UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: Ing. Bryan Gustavo Jaya Quishpe
Ing. Robert Napoleón Granda García
Lic. Yadira Pamela García Toapanta
Ing. Julio César Gancino Vargas
TUTOR: Mgs. Ronie Martínez

Análisis de Ransomware con SIEM y Hacking Ético para la Empresa SoftwareSystem GC

APROBACIÓN DEL TUTOR

Yo, Mgs. Ronie Martinez, certifico que conozco a los autores del presente trabajo siendo los responsables exclusivos tanto de su originalidad y autenticidad, como de su contenido.

Firmado electrónicamente por:
RONIE STALIN
MARTINEZ GORDON

Mgs. Ronie Martinez

DIRECTOR DE TESIS

AGRADECIMIENTO.

CERTIFICACIÓN DE AUTORÍA

Nosotros, Pamela García, Gustavo Jaya, Julio Gancino y Robert Granda, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Pamela García.
CC. 1718294281

Gustavo Jaya.
CC. 1718322777

Julio Gancino.
CC. 1714626270

Robert Granda
CC. 1709693855

DEDICATORIA

A nuestras familias, quienes supieron estar ahí, para apoyarnos de manera desinteresada**.**

AGRADECIMIENTO

A la Universidad Internacional del Ecuador, al cuerpo docente y administrativo, por todo el apoyo otorgado en este proceso y de manera especial a todos nuestros profesores quienes, durante la Maestría, aportaron de manera profesional, con su conocimiento y experiencias para mejorar nuestras competencias.

RESUMEN.

Si observamos el paso del tiempo y a ello, le sumamos el desarrollo social, por ende encontramos que la tecnología avanza a pasos agigantados, va transformando la realidad humana en muchos ámbitos, herramientas tecnológicas de diversas finalidades que se muestran letales, se fraguan paulatinamente en la realidad que vivimos, colapsando en muchos casos infraestructuras críticas de estados inutilizando dichos servicios a los pobladores así como afectando a la información personal de millones a cambio de una recompensa, estamos hablando del Ransomware[1].

Es importante citar, que la tecnología también ofrece soluciones que acompañados de protocolos como OSWAP[2] sumado a técnicas de Hacking Ético y herramientas como SIEM[3], hacen posible minimizar los posibles vectores de ataque hacia una determina infraestructura empresarial sea esta pública o privada, para minimizar el impacto de ciberataques que son mitigados a través de buenas prácticas profesionales en el campo de la ciberseguridad, es por ello, que la utilización correcta de todas las facilidades tecnológicas, sumado al adecuado asesoramiento, capacitación constante a los involucrados, son factores esenciales al momento de hablar de ciberseguridad.

[1] Tipo de Malware que busca comprometer la información de personas o la infraestructura que contiene esta, encriptando las bases de datos y exigiendo para su liberación una recompensa económica.
[2] Open Web Application Security Project, Propone directrices para mejorar la seguridad de aplicaciones, a través de buenas prácticas profesionales.
[3] Security Information and Event Management, gestiona las alertas que detecta en la infraestructura de una organización, para ayudar a prevenir incidentes futuros de ciberseguridad.

ABSTRACT

If we observe the passage of time and add social development to this, we find that technology, by leaps and bounds, is transforming human reality in many areas, technological tools for various purposes that prove to be lethal, are gradually forged in the reality that We live, collapsing in many cases critical infrastructures of states, rendering said services useless to residents in addition to impacting the personal data of millions in exchange for a reward, we are talking about Ransomware.

It's worth noting that technology also offers solutions that, accompanied by protocols such as OSWAP, added to Ethical Hacking techniques and tools such as SIEM, make it possible to minimize the possible attack vectors towards a certain business infrastructure, whether public or private, to minimize the impact of cyberattacks that are mitigated through good professional practices in the field of cybersecurity, which is why the correct use of all technological facilities, added to adequate advice, constant training for those involved, are essential factors when speaking cybersecurity.

ÍNDICE

TABLA DE ILUSTRACIONES

CAPÍTULO I GENERALIDADES.

