realiza búsqueda de archivos con base en el nombre de archivo o en el contenido
- Windows.Detection.ProcessMemory: Escanea la memoria en busca de una poderosa e invasiva técnica de ataque
- Linux.Syslog.SSHLogin: Extrae de los registros de autenticación los intentos de inicio de sesión a través de SSH

6.1.4. Hunts: Consiste en la ejecución de tareas sobre los clientes con el fin de extraer información muy específica lo cual resulta bastante útil cuando se ha definido un nuevo Indicador de compromiso y se requiere determinar el compromiso real sobre los equipos dentro de la red. La información recopilada puede ser descargada posteriormente para análisis e investigación.

6.2. ARQUITECTURA PARA LA IMPLEMENTACIÓN

Se muestra a continuación la arquitectura de red sobre la cual se desarrolló la implementación y prueba de funcionamiento de la herramienta velociraptor

Figura 20. Arquitectura para desarrollo de la práctica



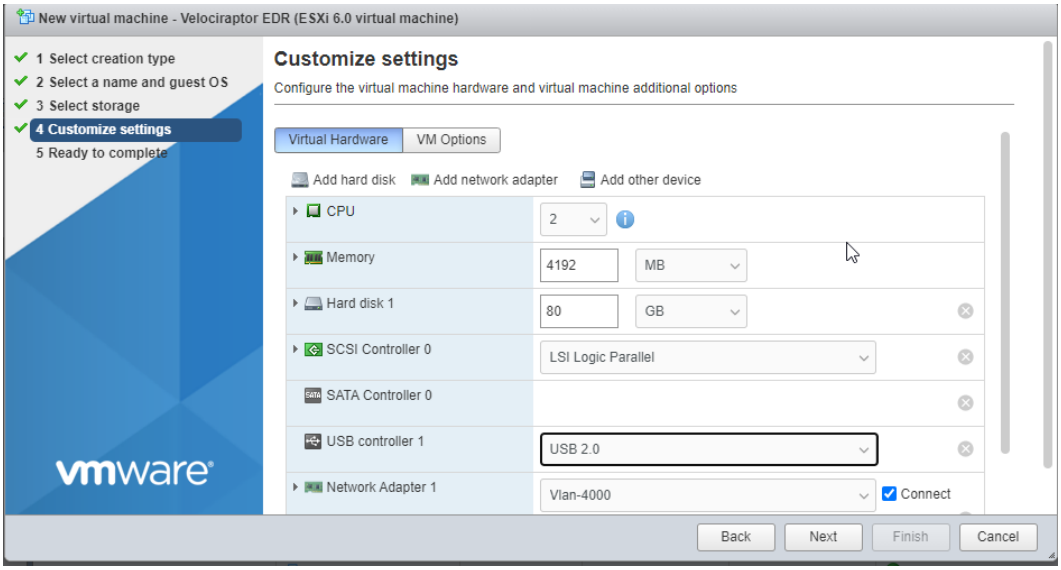
Fuente: El autor

6.3. IMPLEMENTACIÓN DEL SERVIDOR VELOCIRAPTOR

Se describe a continuación la máquina virtual creada en la cual se instaló el servidor Velociraptor la cual dispone de las siguientes características

- CPU: 2vCPU
- Memoria RAM: 4GB
- Espacio en disco: 80GB

Figura 21. Creación de máquina virtual servidor EDR

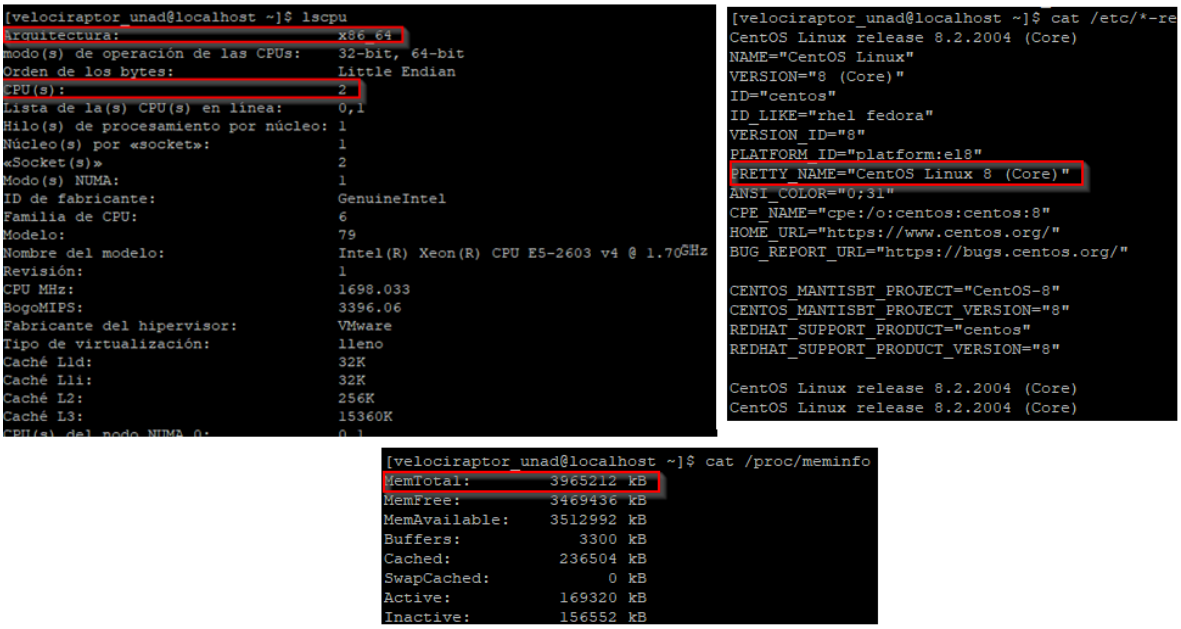


Fuente: El autor

Se verifican los recursos de máquina del servidor creado con los siguientes comandos:

lscpu
cat /etc/.release*
cat /proc/meminfo

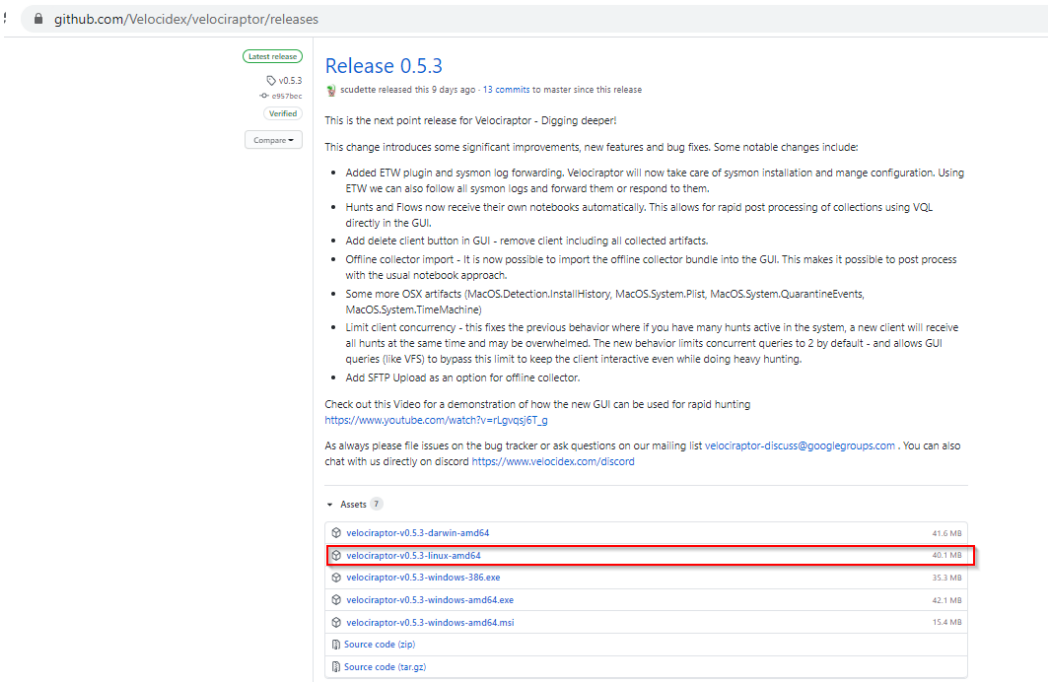
Figura 22. Verificación recursos de hardware servidor Velociraptor



Fuente: El autor

Se accede a https://github.com/Velocidex/velociraptor/releases repositorio oficial en GitHub desde el cual se realizará la descarga

Figura 23. Repositorio de Velociraptor en GitHub

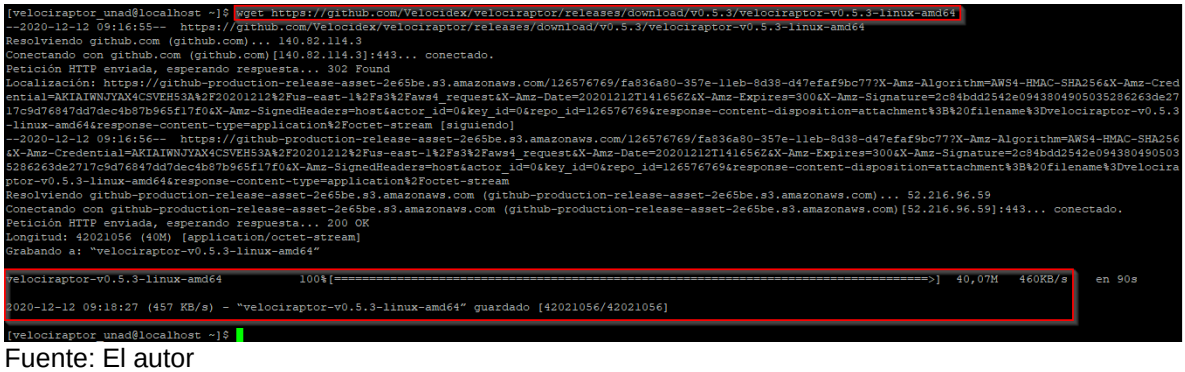


Fuente: El autor

Se realizó la descarga del software con la siguiente instrucción:

wget https://github.com/Velocidex/velociraptor/releases/download/v0.5.3/velociraptor-v0.5.3-linux-amd64

Figura 24. Descarga de Velociraptor



Fuente: El autor

Se otorgaron permisos de ejecución al archivo descargado con la siguiente instrucción:

chmod +x velociraptor-v0.5.3-linux-amd64

Figura 25. Asignación permisos de ejecución

```
[velociraptor_unad@localhost ~]$ chmod +x velociraptor-v0.5.3-linux-amd64
```

Fuente: El autor

Se inició el proceso para generar los archivos de configuración para servidor y cliente. En este caso se eligió Sistema Operativo “Linux”:

./velociraptor-v0.5.3-linux-amd64 config generate -i

Figura 26.Inicio de generación de archivos de configuración

```
[velociraptor_unad@localhost ~]$ ./velociraptor-v0.5.3-linux-amd64 config generate -i
?
Welcome to the Velociraptor configuration generator
--------------------------------------------------

I will be creating a new deployment configuration for you. I will
begin by identifying what type of deployment you need.


What OS will the server be deployed on?
  [Use arrows to move, type to filter]
> linux
  windows
  darwin
```

Fuente: El autor

El almacenamiento de la información se puede realizar en un archivo o en una base de datos. Para este caso el almacenamiento se realizó en archivo por lo cual se eligió “FileBaseDataStore”

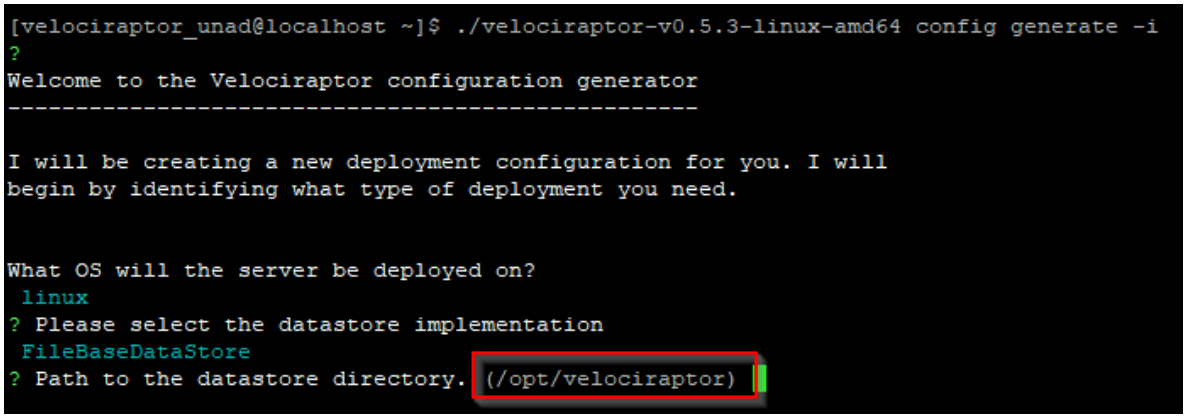
Figura 27. Elección almacenamiento datastore

```
[velociraptor_unad@localhost ~]$ ./velociraptor-v0.5.3-linux-amd64 config generate -i
?
Welcome to the Velociraptor configuration generator
--------------------------------------------------

I will be creating a new deployment configuration for you. I will
begin by identifying what type of deployment you need.


What OS will the server be deployed on?
 linux
? Please select the datastore implementation
  [Use arrows to move, type to filter]
> FileBaseDataStore
  MySQL
```

Fuente: El autor

En seguida se seleccionó la ruta en la cual se almacena el datastore. Se eligió la ruta por defecto: /opt/velociraptor

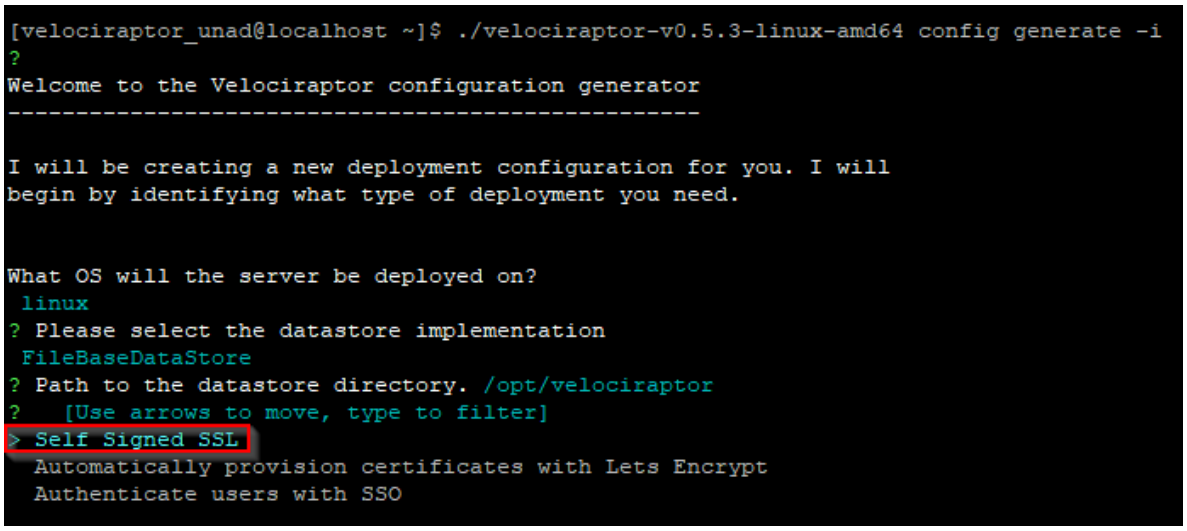
Figura 28. Ruta para el datastore



Fuente: el autor

Luego, se eligió la opción para configuración de certificado SSL cuya función es permitir una comunicación segura entre el usuario y la plataforma. Se seleccionó certificados autofirmados.

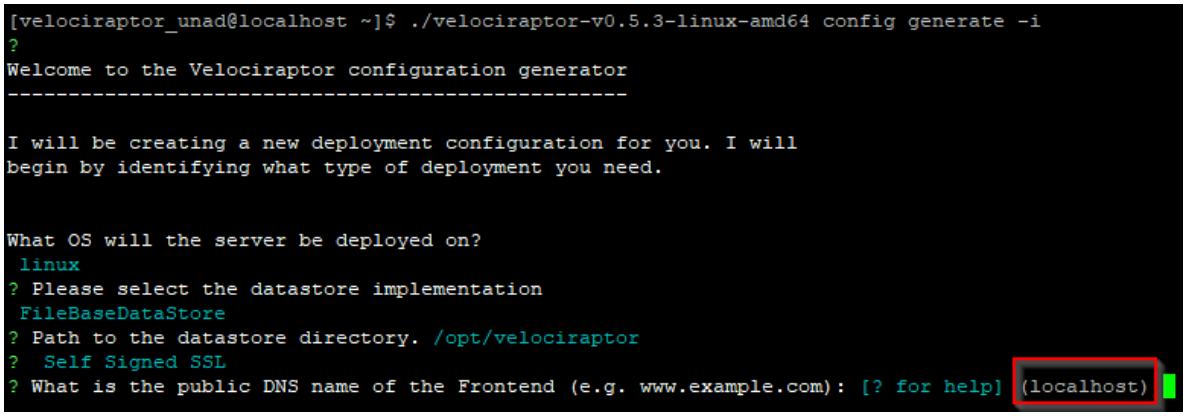
Figura 29. Elección de configuración de certificado SSL



Fuente: El autor

Dado que no se cuenta con un DNS asignado al servidor, se eligió el default: “localhost”

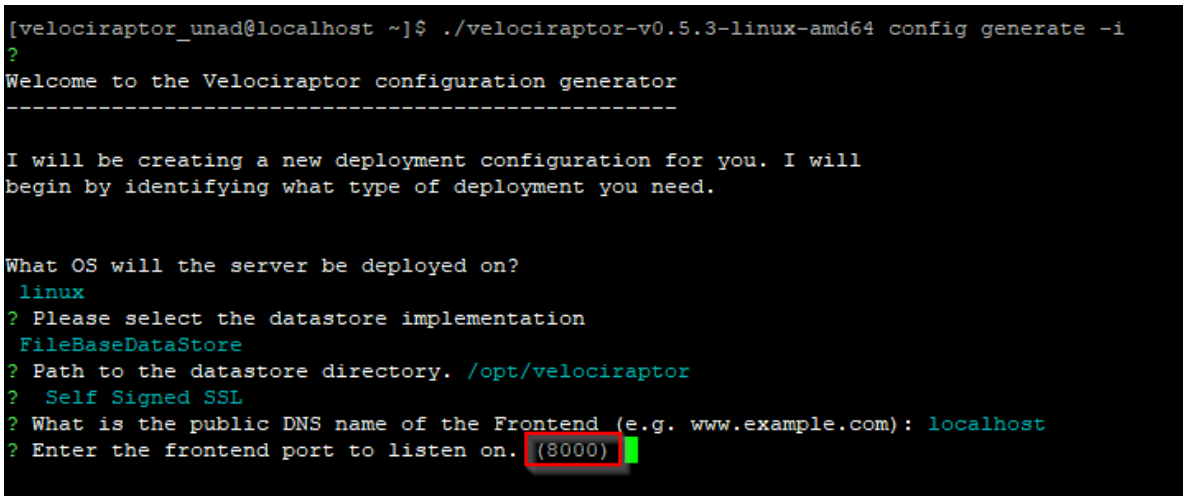
Figura 30. Configuración de DNS



Fuente: El autor

Se configuró el puerto para el frontend a través del cual el servidor de Velociraptor recibe la comunicación de los clientes. Se configuró el puerto por defecto: “8000”

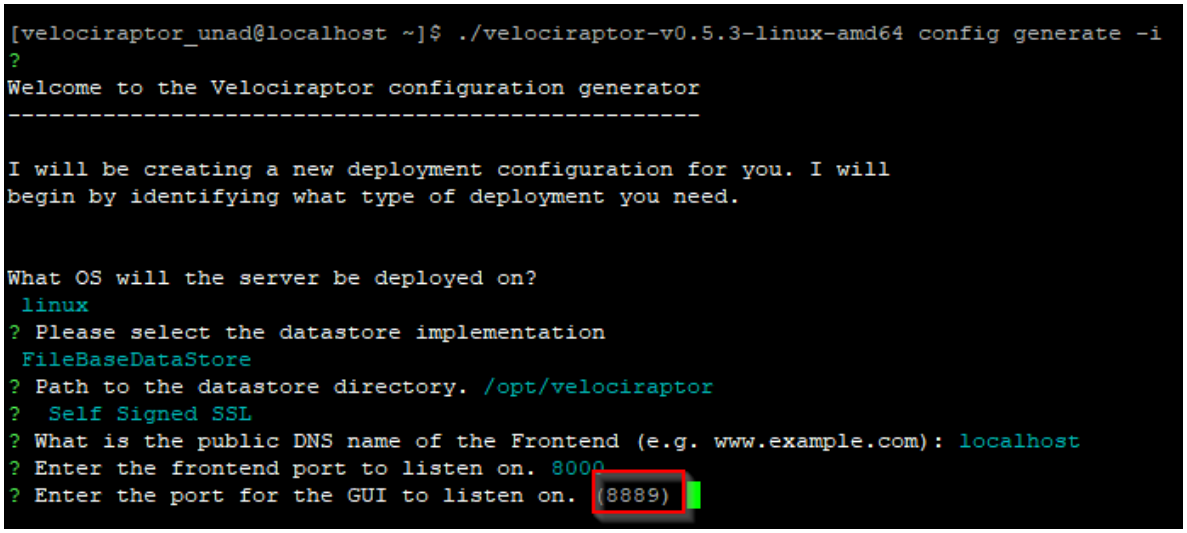
Figura 31. Configuración de puerto para el FrontEnd



Fuente: El autor

Se configuró el puerto de acceso a la interfaz gráfica de usuario, a través de la cual un usuario realizará gestión de la plataforma. Se configuró el puerto por defecto: “8889”

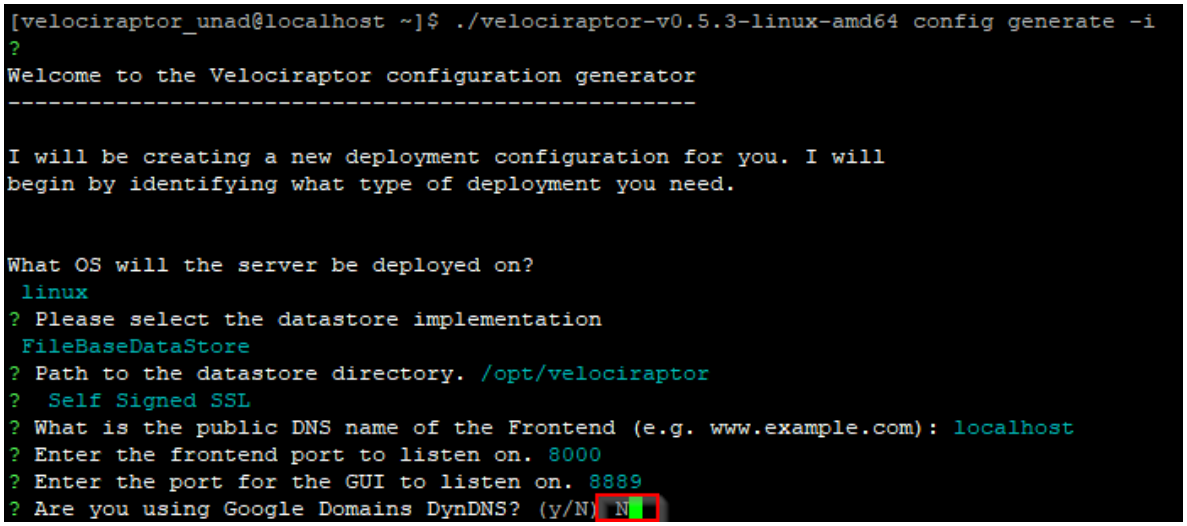
Figura 32. Configuración de puerto para GUI



Fuente: El autor

Dado que no se está usando el servicio de DNS dinámico de Google se seleccionó “No”

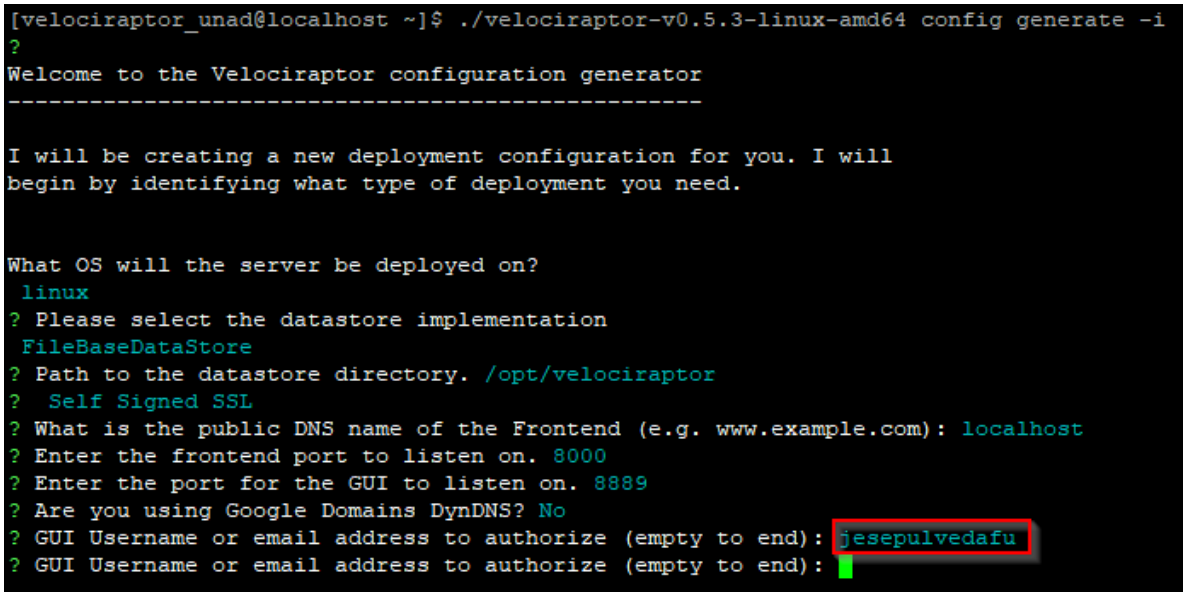
Figura 33. Configuración DNS dinámico de Google



Fuente: El autor

Luego, se creó el usuario administrador de la plataforma “jesepulvedafu”

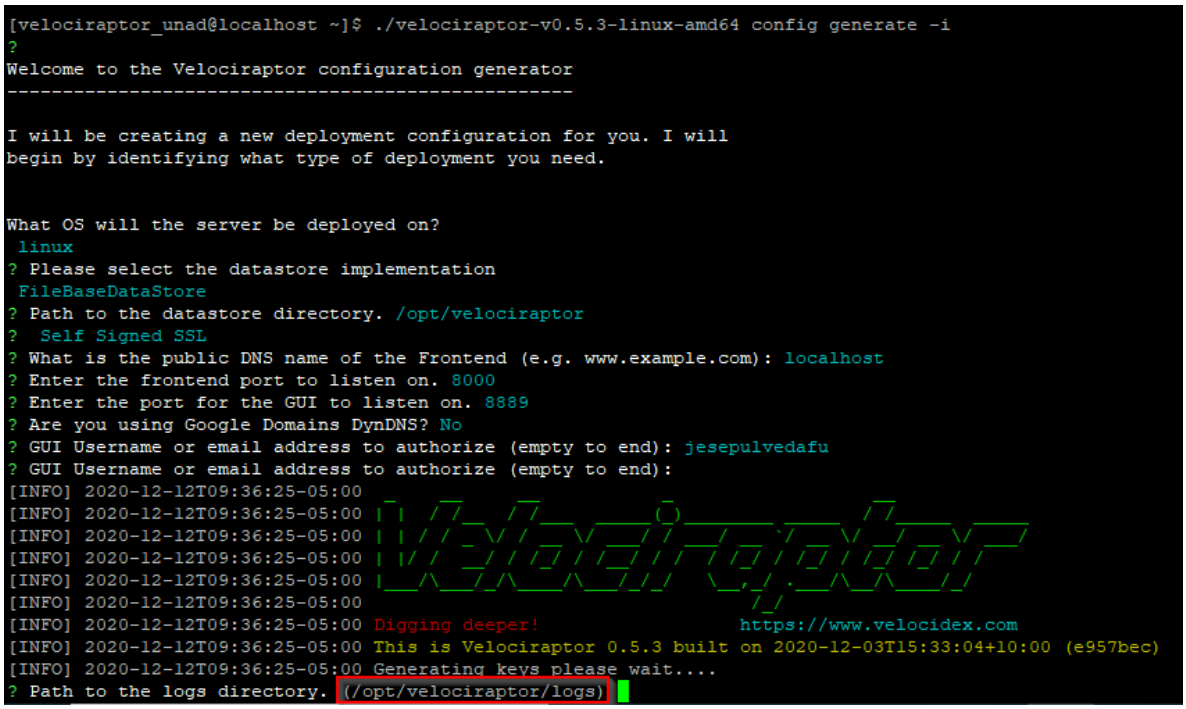
Figura 34. Creación de usuario



Fuente: El autor

Luego, se eligió la ruta por defecto para guardar los logs de la plataforma /opt/velociraptor/logs

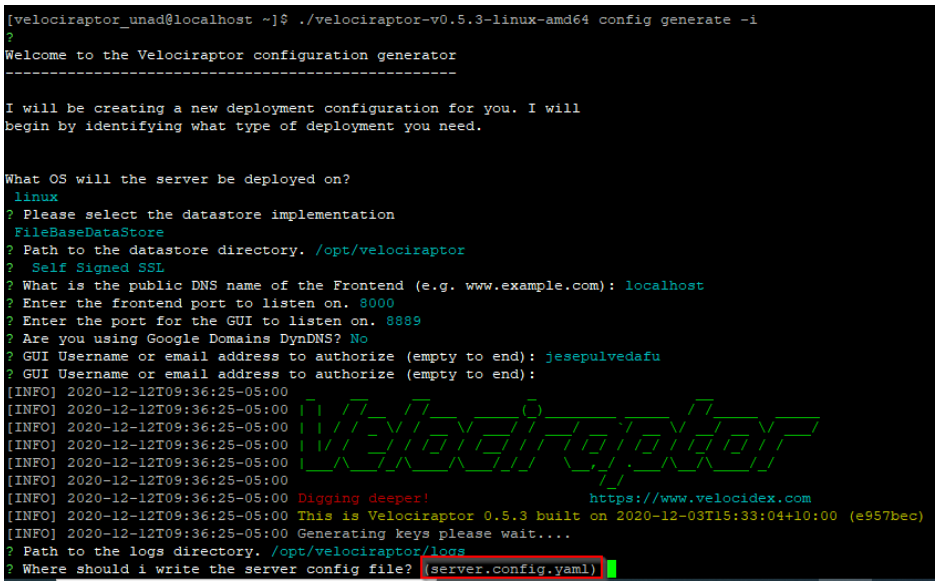
Figura 35. Configuración de ruta para almacenamiento de logs



Fuente: El autor

Se elige el directorio en el cual se guardará el archivo de configuración del servidor, tal como en este caso, si no se especifica una ruta, entonces el archivo se guarda en la ruta actual

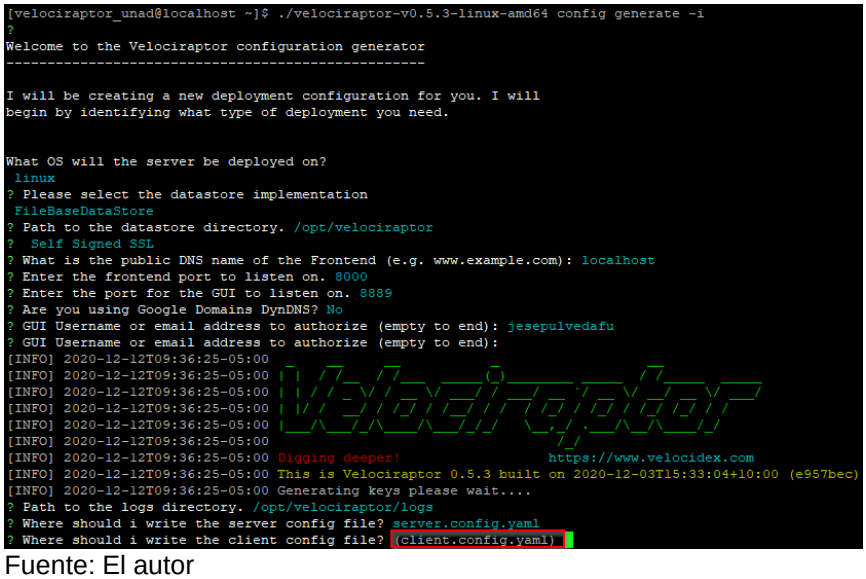
Figura 36. Ruta de escritura de archivo de configuración del servidor



Fuente: El autor

Se elige el directorio en el cual se guardará el archivo de configuración del cliente, tal como en este caso, si no se especifica una ruta, entonces el archivo se guarda en la ruta actual

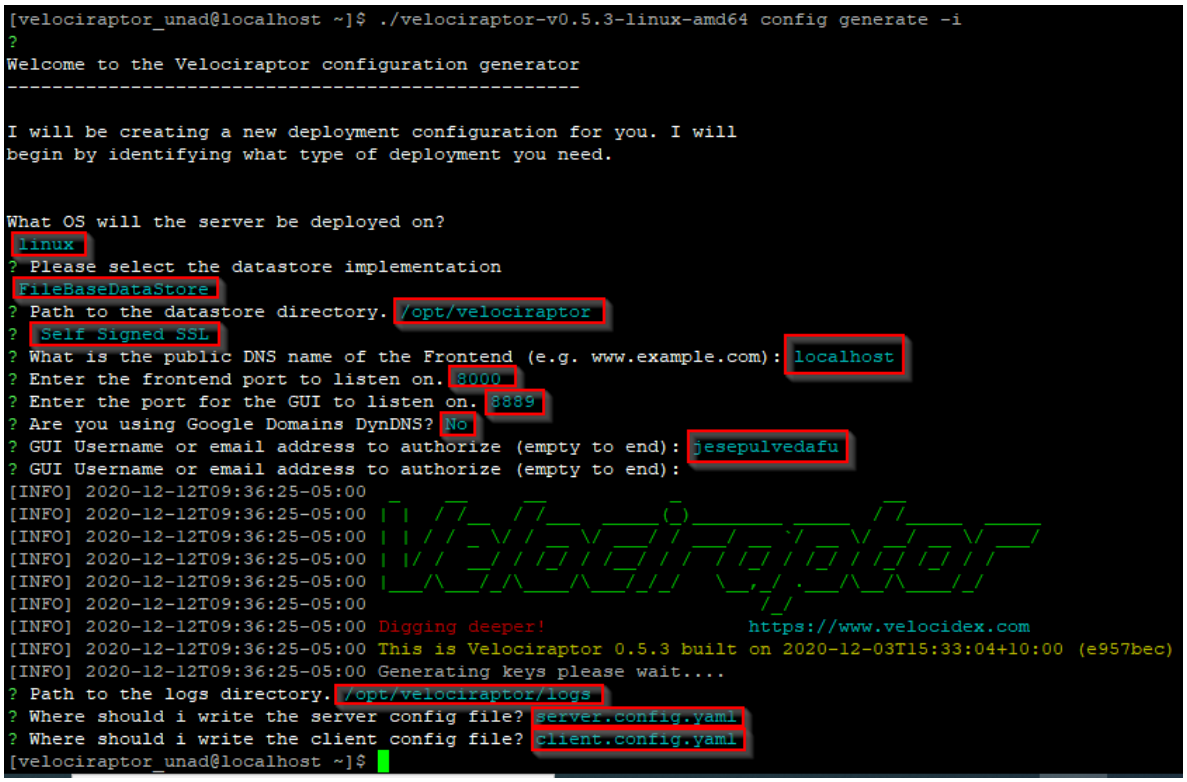
Figura 37. Ruta de escritura de archivo de configuración de cliente



Fuente: El autor

En la siguiente figura se resalta a modo de resumen la configuración que se realizó para la generación de los archivos de configuración

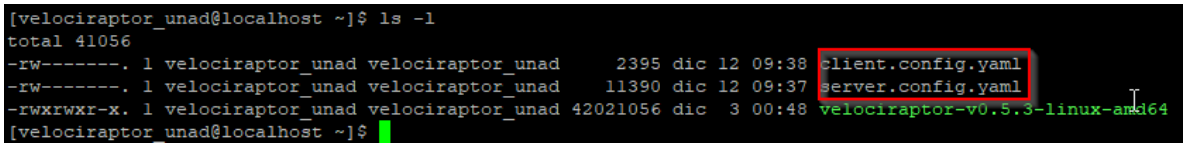
Figura 38. Resumen configuración inicial Velociraptor



Fuente: El autor

Se visualizan los archivos de configuración generados:
server.config.yaml
client.config.yaml

Figura 39. Archivos de configuración generados



Fuente: El autor

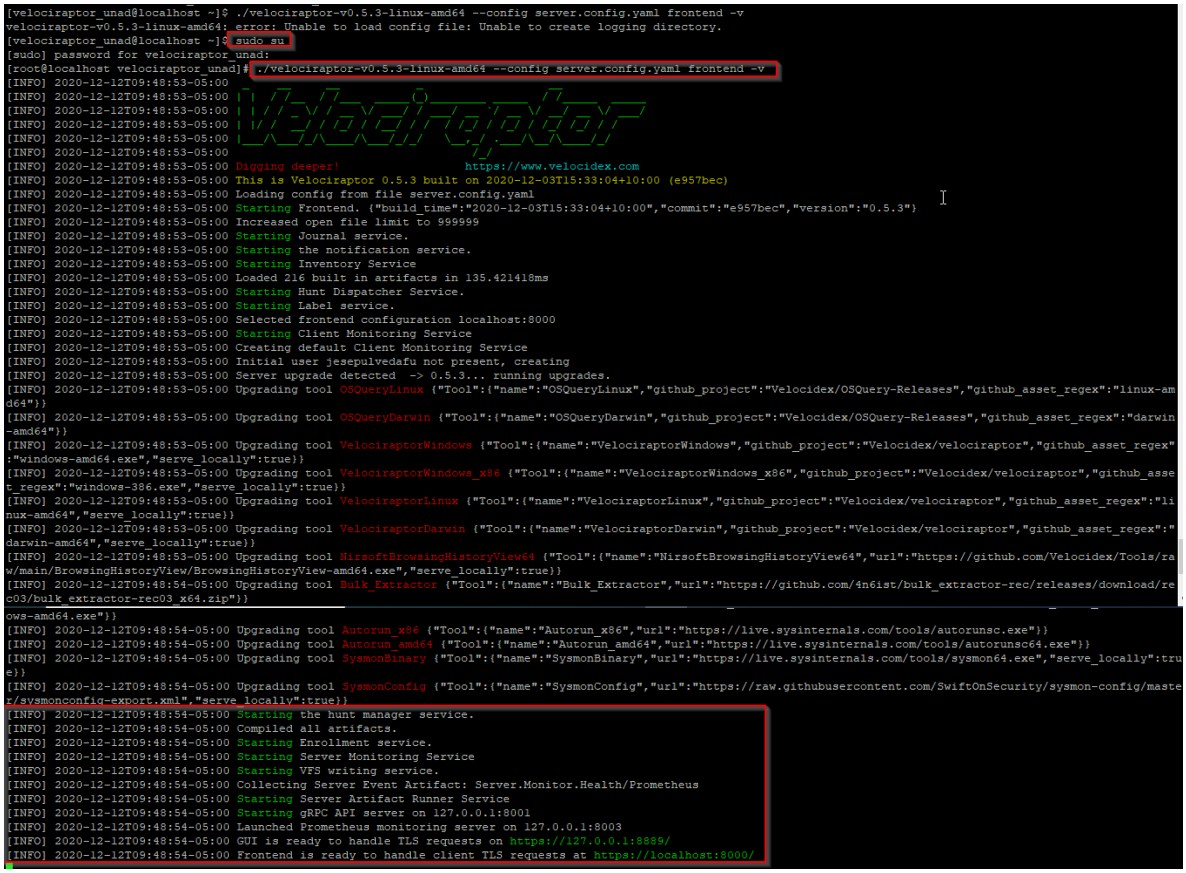
Es importante resaltar la posibilidad de la plataforma de crear usuarios con diferentes roles como analista, investigador, administrador y desarrollador de artefactos.

Se inició la ejecución como superusuario de Velociraptor en el servidor con el archivo de configuración con la siguiente instrucción

./velociraptor-v0.5.3-linux-amd64 --config server.config.yaml frontend -v

Se visualizan los servicios iniciados y en escucha

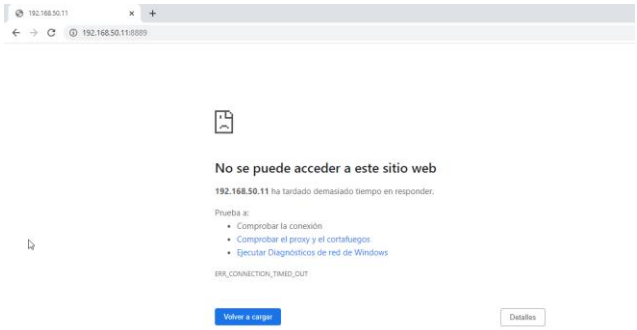
Figura 40. Servicios en ejecución



Fuente: El autor

Dado que el Sistema Operativo se instaló sin Interfaz de usuario, se intentó el acceso desde otro equipo dentro de la red, sin embargo, no se logró la conexión

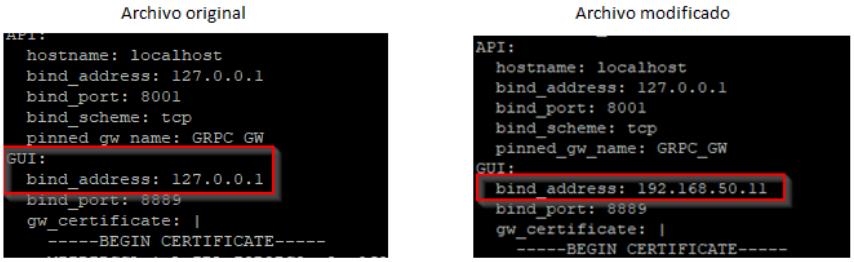
Figura 41. Error en la conexión



Fuente: El autor

Para lograr este acceso fue necesario detener la ejecución y modificar el archivo "server.config.yaml"

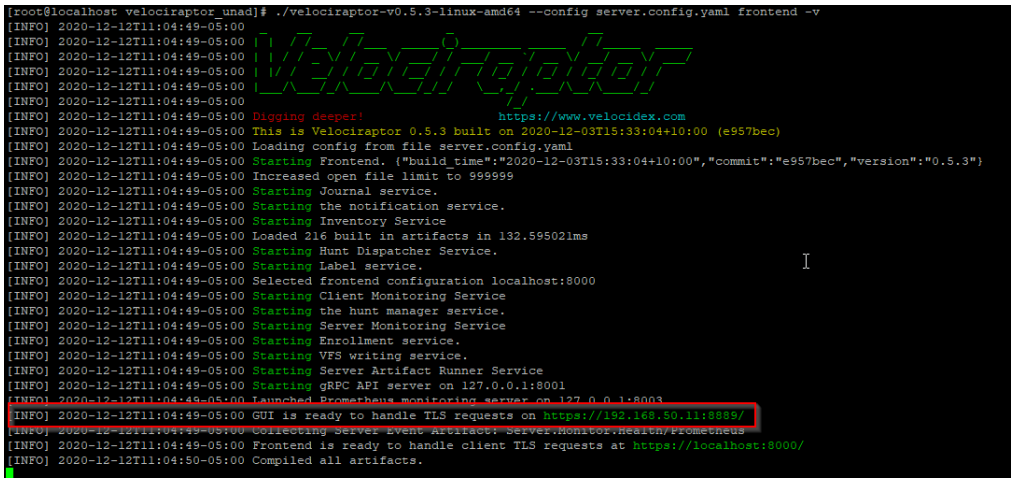
Figura 42. Modificación de archivo de configuración de servidor



Fuente: El autor

Se realizó de nuevo la ejecución y se evidenció el servicio GUI correctamente expuesto a través de la dirección IP

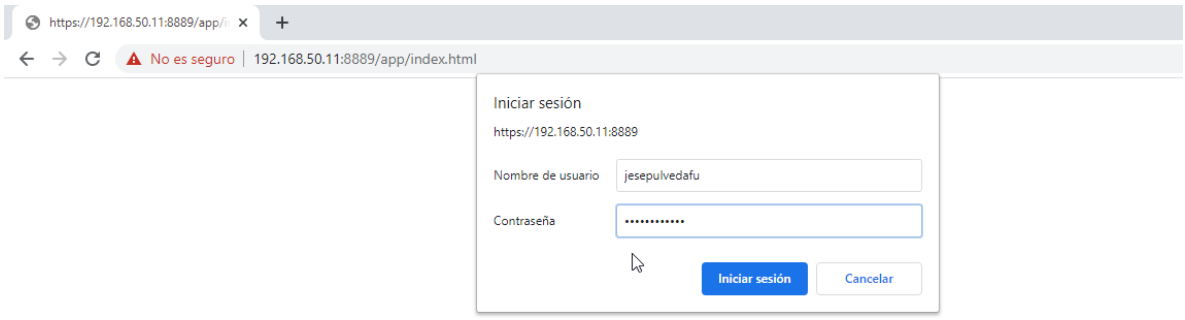
Figura 43. Servidor velociraptor en ejecución



Fuente: El autor

Se confirmó acceso a través de la GUI y el ingreso con el usuario creado previamente “jesepulvedafu”

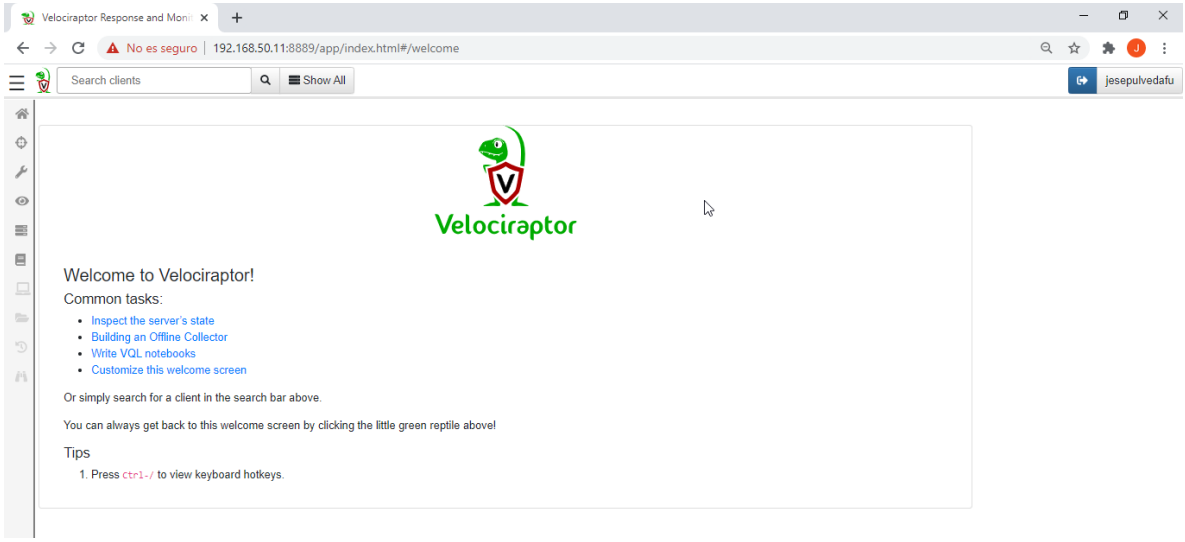
Figura 44.Acceso a GUI



Fuente: El autor

Se observó la pantalla de bienvenida a la plataforma. En este punto el servidor Velociraptor se encuentra en ejecución y en escucha para recibir las conexiones de clientes

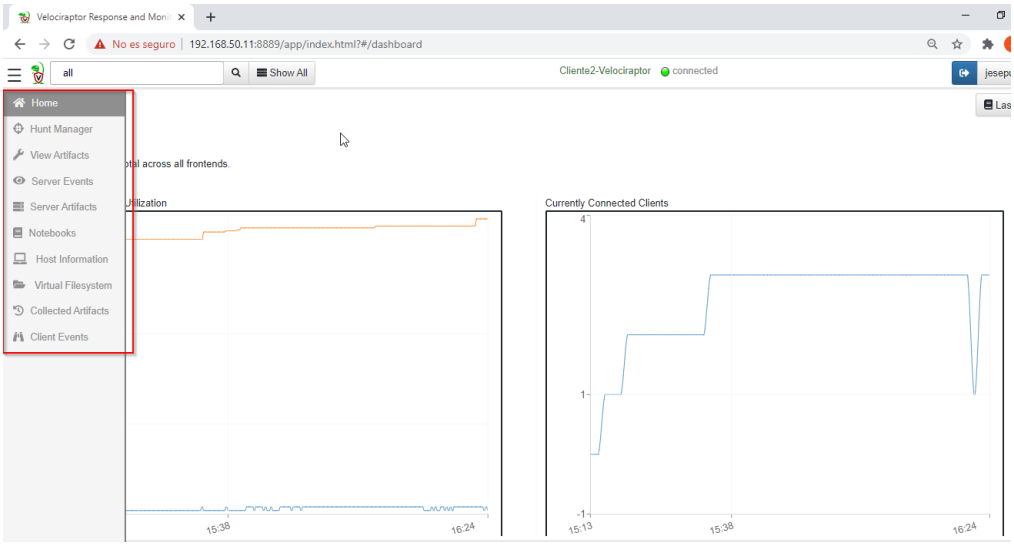
Figura 45. Página de bienvenida Velociraptor



Fuente: El autor

En siguiente figura se observa el menú principal de Velociraptor y el dashboard con información de importancia como uso de recursos del servidor y cantidad de clientes conectados

Figura 46. Dashboard y menú principal Velociraptor



Fuente: El autor

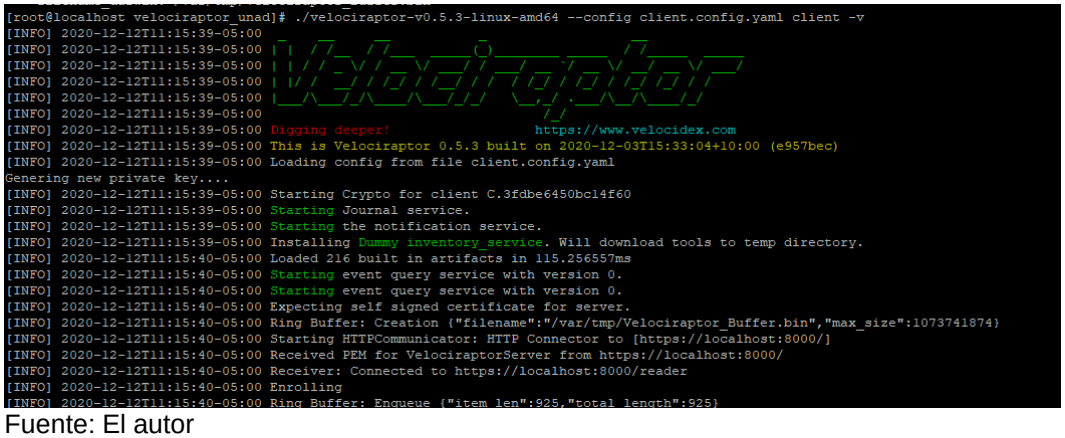
6.4. IMPLEMENTACIÓN DE CLIENTES

Para el despliegue de velociraptor en los clientes es posible utilizar el mismo software descargado desde el repositorio en GitHub dependiendo del sistema operativo del cliente y su arquitectura. Lo importante es que en el momento de la ejecución del archivo descargado se incluya como parámetro el archivo de configuración de cliente generado previamente desde el servidor, es decir el archivo "client.config.yaml"

6.4.1. Cliente0. Centos 8.2. Se inició la ejecución de Velociraptor cliente con el archivo de configuración generado previamente con la siguiente instrucción

./velociraptor-v0.5.3-linux-amd64 --config client.config.yaml client -v

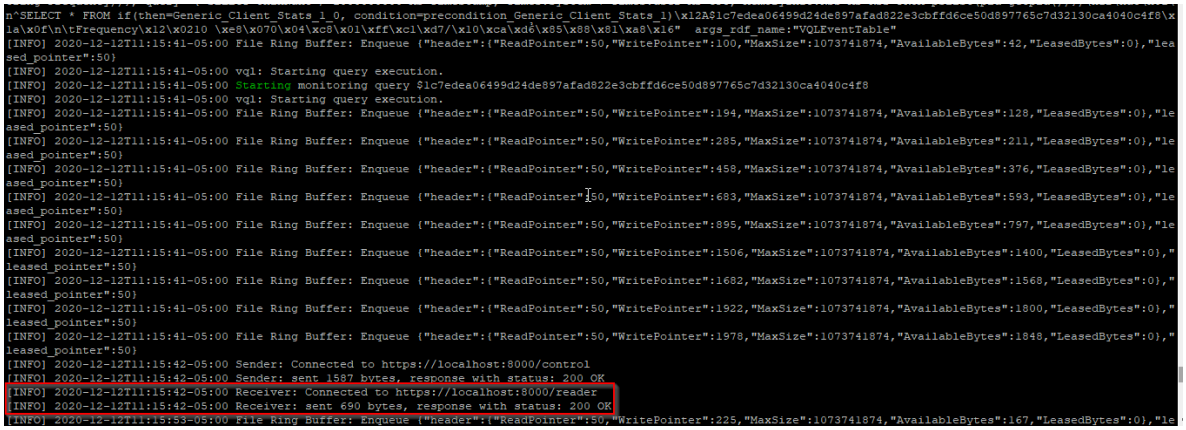
Figura 47. Implementación velociraptor en Cliente0



Fuente: El autor

Se visualiza la conexión del cliente con el servidor a través del puerto 8000

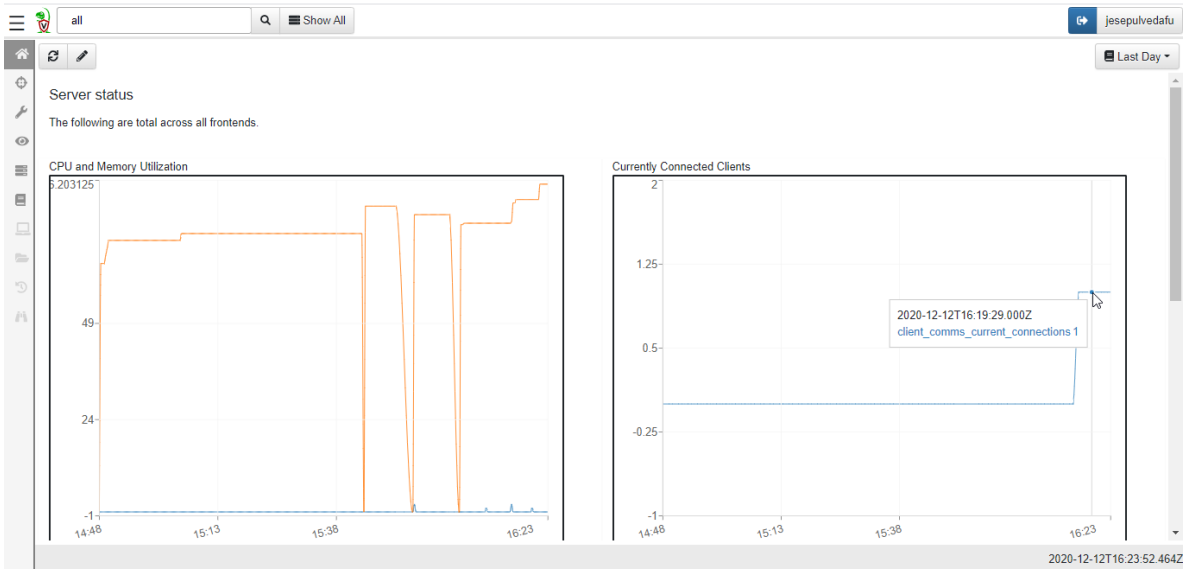
Figura 48. Conexión de Cliente0 con servidor velociraptor



Fuente: El autor

En la interfaz de administración del servidor se observó el evento de conexión del *Cliente0*

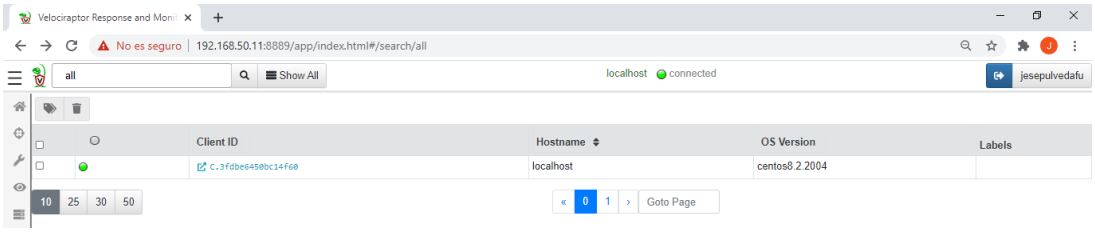
Figura 49. Evento de conexión de Cliente0 al servidor velociraptor



Fuente: El autor

Se visualizan los clientes (endpoints) gestionados. En este punto sólo se había realizado el despliegue de velociraptor en un cliente

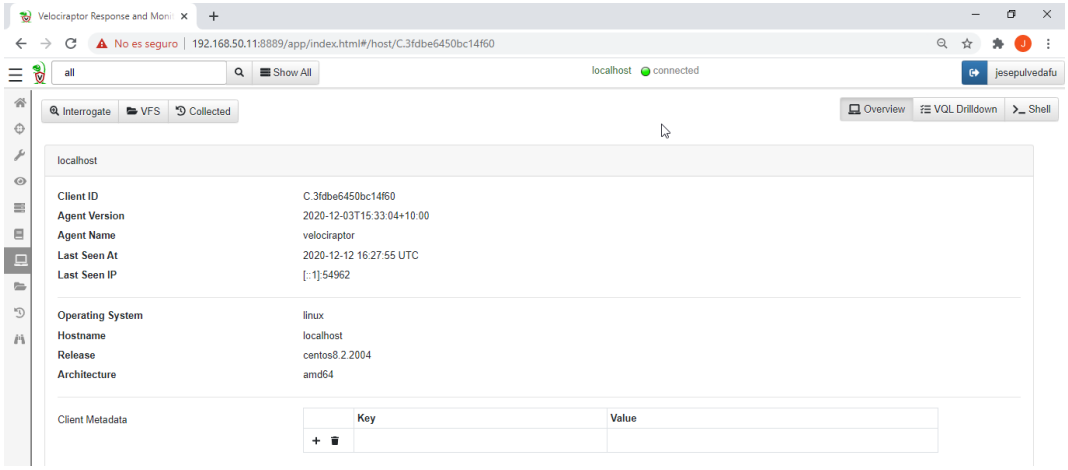
Figura 50. Vista general de endpoints administrador por velociraptor (1)



Fuente: El autor

Al dar clic en el campo de “Client ID” se visualiza información básica del cliente conectado como hostname, arquitectura, sistema operativo y distribución, última hora en la que fue visto por el servidor, entre otra.

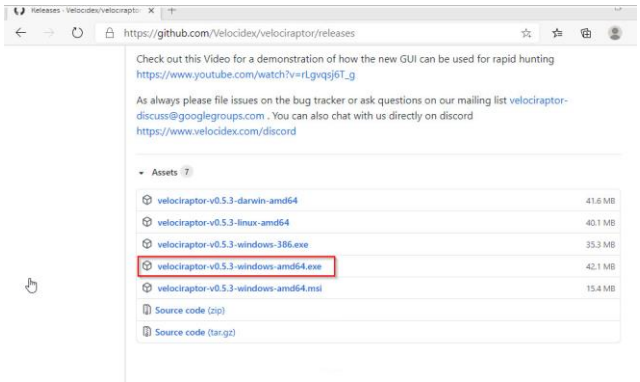
Figura 51. Información básica de *Cliente0* vista desde Velociraptor



Fuente: El autor

6.4.2. Cliente1. Windows 10. Se realizó la descarga del software desde el repositorio de velociraptor en GitHub

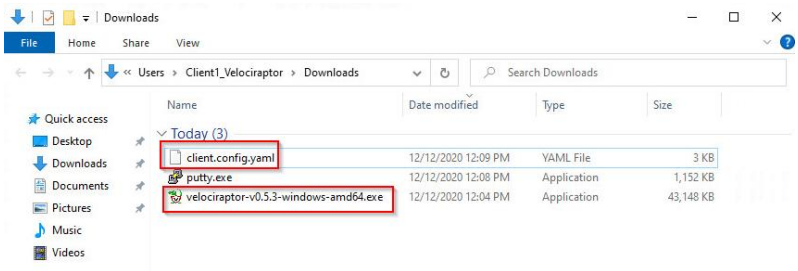
Figura 52. Descarga de velociraptor para *Cliente1*



Fuente: El autor

Se observa el software descargado y el archivo de configuración cliente “client.config.yaml” el cual fue generado desde el servidor previamente

Figura 53. Software y archivo para despliegue de velociraptor en *Cliente1*



Fuente: El autor

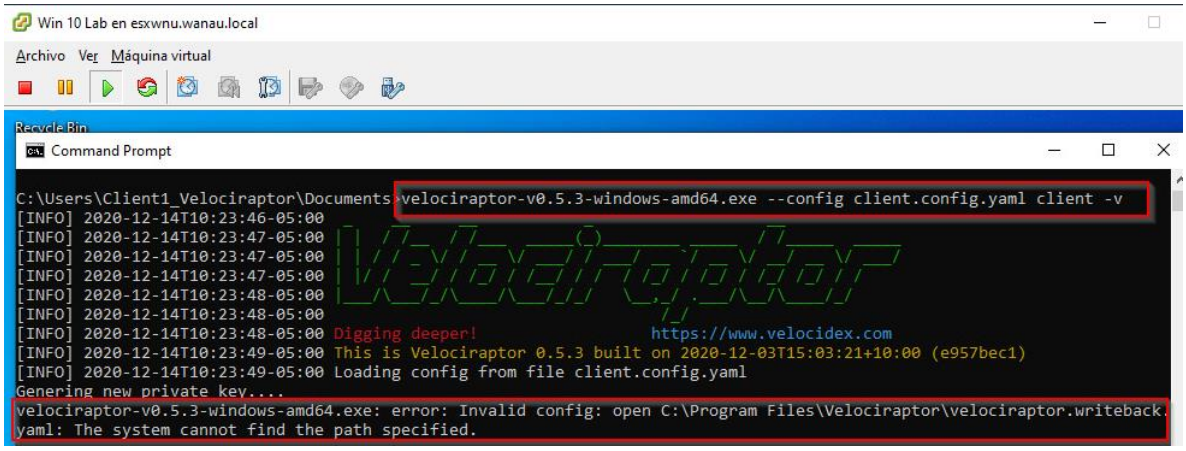
A diferencia del *Cliente0* el cual corresponde al mismo servidor de velociraptor, con los demás clientes es necesario modificar el archivo de configuración “client.config.yaml” con el fin de que la conexión la realice hacia el DNS o dirección IP del servidor velociraptor. Se observa en la siguiente figura la modificación realizada sobre el archivo de configuración de cliente velociraptor

Figura 54. Modificación de URL de servidor velociraptor en archivo de configuración cliente

Fuente: El autor

Se inició la ejecución (desde CMD como administrador) del software con el archivo de configuración cliente, sin embargo, se obtuvo el error mostrado a continuación

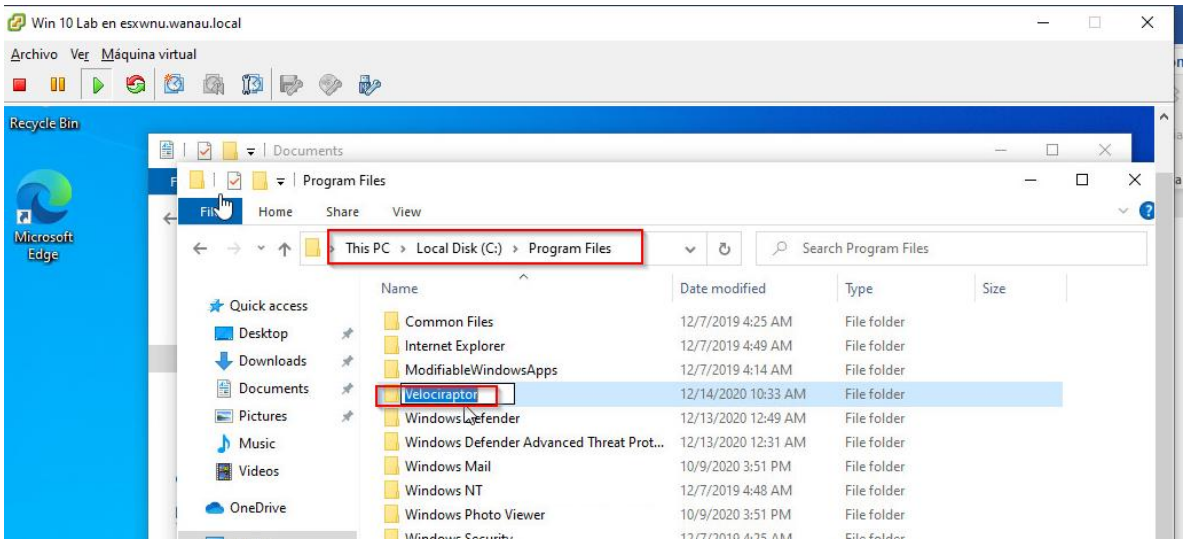
Figura 55. Error en despliegue de velociraptor en Cliente1



Fuente: El autor

Revisando documentación y foros se detectó que el error se debe a la inexistencia del directorio “Velociraptor” en la ruta indicada. Se procede con la creación de dicho directorio

Figura 56. Solución de error encontrado en despliegue de velociraptor en Cliente1

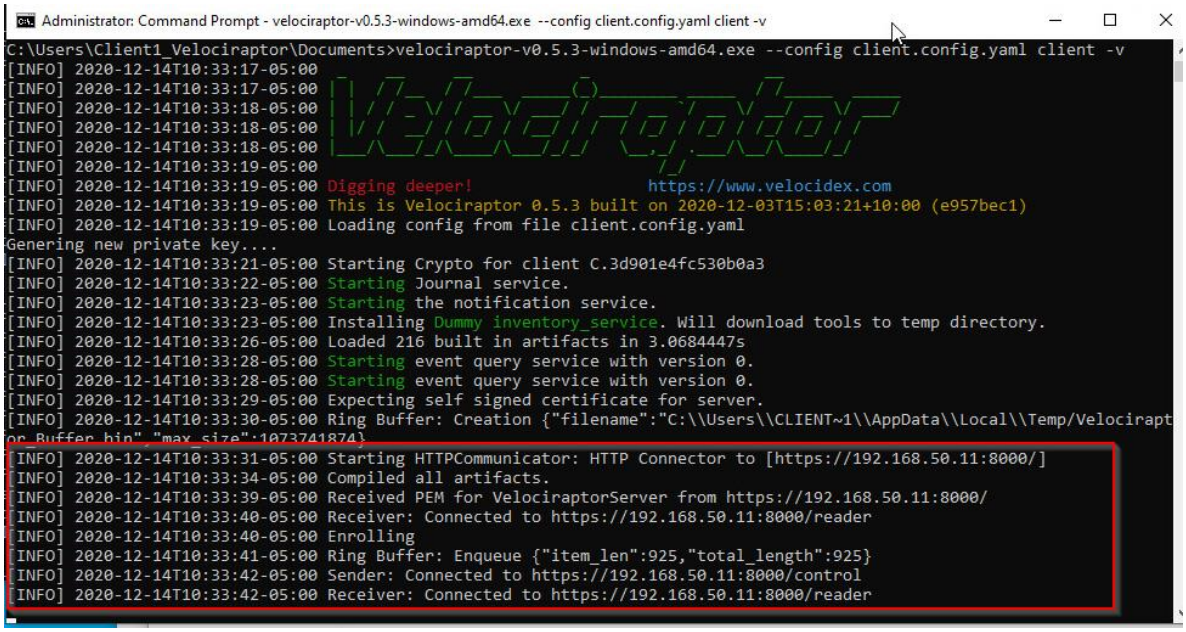


Fuente: El autor

Se ejecutó nuevamente la instrucción para ejecución del software con el archivo de configuración de cliente como parámetro y se evidenció la conexión exitosa al servidor velociraptor a través del puerto 8000

velociraptor-v0.5.3-windows-amd64.exe --config client.config.yaml client -v

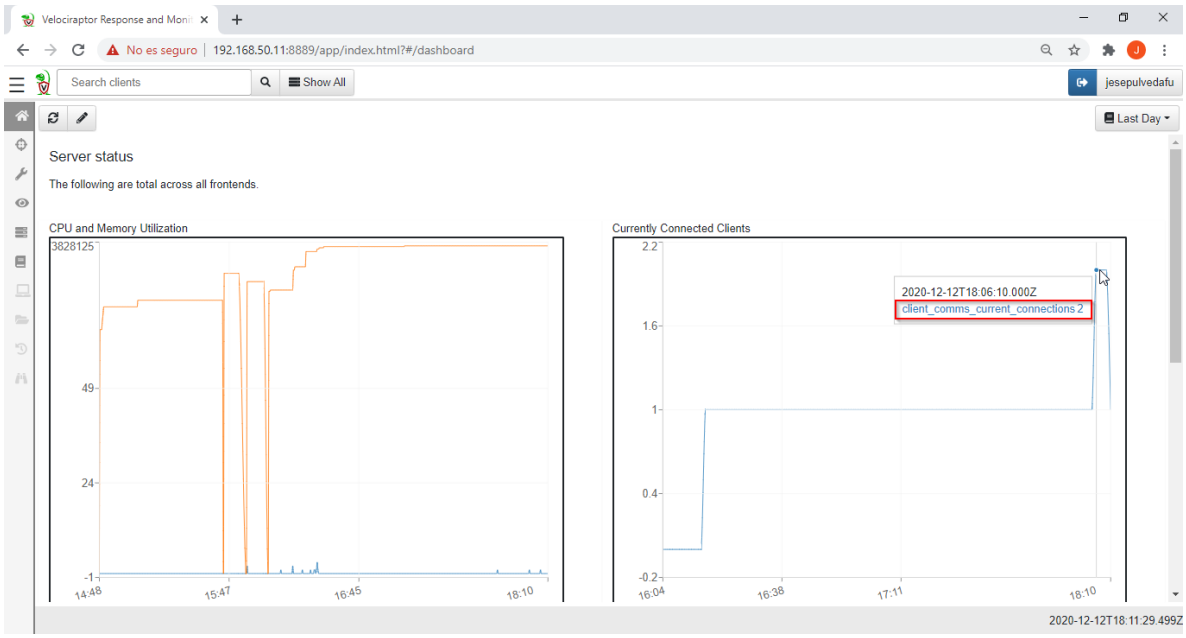
Figura 57. Conexión de *Cliente1* con servidor Velociraptor



Fuente: El autor

Se observó el evento de conexión de un nuevo cliente en la interfaz de administración del servidor de velociraptor

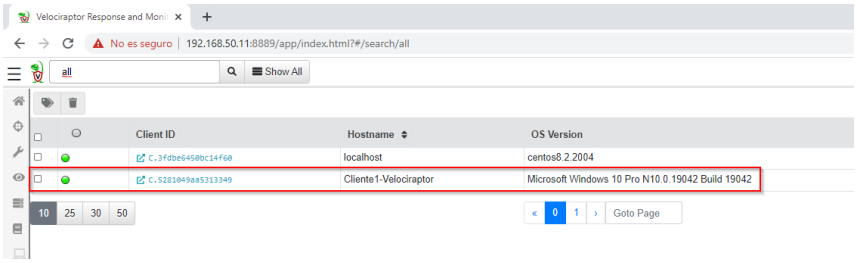
Figura 58. Evento de conexión de *Cliente1* en servidor velociraptor



Fuente: El autor

Se observan los clientes (endpoints) ya gestionados. En este punto se había realizado el despliegue de velociraptor en dos clientes.

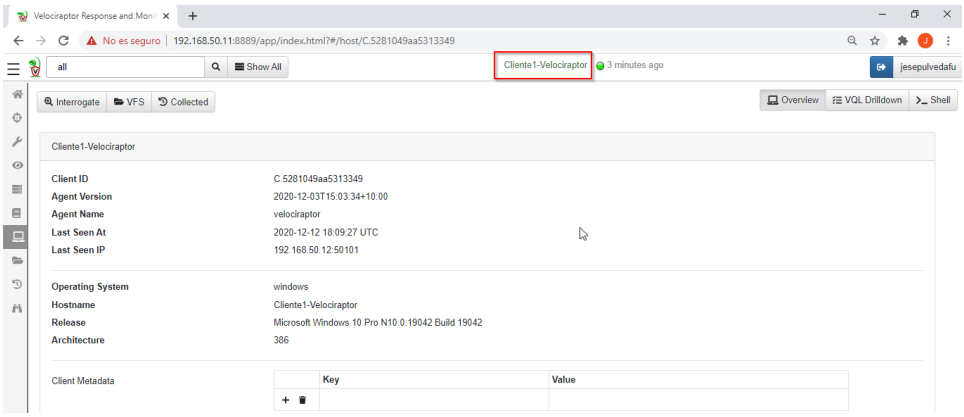
Figura 59. Vista general de clientes(endpoints) administrados por Velociraptor (2)



Fuente: El autor

Se visualiza información básica del cliente agregado *Cliente1*

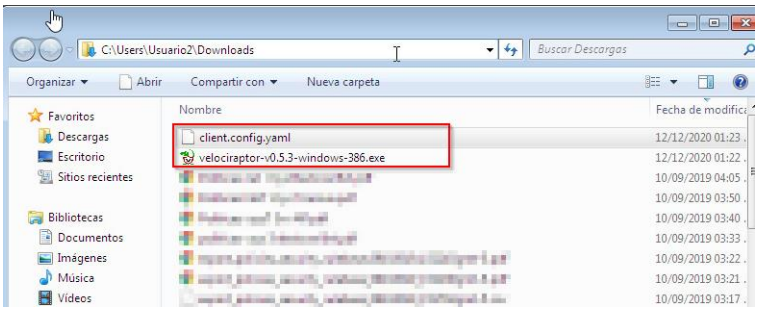
Figura 60. Información básica de *Cliente1* obtenida desde velociraptor



Fuente: El autor

6.4.3. Cliente2. Windows7. Se visualiza el software velociraptor descargado y el archivo de configuración de cliente generado previamente desde el servidor velociraptor

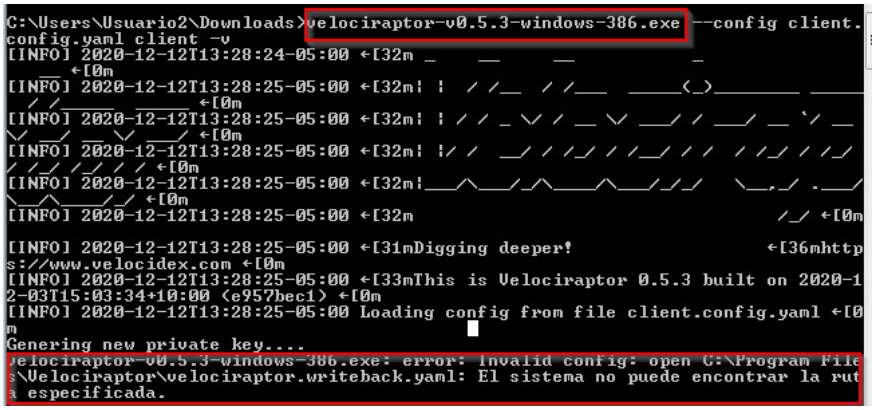
Figura 61. Software y archivo de configuración para despliegue de velociraptor en *Cliente2*



Fuente: El autor

Se inició la ejecución del software con el archivo de configuración cliente como parámetro, sin embargo, se obtuvo el mismo error presentado en el despliegue de velociraptor en *Cliente1*

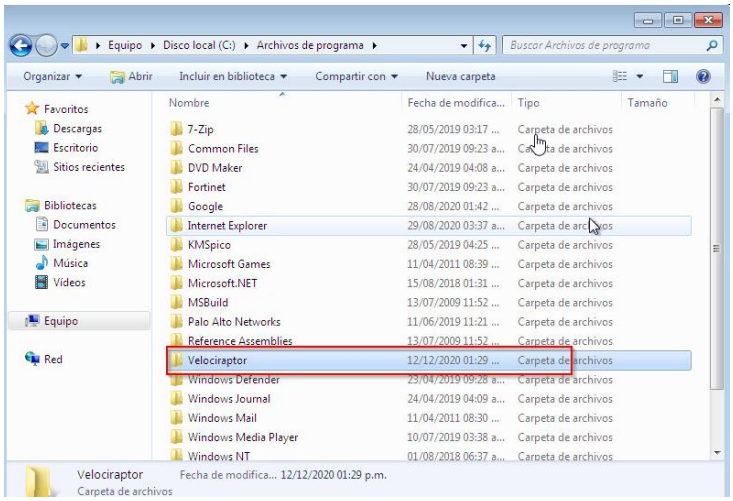
Figura 62. Error en despliegue de velociraptor en *Cliente2*



Fuente: El autor

Se procedió con la creación del directorio “Velociraptor” en la ruta indicada en el error

Figura 63. Solución de error obtenido en despliegue de velociraptor en *Cliente2*

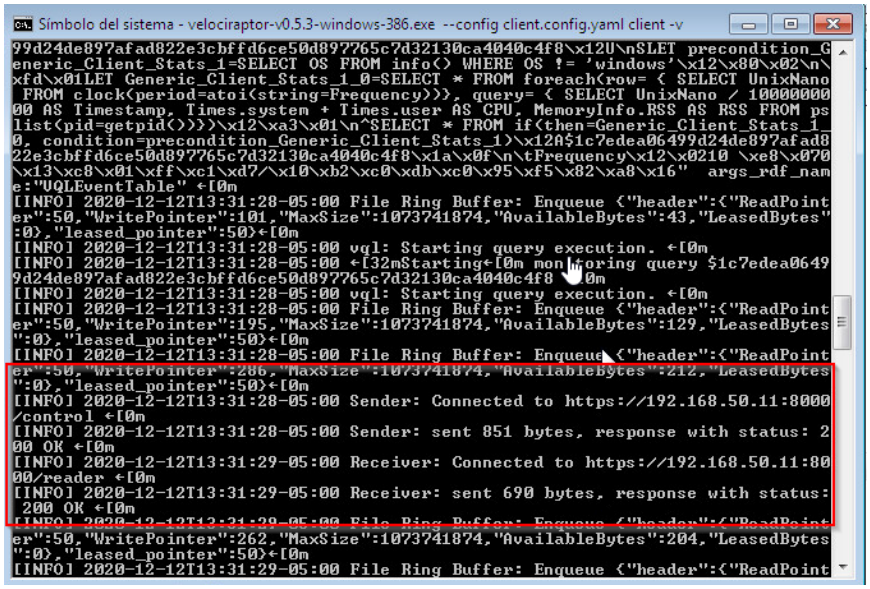


Fuente: El autor

Se realizó nuevamente la ejecución del software con el archivo de configuración cliente como parámetro y se observó la conexión correcta con el servidor velociraptor a través del puerto 8000

velociraptor-v0.5.3-windows-386.exe --config client.config.yaml client -v

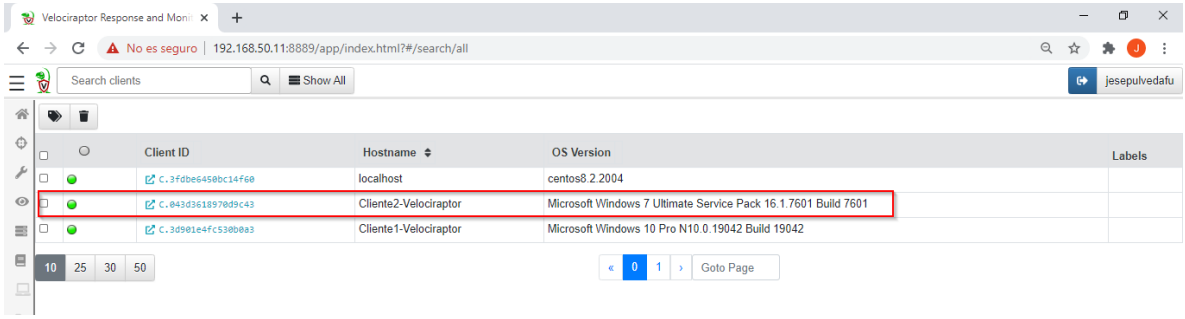
Figura 64. Conexión entre *Cliente2* y servidor velociraptor



Fuente: El autor

Desde la interfaz de administración de velociraptor se visualizan los clientes(endpoints) administrados

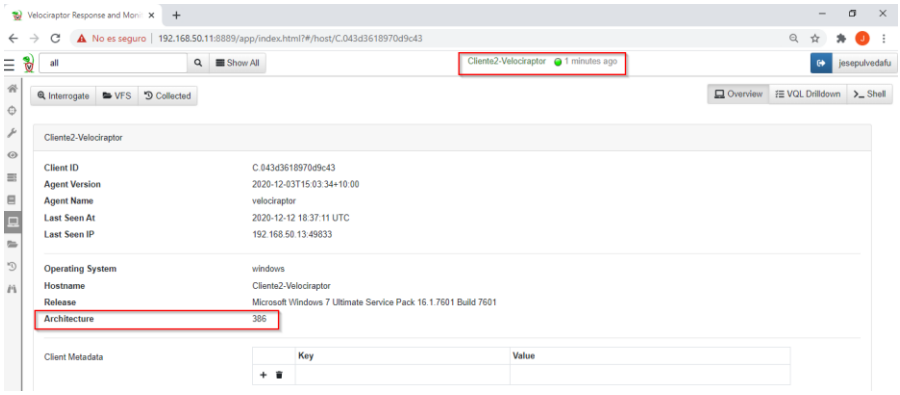
Figura 65. Vista general de clientes administrados por velociraptor (3)



Fuente: El autor

Se observa información básica de *Cliente2* obtenida desde Velociraptor

Figura 66. Información básica de Cliente2



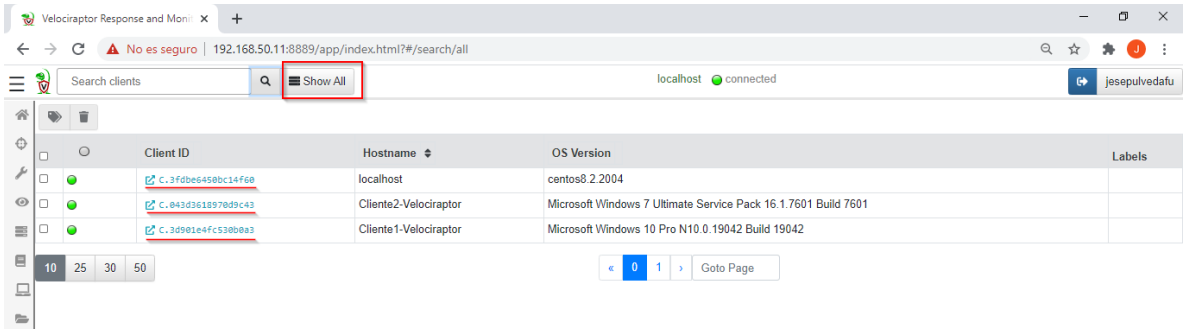
Fuente: El autor

En este punto, ya los endpoints pueden ser protegidos y gestionables a través del servidor de Velociraptor

6.5. INVESTIGACIÓN Y RECOPILACIÓN DE INFORMACIÓN DE ENDPOINTS

Desde el cuadro de búsqueda en la pantalla principal es posible filtrar por algún cliente específico o se da clic en “Show All” para ver todos los clientes

Figura 67. Vista de todos los clientes



Fuente: El autor

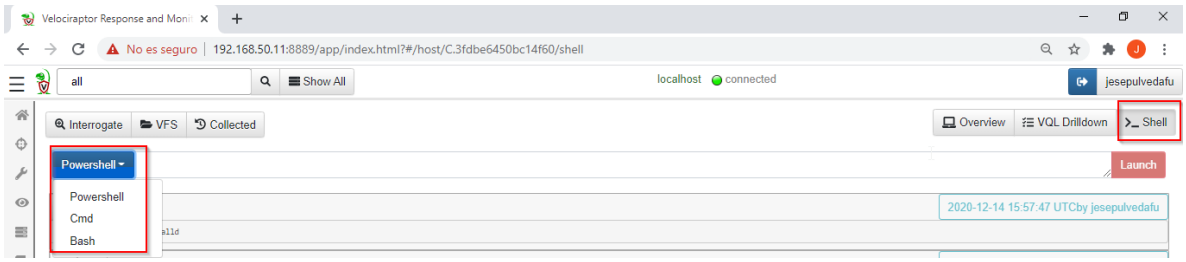
Para ver información en detalle de un cliente y ejecutar acciones específicas sobre el mismo se da clic sobre el campo de “Client ID”.

6.5.1. Gestión remota a través de línea de comandos (bash/powershell/CMD)

Se ejecutaron remotamente algunas instrucciones a través de Shell desde velociraptor para extracción de información de los endpoints

Tener en cuenta que se debe seleccionar la opción remota de Shell (Powershell, Cmd o Bash), dependiendo del sistema operativo del cliente y/o la información que se desea obtener

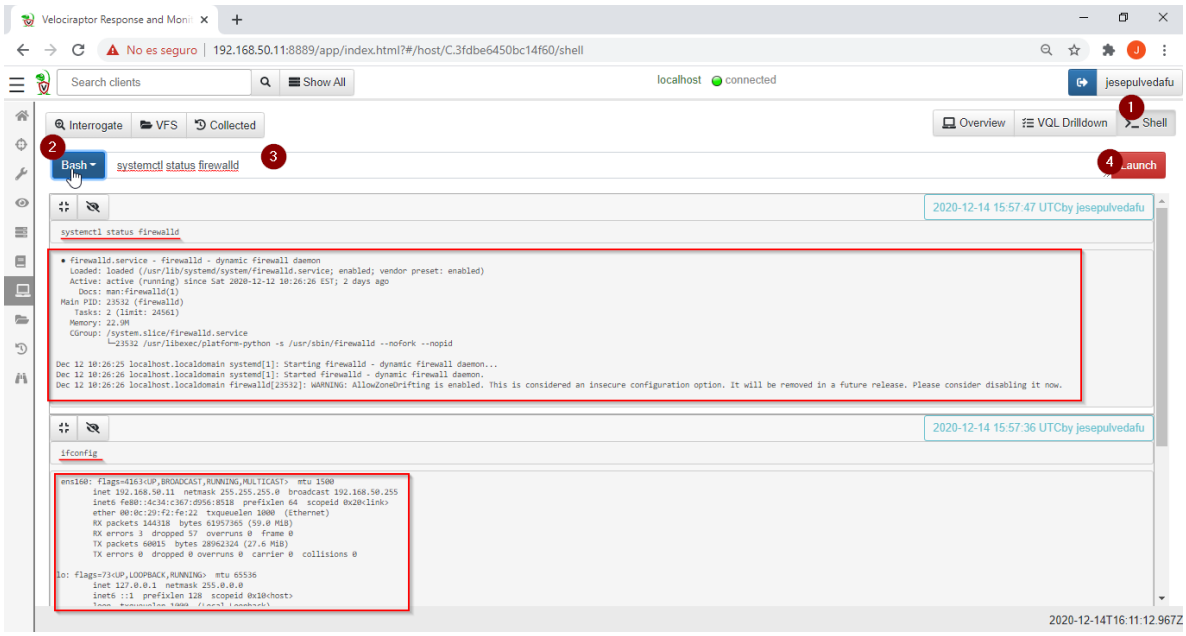
Figura 68. Opciones para ejecución de instrucciones Shell



Fuente: El autor

Con el procedimiento mostrado en la siguiente figura se logró la extracción de estado actual del firewall local en *Cliente0* (localhost) e información de configuración de interfaz de red

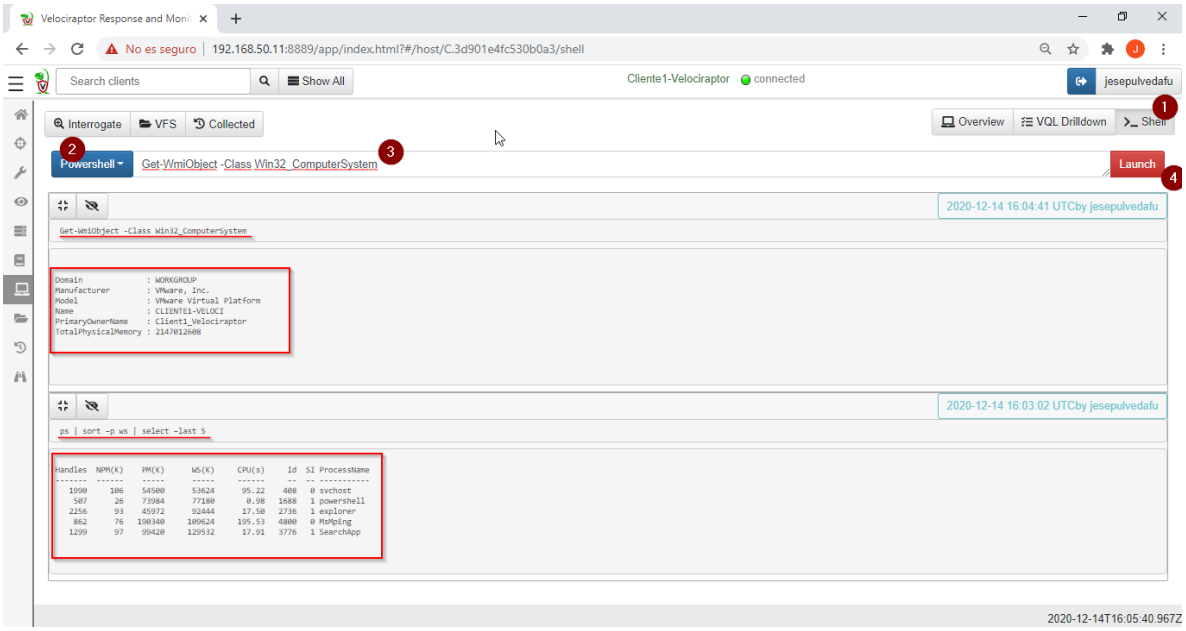
Figura 69. Instrucciones en bash para Cliente0



Fuente: El autor

Con el procedimiento mostrado en la siguiente figura sobre el *Cliente1* se listaron los 5 procesos con mayor consumo de memoria y se obtuvo información de fábrica y modelo del computador

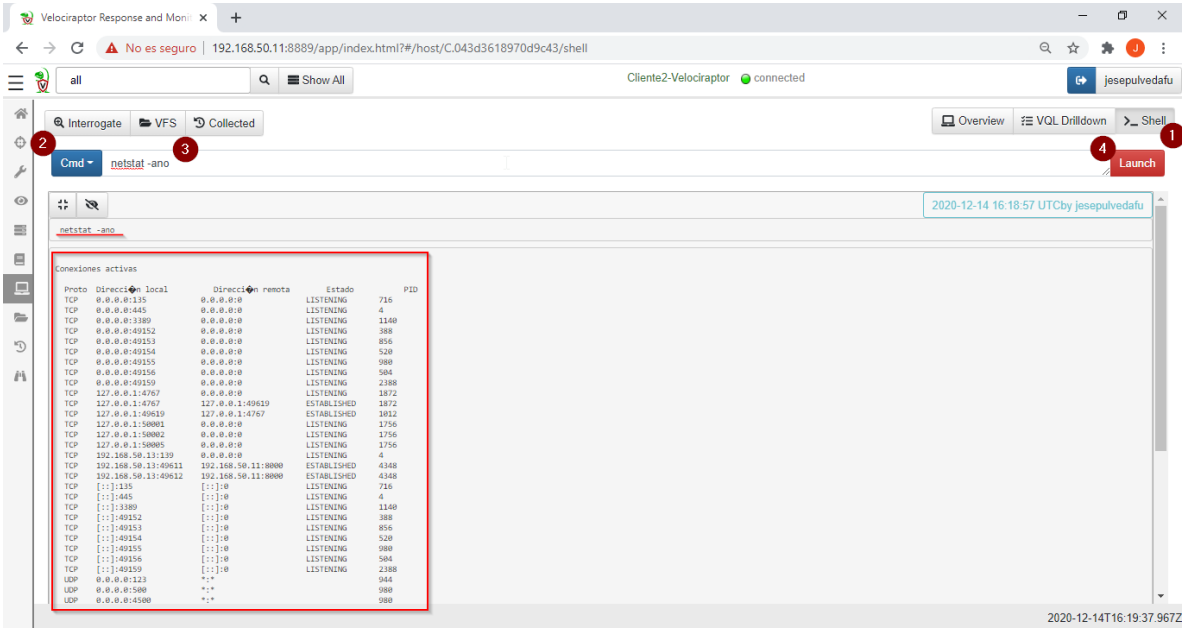
Figura 70. Instrucciones en PowerShell para Cliente1



Fuente: El autor

Con el procedimiento mostrado en la siguiente figura sobre el *Cliente2*, se obtuvo información de conexiones activas TCP/UDP a través del comando *netstat*

Figura 71. Instrucciones en CMS para Cliente2

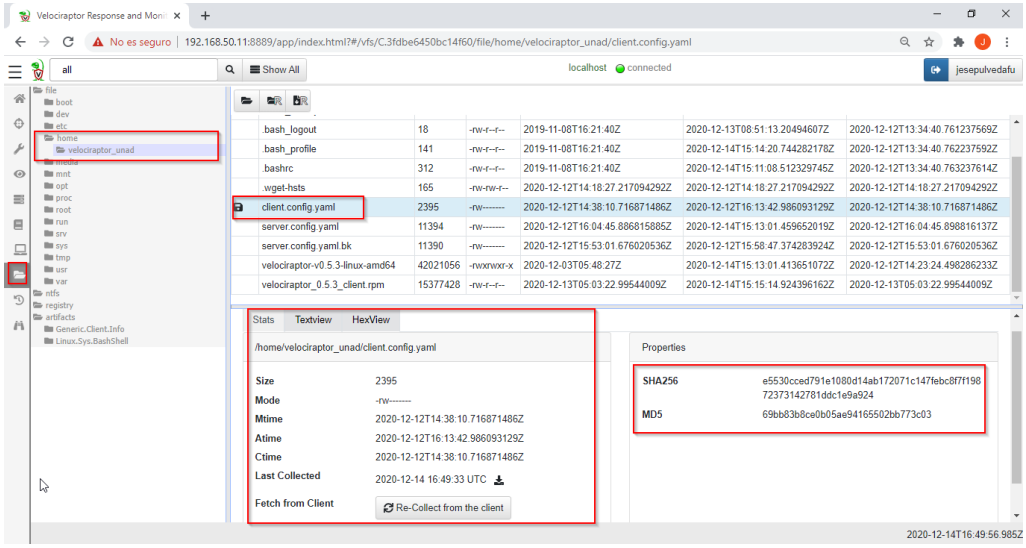


Fuente: El autor

6.5.2. Navegación en sistema de archivos. Desde la función de VFS (Virtual File System) es posible navegar a través del sistema de archivos de los clientes gestionados

La siguiente figura muestra la exploración del sistema de archivos en *Cliente0* desde velociraptor a través de la función de VFS ubicada en el menú de velociraptor (lateral izquierdo)

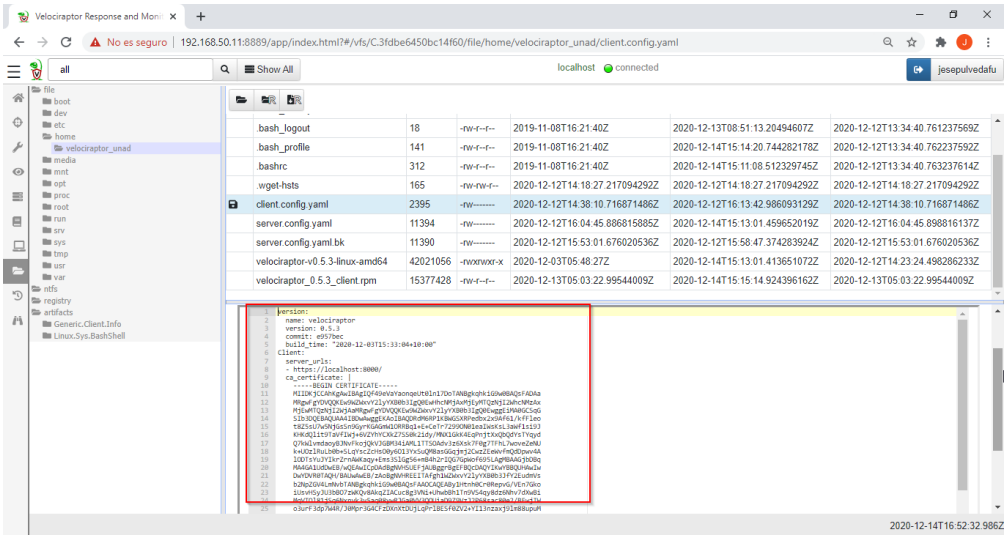
Figura 72. Navegación en sistema de archivos de *Cliente0*



Fuente: El autor

La siguiente figura muestra la visualización del archivo “client.config.yaml” alojado en *Cliente0* desde velociraptor a través de la función de VFS

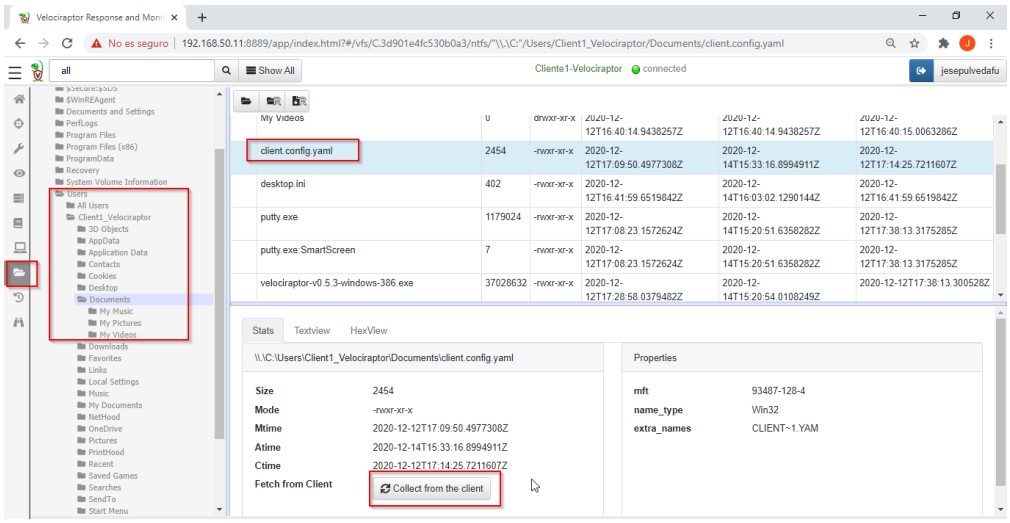
Figura 73. Visualización de archivo de Cliente0



Fuente: El autor

La siguiente figura muestra la exploración del sistema de archivos en *Cliente1* desde velociraptor a través de la función de VFS

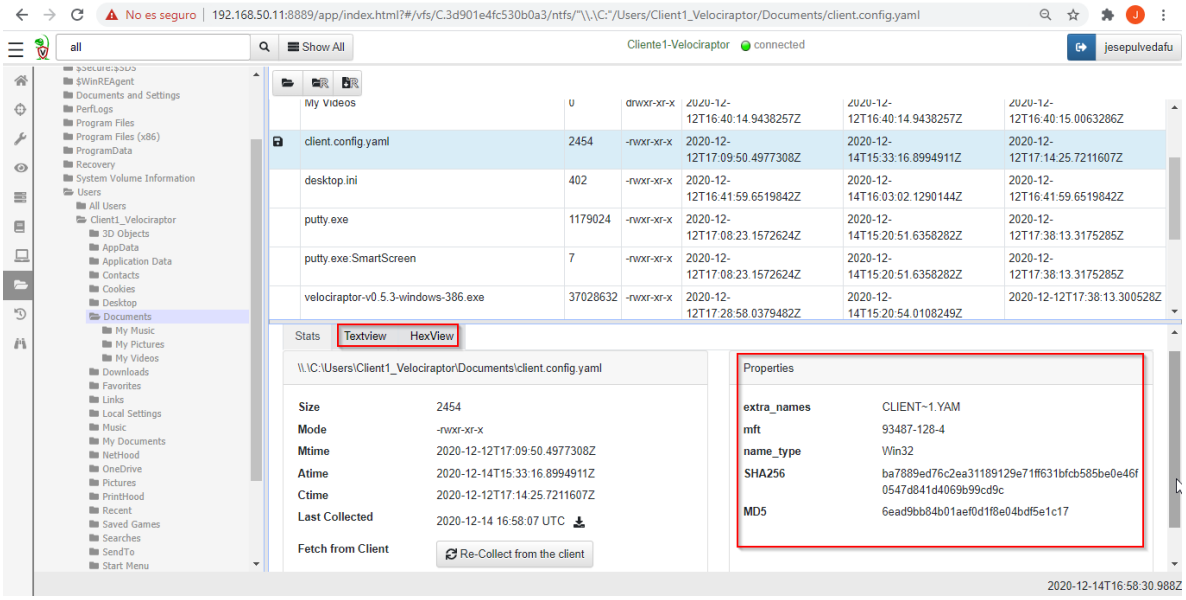
Figura 74. Navegación por sistema de archivos de *Cliente1*



Fuente: El autor

La siguiente figura muestra como a través de la función VFS de velociraptor se obtuvieron detalles importantes del archivo “client.config.yaml” alojado en *Cliente1* como las funciones hash (SHA256 y MD5)

Figura 75. Detalles en archivo de Cliente1 desde VFS

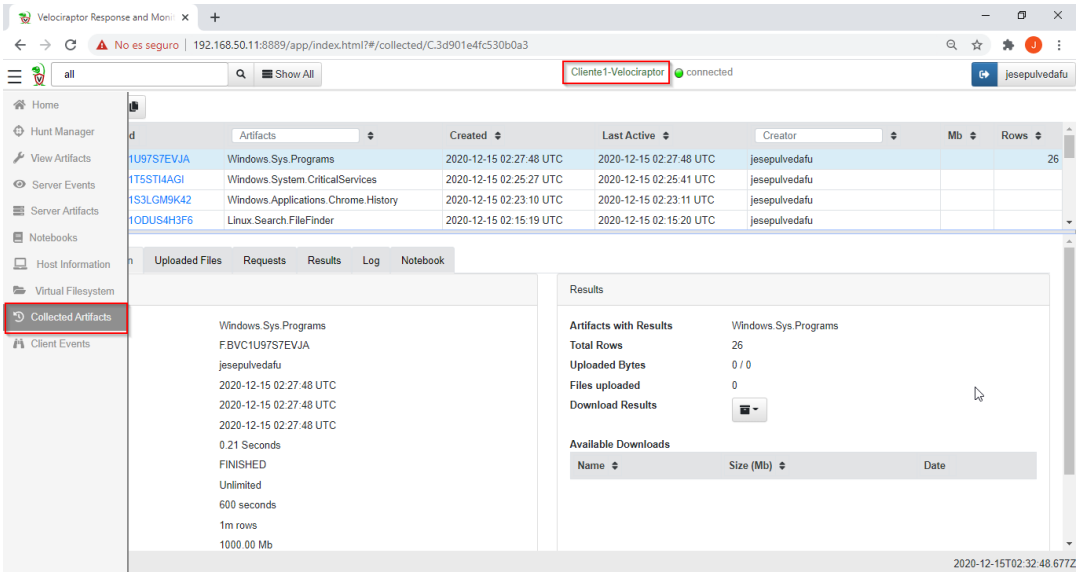


Fuente: El autor

6.5.3. Uso de artefactos. Luego de seleccionar un cliente, es posible hacer uso de los diferentes artefactos con el fin de recopilar información o tomar alguna acción de forma rápida sobre el cliente seleccionado.

Se hizo uso del artefacto “Windows.Forensics.LocalHashes.Glob” con el cual se obtuvo en el servidor de velociraptor una base de datos de los archivos del cliente con su respectivo hash

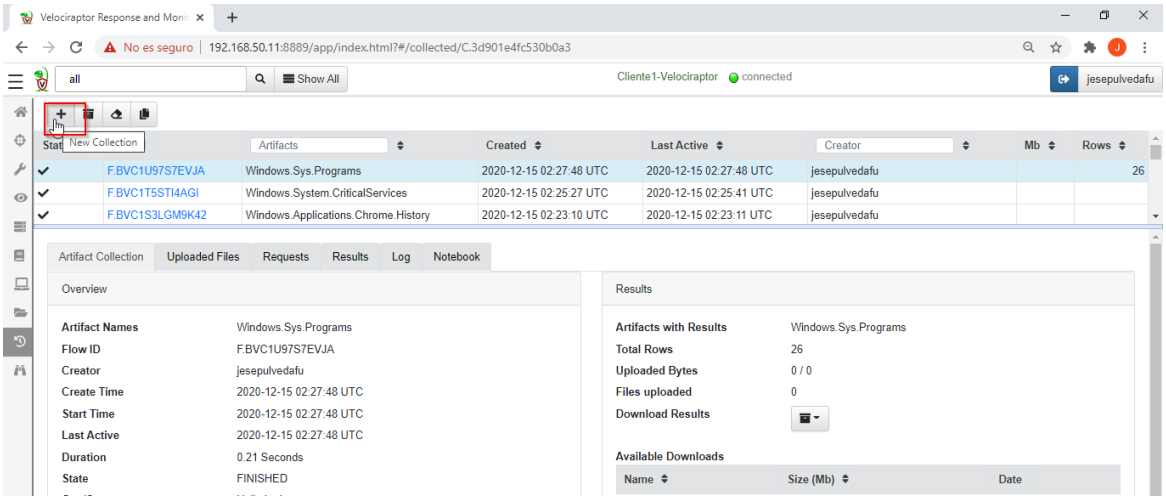
Figura 76. Recolección de información con artefactos



Fuente: El autor

Dar clic en el botón “New Collection”

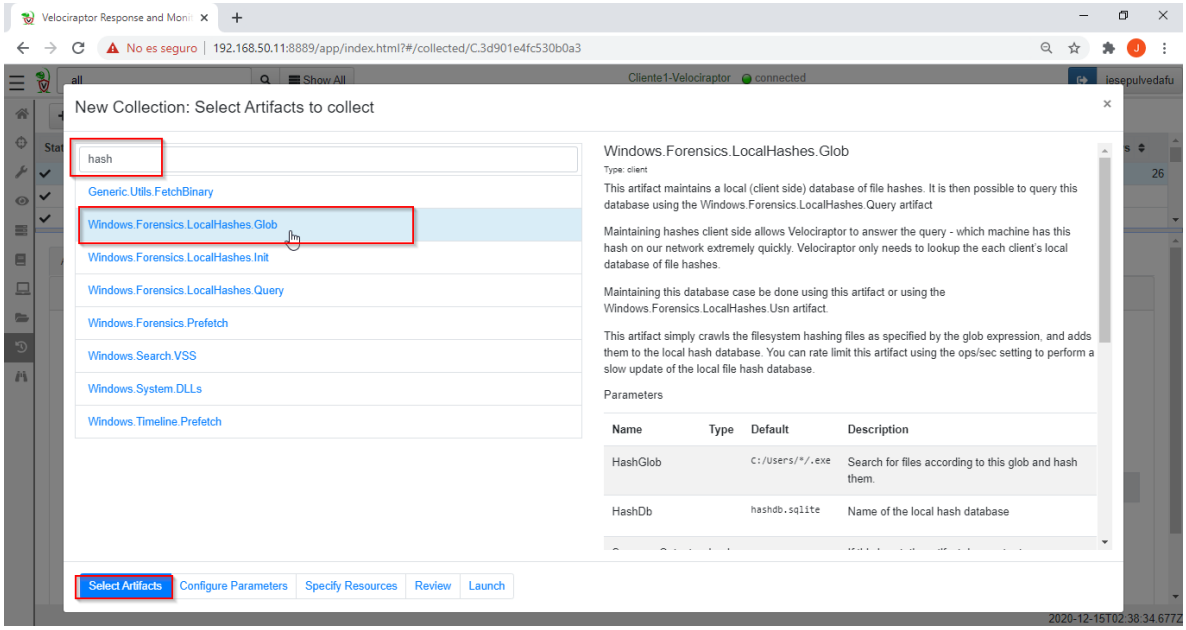
Figura 77. Creación de tarea de recolección de información (1)



Fuente: El autor

Se ingresó una palabra clave en el cuadro texto con el fin de filtrar los resultados y se seleccionó el artefacto a usar

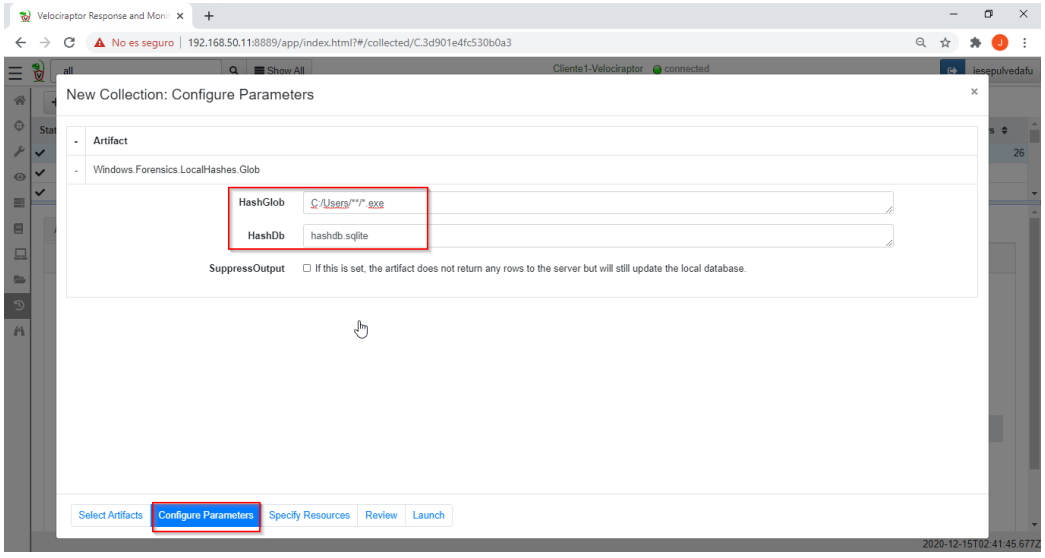
Figura 78. Creación de tarea de recolección de información (2)



Fuente: El autor

Se configuraron los parámetros para el uso del artefacto, por ejemplo, la ubicación en la cual están los archivos de los que se quiere tener el hash

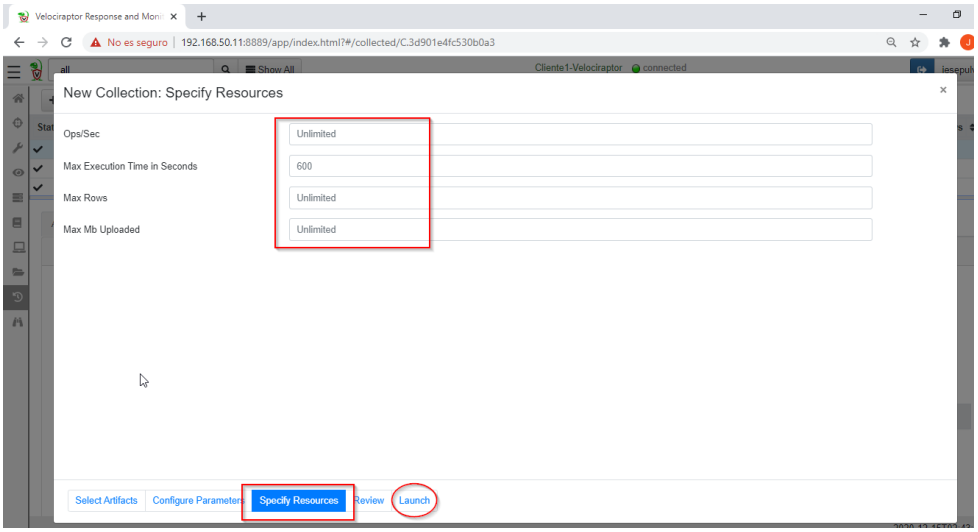
Figura 79. Creación de tarea de recolección de información (3)



Fuente: El autor

Es posible limitar el tiempo o consumo de recursos con el fin de prevenir un comportamiento inesperado en el cliente. Se dejaron los valores por defecto y se continuó con clic en el botón “Launch”

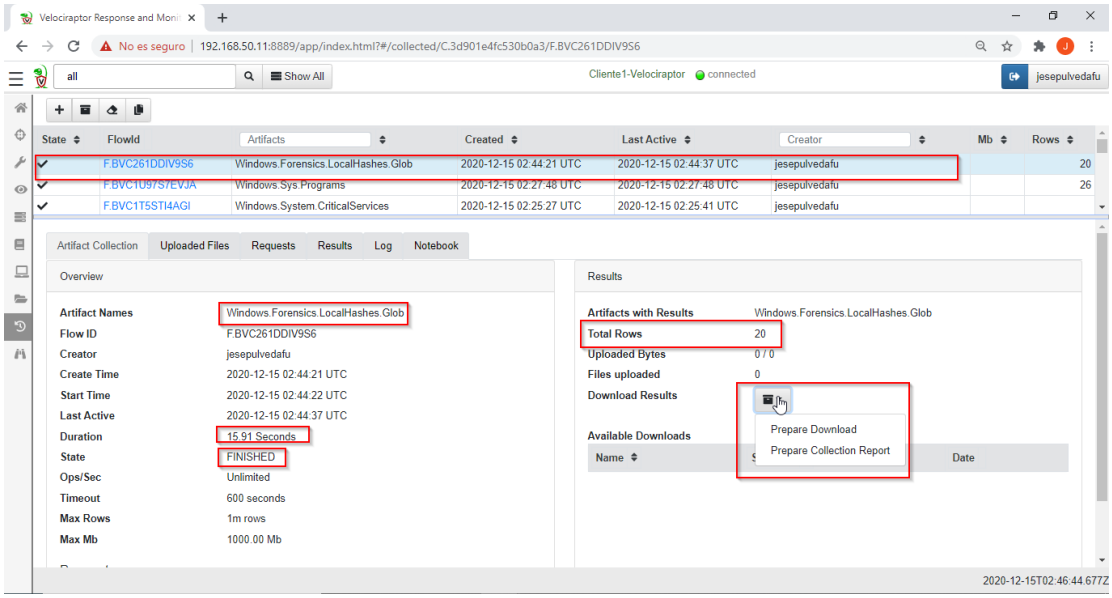
Figura 80. Creación de tarea de recolección de información (4)



Fuente: El autor

Se observó la recolección de data mediante el uso del artefacto definido e información como el estado, tiempo en ejecución, resultados, entre otra. También es posible exportar el reporte de la información

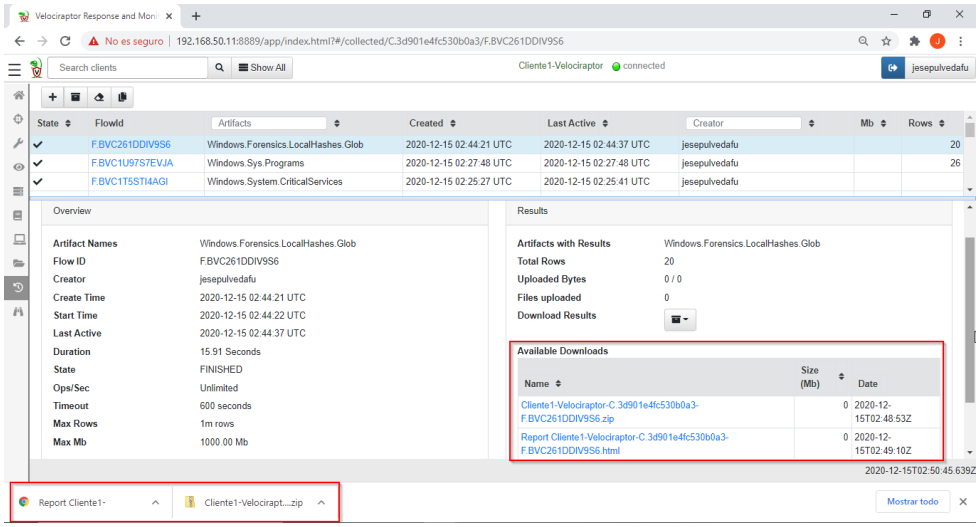
Figura 81. Resultado de recolección de data con artefactos



Fuente: El autor

Se dispone de los reportes para descarga

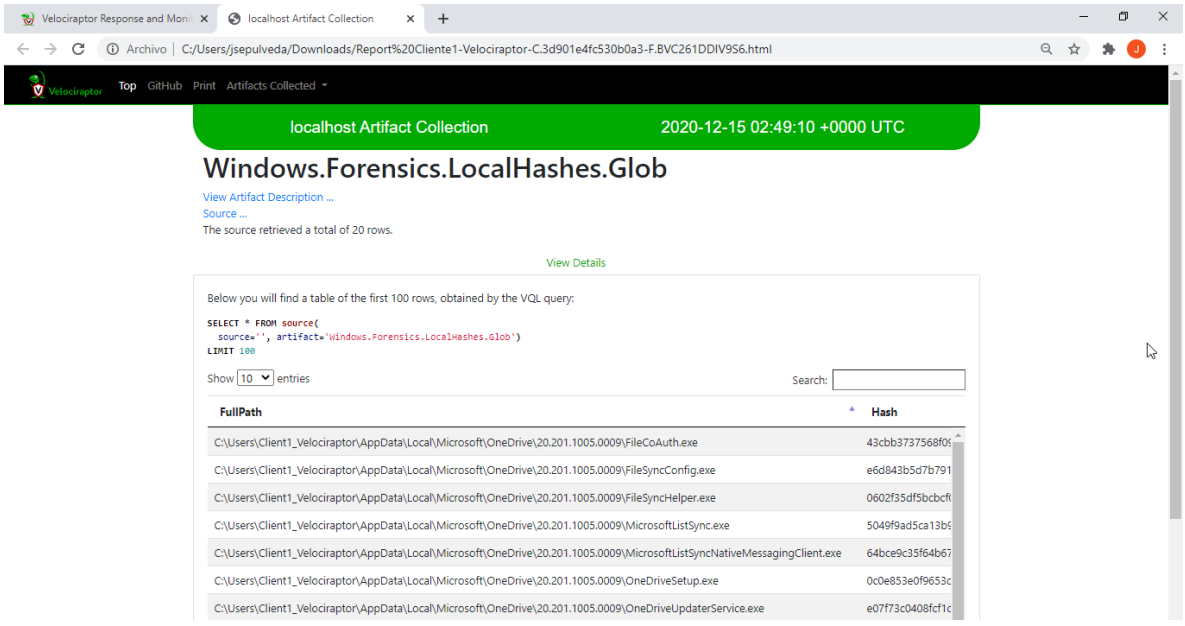
Figura 82. Generación y descarga de reportes de recolección de data con artefactos



Fuente: El autor

Se observa el reporte obtenido generado en formato html

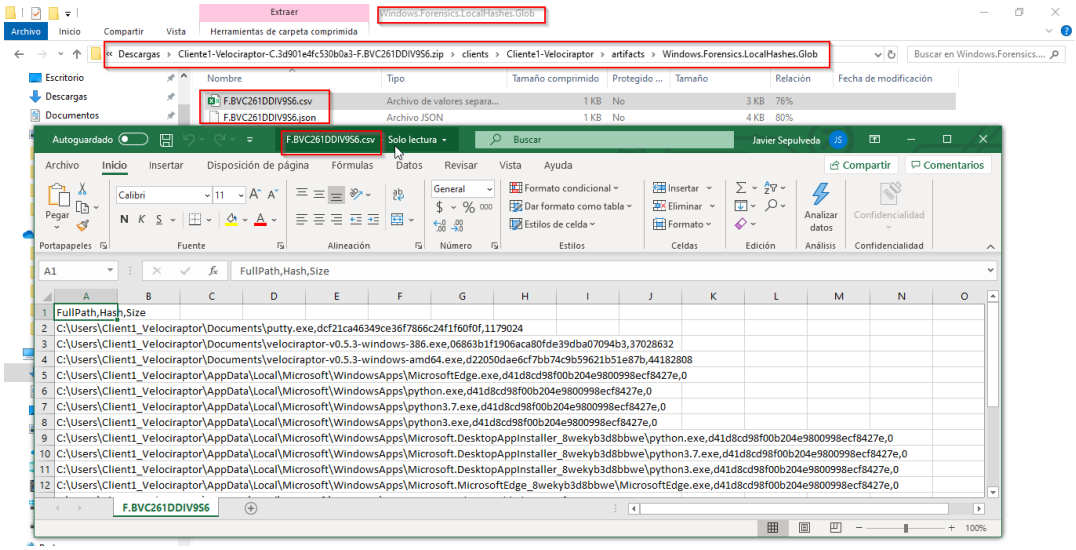
Figura 83. Reporte HTML generado



Fuente: El autor

Se observa la data exportada, se cuenta con formato CSV y JSON

Figura 84. Reporte en CSV de recolección de data con artefactos



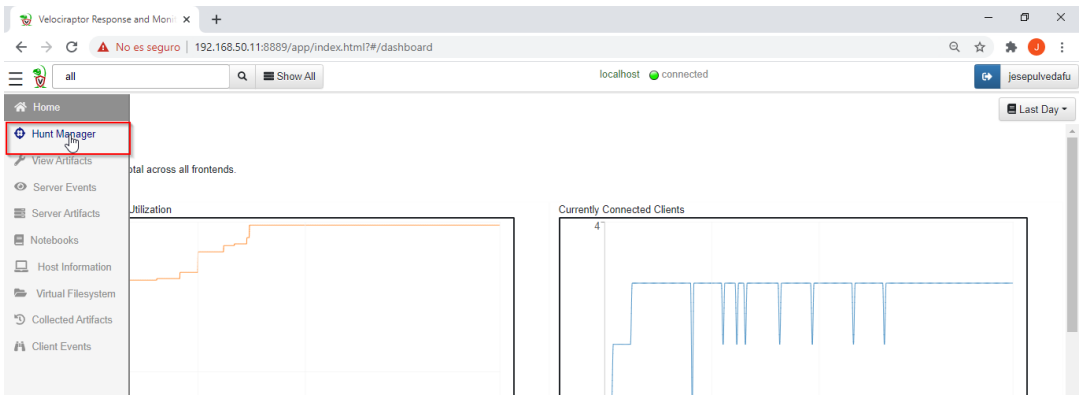
Fuente: El autor

6.5.4. Ejecución de Hunts. Los Hunts son actividades que un investigador puede programar para que se ejecuten a través del tiempo de forma constante. Se puede hacer uso de diferentes Artefactos y configurar una fecha fin para la ejecución, así como la aplicación de filtros por sistema operativo. Los Hunts pueden ser ejecutados en muchos clientes de forma simultánea.

Se ejecutó un Hunt con el fin de extraer información general de los clientes mediante el artefacto “Generic.Client.Info” y la dirección IP pública mediante el artefacto “Network.ExternalIpAddress”

Ubicado en el dashboard principal, se accede al “Hunt Manager” desde el menú de Velociraptor (lateral izquierdo)

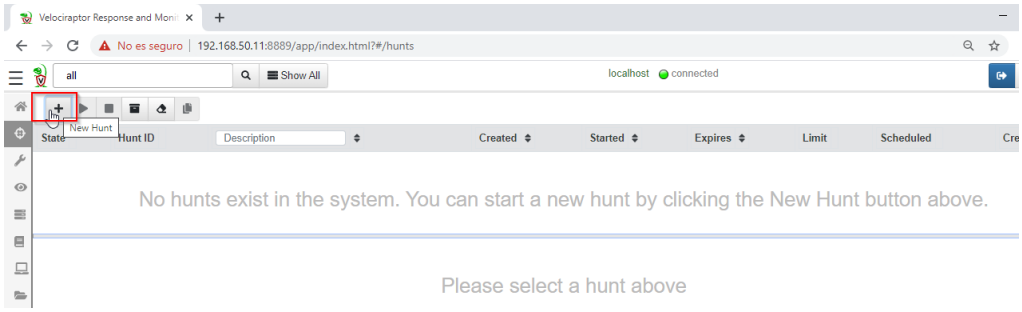
Figura 85. Acceso a Hunt Manager



Fuente: El autor

Dar clic en el botón de “New Hunt”

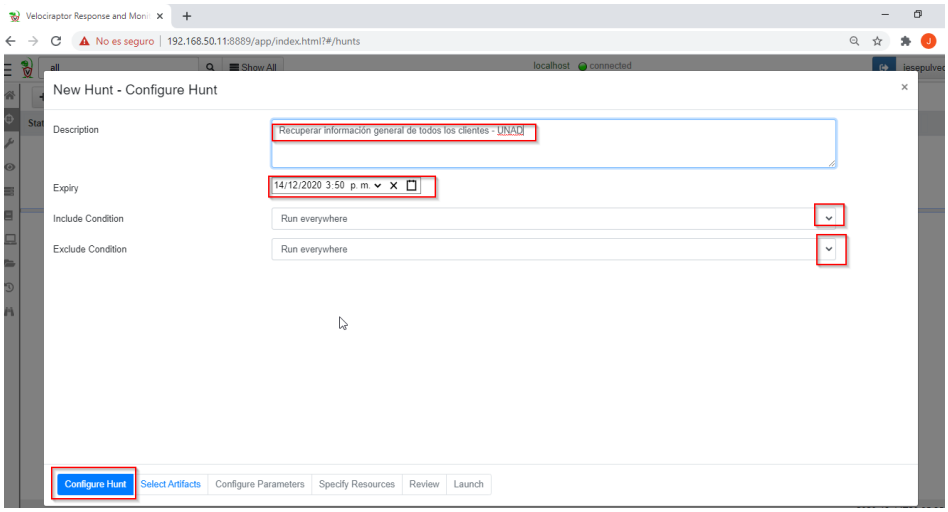
Figura 86. Creación de Hunt (1)



Fuente: El autor

Se ingresó una descripción general y se configuró la fecha de expiración, es decir, la fecha en la que se detiene la ejecución del Hunt. También es posible configurar filtros como por ejemplo ejecutar para determinados sistemas operativos. En este caso se ejecutará el Hunt para todos los clientes

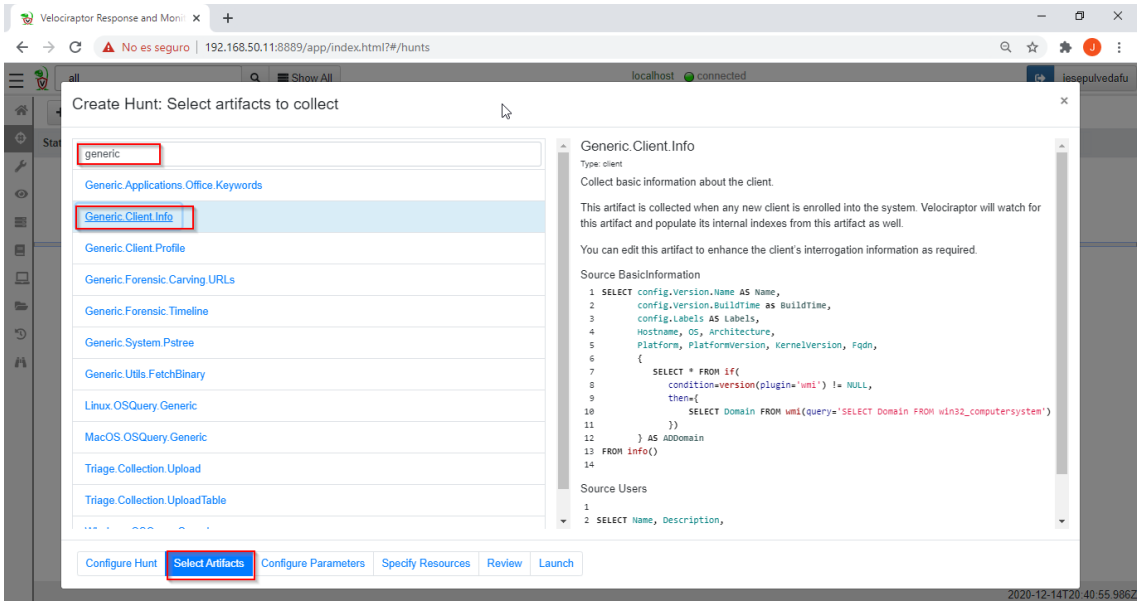
Figura 87. Creación de Hunt (2)



Fuente: El autor

Se seleccionan los artefactos a incluir en el Hunt

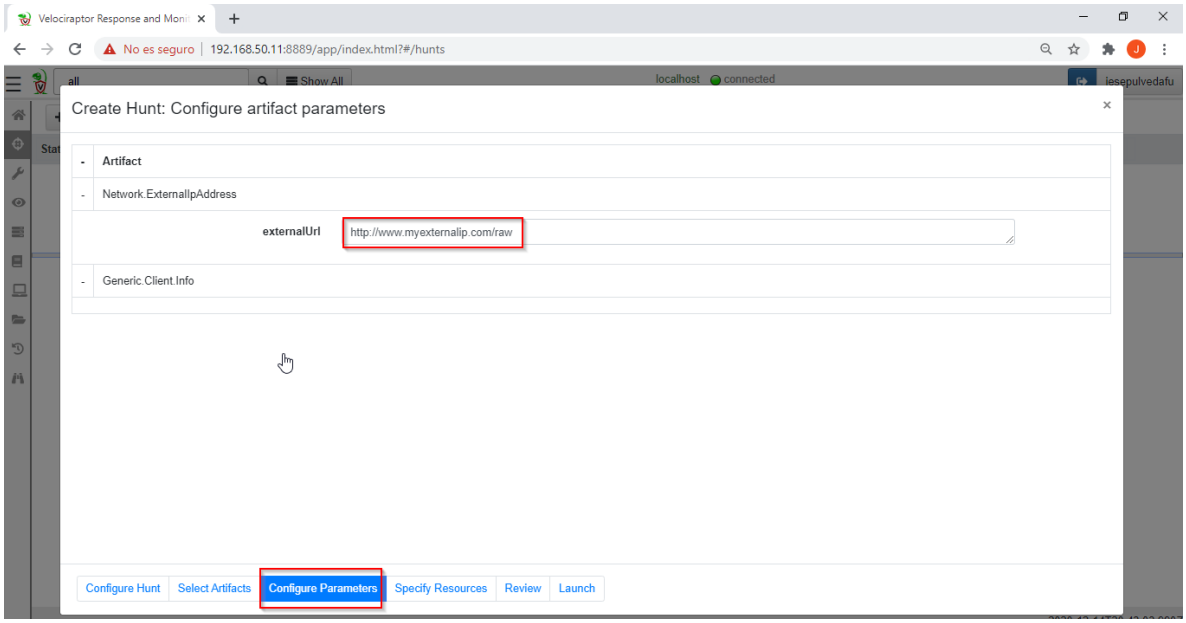
Figura 88. Creación de Hunt (3)



Fuente: El autor

Algunos artefactos requieren parámetros para su correcta ejecución. En este caso el artefacto “Network.ExternalIpAddress”, el cual retorna la dirección IP pública del cliente, permite elegir la URL en internet a través de la cual obtendrá dicha información

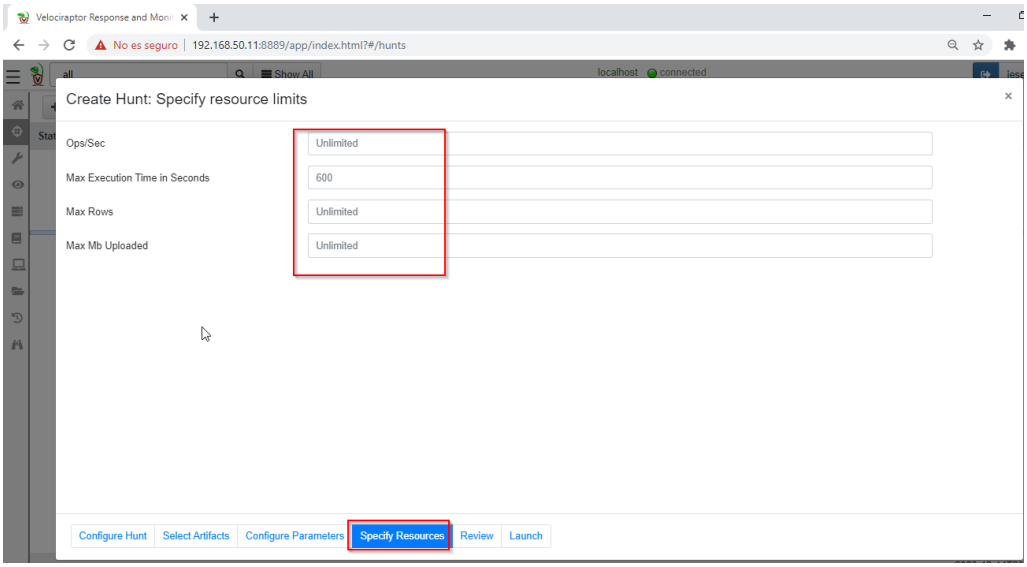
Figura 89. Creación de Hunt (4)



Fuente: El autor

La ejecución del “Hunt” se puede limitar en tiempo o uso de recursos con el fin de evitar un impacto negativo en el rendimiento de los clientes. En este caso se dejaron los valores por defecto

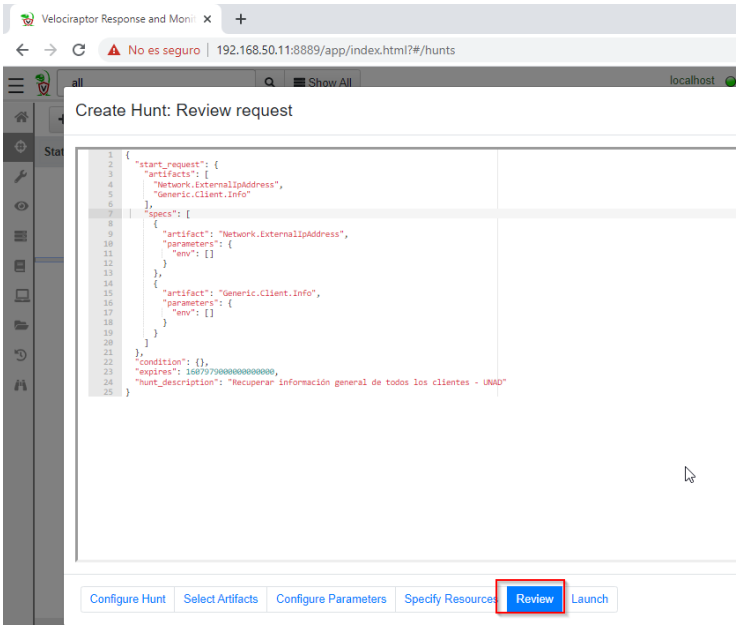
Figura 90. Creación de Hunt (5)



Fuente: El autor

En la pestaña de “review” se observa la configuración del Hunt en formato JSON

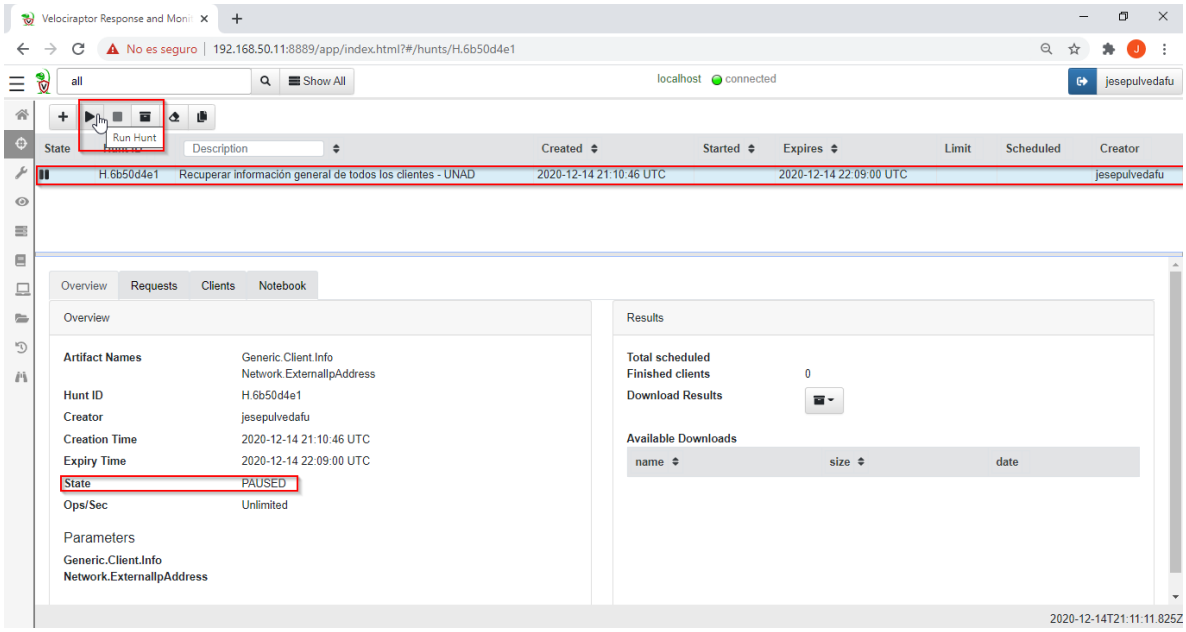
Figura 91. Creación de Hunt (6)



Fuente: El autor

Al dar clic en “Launch” se visualiza en el dashboard de Hunt Manager el Hunt creado, en el estado “Pausado”. Se procedió con clic en el botón “Run Hunt” para iniciar la ejecución

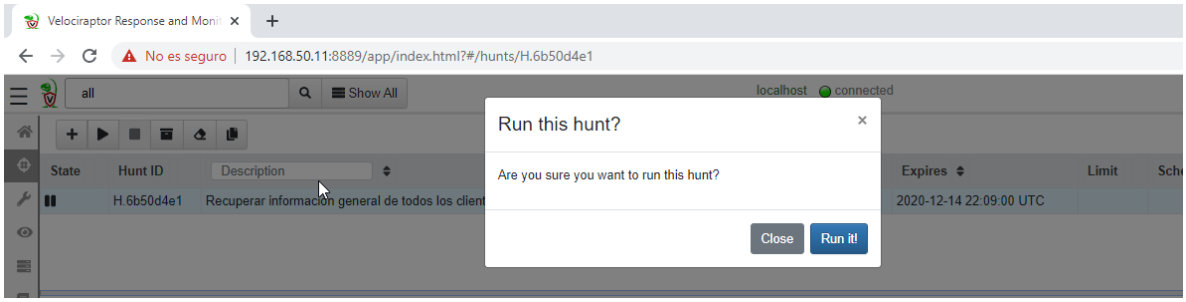
Figura 92. Ejecución del Hunt (1)



Fuente: El autor

Se confirmó la ejecución con “Run It”

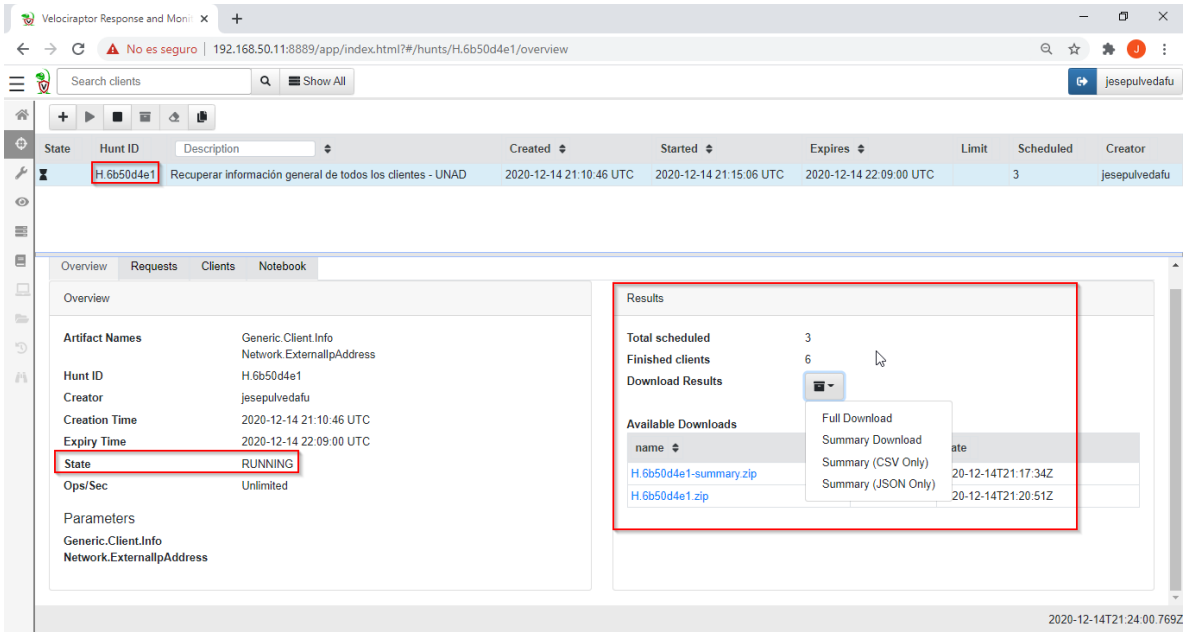
Figura 93. Ejecución del Hunt (2)



Fuente: El autor

Se observó el Hunt en ejecución y con resultados. La información puede ser descargada en diferentes formatos

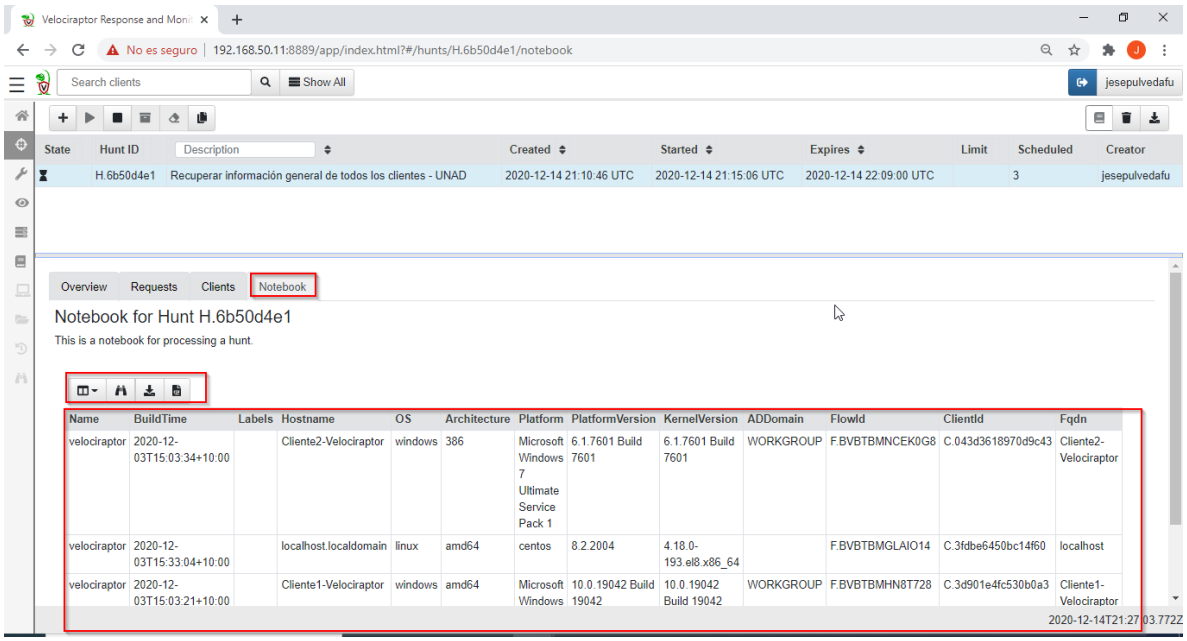
Figura 94. Resultados del Hunt y reportes para descargar (1)



Fuente: EL autor

La información también puede ser inspeccionada o descargada desde el TAB de “Notebook”

Figura 95. Resultados del Hunt y reportes para descargar (2)

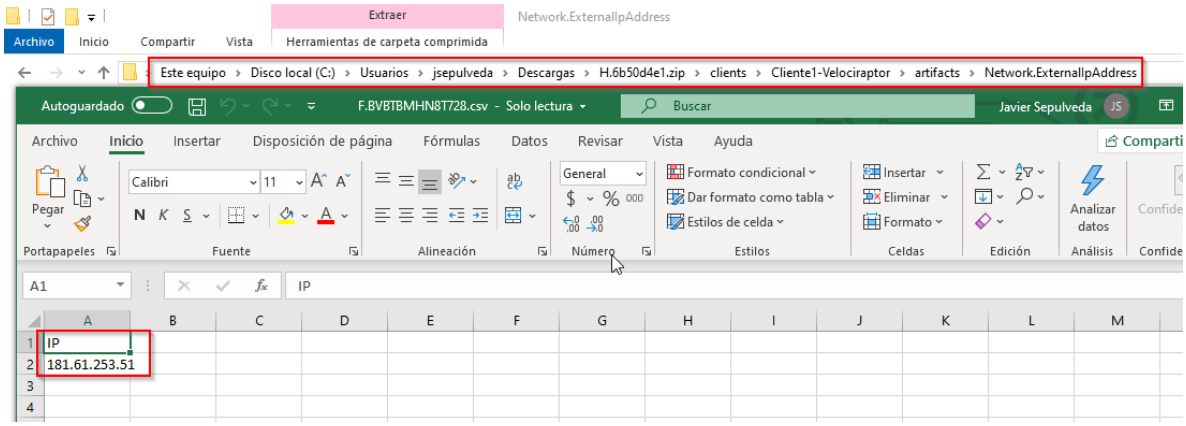


Fuente: El autor

Dentro de las opciones de descarga es posible obtener la información completa y separada para cada cliente o en forma conjunta (resumida).

Se visualiza la información obtenida “Network.ExternalIpAddress” en *Cliente1*

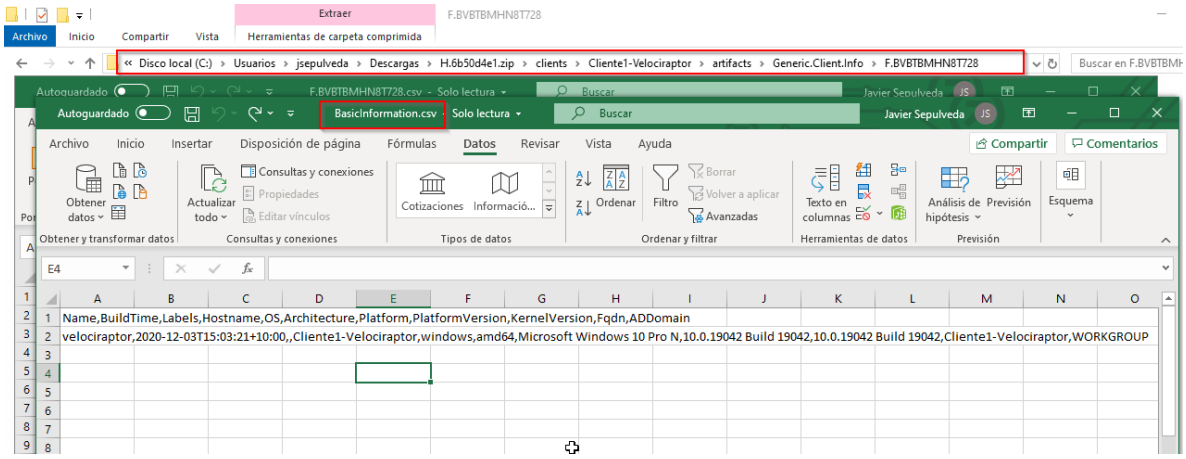
Figura 96. Información descargada de Hunt (1)



Fuente: El autor

Se visualiza la información obtenida para “Generic.Client.Info” en *Cliente1*.

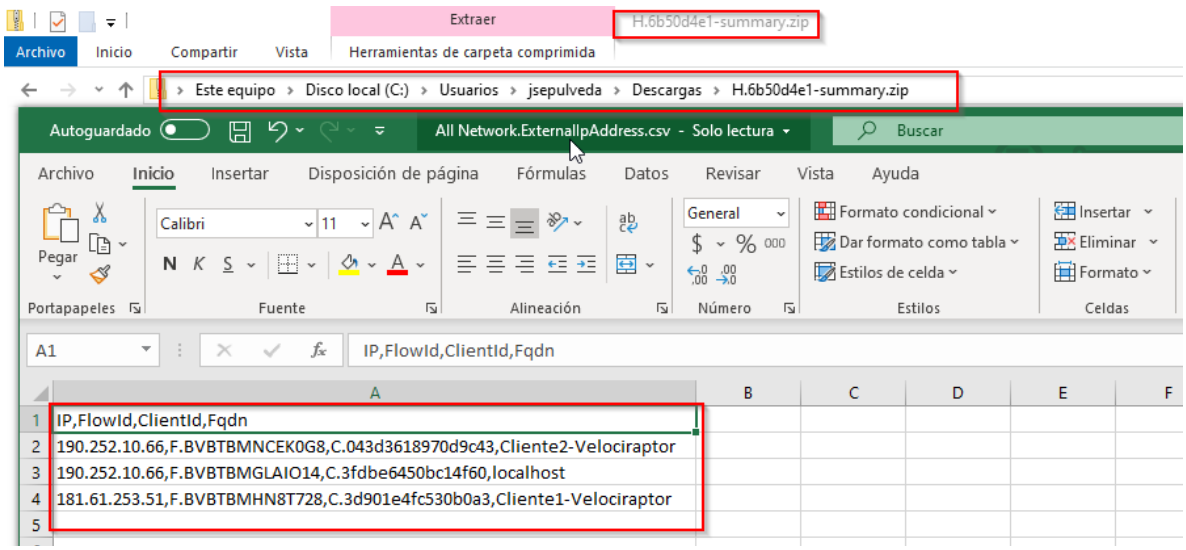
Figura 97. Información descargada de Hunt (2)



Fuente: El autor

Se visualiza la información resumida para Network.ExternalIpAddress

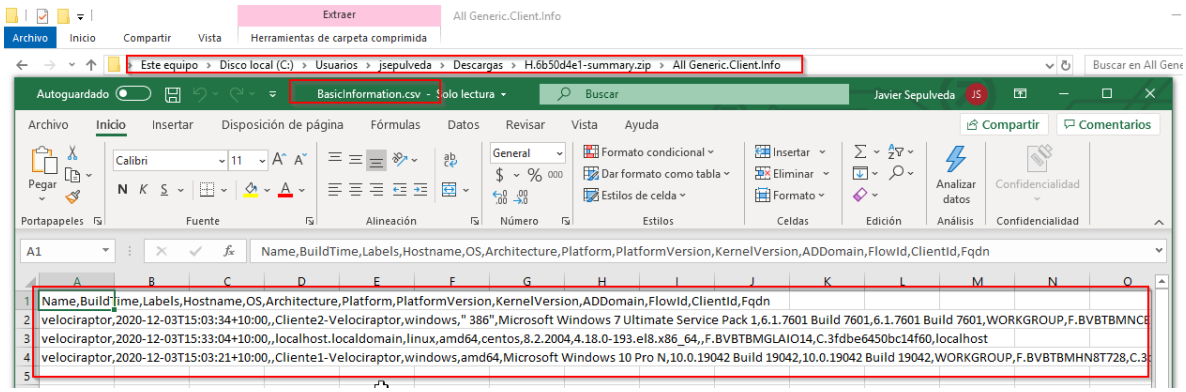
Figura 98. Información descargada de Hunt (3)



Fuente: El autor

Se visualiza la información resumida para Generic.Client.Info

Figura 99. Información descargada de Hunt (4)



Fuente: El autor

6.5.5. Otras funciones. Dado el alcance del desarrollo de esta revisión bibliográfica se entrega al lector y posible implementador y usuario de la plataforma velociraptor la decisión de consultar el cómo mediante la comprensión del funcionamiento del VQL y los artefactos, puede generar estrategias que se adapten a las necesidades de su entorno.

En la web se encuentra bastante documentación y diferentes casos de uso que permiten a través de velociraptor la realización de tareas mucho más avanzadas y que en materia de seguridad informática serán de mucho valor para hacer frente al creciente volumen de amenazas informáticas que con el paso del tiempo evolucionan y dificultan su detección

7. CONCLUSIONES

- Así como día a día surgen nuevas amenazas y técnicas de ataques informáticos, también existe una comunidad de desarrollo de herramientas de código abierto que pone a disposición de las organizaciones variedad de herramientas las cuales pueden aportar en gran medida a la protección de los activos de información y de la infraestructura tecnológica. Con esto, es sumamente importante que las organizaciones, sobre todo las mipymes, conozcan y permitan la adopción de este tipo de plataformas y con mayor razón cuando no se dispone del presupuesto necesario para adoptar una solución de pago.

- Con el análisis de las alternativas de plataformas EDR dispuestas por la comunidad open source analizadas, se evidencia la importancia de conocer el entorno tecnológico en el cual la plataforma va a ser implementada ya que la cantidad de dispositivos a proteger, la variedad en sistemas operativos, la disponibilidad de recurso humano para la administración, entre otros, deben ser factores decisivos para la elección de determinada plataforma.

- Con el desarrollo práctico, se evidenció que la plataforma EDR Velociraptor es una excelente alternativa ya que brinda facilidad en la implementación tanto en el servidor como en el despliegue de los agentes en los clientes, no se presentó afectación con en el rendimiento de los clientes, los tiempos de respuesta en la ejecución son muy bajos y de acuerdo con lo indicado en la documentación, el despliegue realizado en el desarrollo de esta práctica es funcional para la gestión de hasta 10.000 clientes.

- Con la documentación del proceso realizado para la implementación de la plataforma velociraptor, se pone a disposición del lector una guía que permitirá mejorar la protección de los activos de información ya sea a manera de prueba o en un entorno productivo.

- Luego de la implementación de la plataforma EDR Velociraptor se logró evidenciar la integración en un entorno con tres clientes y le ejecución correcta de funciones de investigación y diagnóstico en los mismos.

8. RECOMENDACIONES

- Usar un FQDN para la implementación de la plataforma lo cual evitará el tener que estar modificando los archivos para mapear direcciones IP que con el paso del tiempo pueden cambiar y con mayor razón si la configuración de la red es DHCP

- Realizando búsqueda en la web como apoyo para el proceso de implementación, fue notorio que el volumen de casos de implementación de la herramienta sobre Sistema Operativo Linux con Ubuntu como distribución es mayor, lo cual, aunque no generó ningún obstáculo en el desarrollo de esta práctica la cual se hizo sobre distribución Centos 8, puede que para el lector sea un factor de importancia para elegir Ubuntu como distribución para el servidor de velociraptor.

- Una vez realizado el despliegue de la plataforma Velociraptor, se evidenció que el estándar horario se configura automáticamente en UTC, por lo cual se recomienda configurarlo de acuerdo con la zona horaria para tener una lectura más fácil de los eventos.

- La documentación para la implementación publicada en el sitio web oficial conlleva a la configuración y despliegue de los servicios de velociraptor en modo no persistente con lo que de reiniciarse el servidor y/o los clientes, los servicios no se iniciarán automáticamente. Desde el servidor de velociraptor es posible generar los paquetes de instalación los cuales instalarán los servicios en el sistema de forma persistente.

- Si bien, el proceso de implementación es sencillo, es altamente recomendable que quien tome el rol de administrador de la herramienta, profundice en los conceptos de VQL y artefactos ya que esto permitirá construir funciones más potentes y apropiadas al entorno en donde se haya implementado

9. BIBLIOGRAFÍA

ALBERTS, C, *et al.* Defining Incident Management Processes for CSIRTs: A Work in Progress. 2004

ASHMAN, O. Top 5 Open Source Incident Response Automation Tools. [sitio web] [Consulta: 21 de noviembre de 2020]. Disponible en https://www.cyberbit.com/blog/security-operations/top-5-open-source-incident-response-automation-tools/ 2017

AUDEA. Indicadores de Compromiso en la gestión de riesgos. [sitio web]. [Consulta: 23 de noviembre de 2020] En: https://www.audea.com/indicadores-compromiso-la-gestion-riesgos/ 2018

AVG. ¿Qué es el malware? Cómo funciona el malware y cómo eliminarlo?. En: https://www.avg.com/es/signal/what-is-malware. 2020

BARCA URBINA, Gabriel. Introducción a la seguridad informática. México D.F. 2016.

BELCIC, Ivan. ¿Qué es un exploit en seguridad informática?. En https://www.avg.com/es/signal/computer-security-exploits Marzo 2021

BELLO VIEDA, Jaime Andrés. Soluciones Endpoint Detection and Response Open-Source. Estado del arte, propuesta de medición, análisis y evaluación para determinar su implementación y aplicabilidad en ambientes empresariales. España, 2019

BEJTLICH, R. The Practice of Network Security Monitoring: Understanding Incident. No starch Press. 2013

BOTTE, Antoine. Antivirus, epp and edr what differences? Vanves. 2020

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES (CCIT). Informe Tendencias Cibercrimen Colombia 2019-2020

CISCO, What Is an Exploit? En: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009. Bogotá. 2009

CYBRINT. Traditional Antivirus vs. EDR (Endpoint Detection and Response). [sitio web]. [Consulta: 21 de diciembre de 2020]. Disponible en: https://cybriant.com

CYNET. Endpoint protection and EDR. [sitio web] New York. [Consulta: 18 de diciembre de 2020]. Disponible en: www.cynet.com

ERIC DAVIS, M. L. (2017). Next-Generation Endpoint Security. INSIGHTS.

ESTRADA, Carlos. Estudio sobre el malware Ransomware. España. 2018

FIREEYE. Endpoint Security Tools. [Consulta: 06 de mayo de 2020]. Disponible en https://www.fireeye.com/solutions/hx-endpoint-security-products.html 2018

FORCEPOINT. What is Phishing? Phishing Attacks and Prevention Explored. En: https://www.forcepoint.com/es/cyber-edu/phishing-attack

FOWLER, Kevvie. Data Breach Preparation and Response: Breaches are Certain, Impact is Not. Cambridge, 2016.

FREILING, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Digital Forensics. [sitio web]. [Consulta: 04 de abril de 2020]. Disponible en https://www.imf-conference.org/imf2007/2%20Freiling%20common_model.pdf 2007

GATTIE, Ian. Why Endpoint Detection and Response (EDR) is Superior to Your Current Antivirus (AV) Tools. [sitio web]. [Consulta: 16 de diciembre de 2020]. Disponible en: https://avaloncybersecurity.com/ New York. 2018

GÓMEZ VIEITES, Álvaro. Enciclopedia de la Seguridad Informática. Madrid. 2014

II, W. G., & Heiser, J. G. Computer Forensics: Incident Response Essentials. Pearson Education. 2002

INCIBE, Instituto Nacional de Ciberseguridad. Una guía de aproximación para el empresario. En: Glosario de términos de Ciberseguridad. León. 2017.

INCIBE, Instituto Nacional de Ciberseguridad. ¿Qué camino debo seguir para gestionar correctamente un incidente de seguridad en mi empresa? España, 2014.

ISO, N. (s.f.). ISO 27001 Seguridad de la Información. [sitio web] [Consulta:17 de diciembre de 2020]. Disponible en http://www.normas-iso.com/iso-27001/

JUMBO, Tatiana. Metodología para el análisis de malware en un ambiente controlado. Cuenca, Ecuador. 2017 p. 49

KENT, Karen, *et al*. Guide to Integrating Forensic Techniques into Incident Response. 2006

KRAL, P. Incident Handler's Handbook. [Consulta:18 de diciembre de 2020]. Disponible en https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 2011

LIGGETT Terry. Evolution of endpoint detection and response platforms. New York. 2018

LOEBENBERGER, Daniel. Evolution! From Creeper to Storm: Presentation for the Seminar on “Malware”

LUTTGENS, J. T., Pepe, M., & Pepe, M. Incident Response & Computer Forensics. McGraw-Hill Education Group. 2014

MANDIA, K. Incident Response: Investigating Computer Crime. McGraw-Hill Professional. 2001

MATACHANA, Y. L. Los virus informáticos: una amenaza para la sociedad. Editorial Universitaria. 2009

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Marco de la Transformación Digital para el Estado Colombiano, Colombia. 2020

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Plan TIC 2018-2022 El Futuro Digital es de Todos. Colombia. 2020

M2PRESSWIRE. Global Endpoint Detection and Response Market Analysis and Forecasts to 2025. M2PressWIRE. 2018

NIST, National Institute of Standars and Technology. Handling an Incident. En: Computer Security Incident Handling Guide

NIST, National Institute of Standards and Technology. Recommendations of the National Institute of Standards and Technology. En: Computer Security Incident Handling Guide. Estados Unidos. 2012

OAS. (s.f.). Metodología de Respuesta a Incidentes (IRMs) IRM5-ComportamientoMaliciosoEnRed-OEA. [documento electrónico]. [Consulta:04 de abril de 2020]. Disponible en https://www.sites.oas.org/cyber/Documents/Metodolog%C3%ADa%20de%20Respuesta%20a%20Incidentes%20(IRMs)%20IRM5-ComportamientoMaliciosoEnRed-OEA.pdf

OPTARIS. Guía de planificación de respuesta a incidentes para 2019. En: www.optaris.com. Buenos Aires. 2017

OWASP, The Open Web Application Security Project. En: Ingeniería Social, Hacking Psicológico. OWASP Latam Tour. República Dominicana. 2016

PEREZ, Ignacio. ¿Qué es una botnet? Conoce al control remoto de los ciberdelincuentes. [sitio web]. [Consulta: 17 de diciembre de 2020] Disponible en: https://www.welivesecurity.com/la-es/2014/08/06/botnets-control-remoto-ciberdelincuentes/ 2014

PETTERS, Jeff. Endpoint Detection and Response (EDR): Everything You Need to Know. [sitio web]. [Consulta: 16 de diciembre de 2020]. Disponible en www.varonis.com

PUENTES, Juan. Empresas colombianas solo invierten 20% de presupuesto en ciberseguridad. En: larepublica.co Septiembre 2018 Palo Alto Networks. What is an Endpoint? [sitio web]. [Consulta: 17 de diciembre de 2020]. Disponible en: https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint 2020

RODRÍGUEZ, Guillermo. En: Como implementar un potente SOC con herramientas Open Source. DragonJARCON Conferencia. Manizales, 2020

ROMERO CASTRO, Martha Irene, et al. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Alcoy, 2018

SANS. Incident Handling - Security 504. [Documento electrónico]. [Consulta:18 de mayo de 2020]. Disponible en www.sans.org 2011

SANS INSTITUTE. Using IOC (Indicators of Compromise) in Malware. SANS INSTITUTE. 2013

SCHULTZ, E., & Shumway, R. Incident response: a strategic guide to handling system and network security breaches. Sams Indianapolis. 2001

VALCK, E. Major incident response: Collecting ante-mortem data. [sitio web]. [Consulta: 21 de diciembre de 2020]. Disponible en https://www.sciencedirect.com/science/article/pii/S0379073806000600 2006

VELOCIRAPTOR. Velocidex sitio web oficial. [sitio web]. 2020. [Consulta: 21 de diciembre de 2020]. Disponible en: https://www.velocidex.com/

VIEITES, Á. G. Seguridad en equipos informáticos. RA-MA Editorial. 2014

VOIGT, L. Incident Response Plan: 6 Essential Steps for Responding to a Security Incident. [sitio web]. [Consulta:21 de diciembre de 2020]. Disponible en https://www.exabeam.com/incident-response/steps/ 2014

YOHAI, Alberto. TENDENCIAS CIBERCRIMEN COLOMBIA 2019 – 2020. Informe de las tendencias del cibercrimen en Colombia (2019-2020), 2019.

ANEXO

Resumen Analítica Especializado -RAE

Fecha de Realización:	16/04/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Infraestructura tecnológica y seguridad de redes
Título:	ANÁLISIS DE HERRAMIENTAS ENDPOINT AND DETECTION RESPONSE (EDR) DE SOFTWARE LIBRE
Autor(es):	Sepulveda Fuentes, Javier Eduardo
Palabras Claves:	Endpoint Detection and Response, Incidente, riesgo, vulnerabilidad, gestión de incidentes, malware.
Descripción:	El proyecto desarrollado permite al lector comprender el funcionamiento de una plataforma EDR y da a conocer las características principales de una herramienta de este tipo, así como su afinidad al proceso de gestión y respuesta a incidentes de seguridad informática. De manera adicional, el lector encontrará un análisis comparativo entre algunas herramientas EDR ofrecidas por la comunidad opensource y contará con una guía de implementación, acerca del paso a paso para implementar una de estas herramientas, así como la experimentación de algunas de sus funciones
Fuentes bibliográficas destacadas: Libro Bejtlich, R. The Practice of Network Security Monitoring: Understanding Incident. No starch Press. 2013 Libro electrónico Eric Davis, M. L. (2017). Next-Generation Endpoint Security. INSIGHTS. Página de sitio web Kral, P. Incident Handler's Handbook. [Consulta:]. Disponible en https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 2011	
Contenido del documento:	El desarrollo de este proyecto establece un punto de partida para que principalmente las MiPymes que para el desarrollo de su funcionamiento y su actividad comercial tengan activos de información, puedan iniciar

	el análisis y posible implementación de una herramienta tecnológica basada en software libre que permita proteger parte de su infraestructura, específicamente los puntos finales (endpoints), de la creciente oleada de ataques informáticos que día a día amenazan con deteriorar e interrumpir sus actividades. Una plataforma EDR (Endpoint and Detection Response) es una herramienta que apoya parte del proceso de gestión y respuesta a incidentes de seguridad de la información aportando información de valor de forma organizada y haciendo posible la ejecución de acciones según lo requerido, de acuerdo con cada una sus etapas. Se abordarán diferentes soluciones EDR ya existentes y ofrecidas al público por la comunidad open source, realizando un análisis sobre características como soporte ofrecido por la comunidad, requisitos de sistema, efectividad, entre otras, que al final darán sustento a la elección de una de ellas. Finalmente, con la plataforma EDR elegida, se analizará la implementación de esta, identificando así su funcionamiento y elaborando la documentación que permita a cualquier persona o entidad replicar dicho proceso en su propia infraestructura tecnológica. Debido a la naturaleza de las plataformas EDR, es fundamental abordar de forma paralela el tema de proceso de gestión y respuesta a incidentes de seguridad informática, entendiendo las acciones a realizar en cada una de sus etapas. PALABRAS CLAVE: EDR, Incidente, evento, riesgo informático, vulnerabilidad, gestión de incidentes, malware.
Conceptos adquiridos :	Luego del desarrollo de este trabajo de grado, se obtiene claridad acerca de los conceptos básicos de la seguridad informática y del proceso de gestión y respuesta a incidentes de seguridad. Se evidencia también el aporte significativo que la comunidad opensource realiza en el

	desarrollo de plataformas tecnológicas, específicamente herramientas de seguridad informática de tipo EDR, las cuales pueden ser incluidas en la infraestructura tecnológica de las organizaciones y apoyar en gran medida a la detección y mitigación de amenazas informáticas.
Conclusiones:	Así como día a día surgen nuevas amenazas y técnicas de ataques informáticos, también existe una comunidad de desarrollo de herramientas de código abierto que pone a disposición de las organizaciones variedad de herramientas las cuales pueden aportar en gran medida a la protección de los activos de información y de la infraestructura tecnológica. Con esto, es sumamente importante que las organizaciones, sobre todo las mipymes, conozcan y permitan la adopción de este tipo de plataformas y con mayor razón cuando no se dispone del presupuesto necesario para adoptar una solución de pago. Con el análisis de las alternativas de plataformas EDR dispuestas por la comunidad open source analizadas, se evidencia la importancia de conocer el entorno tecnológico en el cual la plataforma va a ser implementada ya que la cantidad de dispositivos a proteger, la variedad en sistemas operativos, la disponibilidad de recurso humano para la administración, entre otros, deben ser factores decisivos para la elección de determinada plataforma. Con el desarrollo práctico, se evidenció que la plataforma EDR Velociraptor es una excelente alternativa ya que brinda facilidad en la implementación tanto en el servidor como en el despliegue de los agentes en los clientes, no se presentó afectación con en el rendimiento de los clientes, los tiempos de respuesta en la ejecución son muy bajos y de acuerdo con lo indicado en la documentación, el despliegue realizado en el desarrollo de esta práctica es funcional para la gestión de hasta 10.000 clientes.

	Con la documentación del proceso realizado para la implementación de la plataforma velociraptor, se pone a disposición del lector una guía que permitirá mejorar la protección de los activos de información ya sea a manera de prueba o en un entorno productivo. Luego de la implementación de la plataforma EDR Velociraptor se logró evidenciar la integración en un entorno con tres clientes y le ejecución correcta de funciones de investigación y diagnóstico en los mismos.