1.1 Introducción

En la actualidad la ciberseguridad se ha convertido en un causal de importancia y análisis en la era del internet, considerando las amenazas constantes especialmente de software maligno, como el ransomware, generando preocupación a todo tipo de empresas, personas particulares e instituciones. El propósito fundamental del presente trabajo, es tomar el problema del ransomware a través de una visión integral, para ello usando herramientas especializadas como las SIEM y los principios del hacking ético, buscaremos que el SIEM muestre los eventos preventivos a un futuro incidente de ciberseguridad.

El panorama actual muestra que las amenazas de ciberseguridad, están evolucionando continuamente, mientras se encuentra soluciones a vulnerabilidades generales y conocidas, los ciberdelincuentes ya están explotando una nueva vulnerabilidad desconocida para los especialistas en seguridad cibernética, tal es así, que es vital comprender y combatir eficazmente el ransomware en todas sus variables para evitar comprometer la información crítica.

Se justifica este estudio considerando el incremento ataques de ransomware a nivel mundial y especialmente en el Ecuador que a la fecha actual de este documento ocupa el número 30 a nivel mundial en ataques informáticos. (Kaspersky, 2024) Este estudio no solo contribuirá en aumentar el conocimiento en el campo del ransomware, sino que ofrecerá una idea global sobre las herramientas afines a fortalecer las seguridades ante un ataque de ransomware.

El principal problema que tendrá el proyecto será identificar los patrones del ransomware, realizar la aplicación de técnicas de detección y respuesta a través del SIEM,

el uso de técnicas de hacking ético para fortalecer y evaluar las seguridades. Entre los sub problemas que se esperan, son los permisos para realizar las pruebas, evaluar vulnerabilidades específicas, optimización de políticas y obtención de muestras de ransomware.

Las variables clave de este estudio incluyen: variable independiente, si la eficacia de las herramientas SIEM permiten una detección de los ataques. En variables dependientes tenemos: la ausencia de patrones o modelos de ransomware y mejora de la seguridad a través del hacking ético.

El proyecto se limita a la generación de un análisis de vulnerabilidades ante el ataque de un ransomware específico a una empresa privada, con conclusiones relacionadas a la posible detección/no detección a tiempo del ataque por medio de herramientas SIEM. Se enfocará en un conjunto definido de herramientas y metodologías que proporcionen un análisis detallado del tema.

1.2 Tema del Proyecto.

"Análisis de un Ransomware con SIEM y Hacking Ético, para la empresa SoftwareSystem GC."

El proyecto se aplicará en el ámbito de la ciberseguridad, con un enfoque específico en la tecnología SIEM (Sistema de Información y Gestión de Eventos de Seguridad) y en las prácticas de Hacking Ético, analizando el comportamiento de este con un ransomware. Estas tecnologías serán implementadas en entornos informáticos controlados, abordando las amenazas de ransomware que pueden afectar a sistemas operativos, redes y aplicaciones.

1.3 Revisión de Literatura y Definición del Problema

El tema del proyecto de maestría está direccionada a un área de estudio que, hasta donde se ha podido verificar, no ha sido explorado en profundidad. Esto asegura que no estamos "reinventando la rueda", sino que se está abordando un problema específico y relevante en el campo de la ciberseguridad. La investigación realizada en bases de datos científicos como Google Scholar, IEEE y demás, indican que, si bien hay publicaciones científicas relacionas al tema de SIEM, no tenemos exactamente un artículo que muestre el tema propuesto como una posible publicación creada, por ello se propone el tema antes descrito.

Se ha revisado algunos documentos científicos encontrados en el repositorio de la UIDE muy útiles que se convierten en un gran soporte para definir y contribuir con información valiosa a algunos de los temas que podemos usarlos como sustento en este proyecto de maestría, y son los siguientes:

- Elaboración de 5 Casos de Uso para Plataforma SIEM Institucional en el Sector Financiero a ser implementado por la empresa de Seguridad Informática Secure Soft (Agudelo Castro Bryan Adrián, 2022)
- Propuesta de implementación de SIEM en un centro de capacitación, con tres casos de usos, utilizando Mitre attack (Gómez Prado Sandra Patricia, 2023)
- Implementación de un SIEM para la identificación de posibles ciberataques en la empresa Torres & Torres (Acuña Paredes Yesenia de las Mercedes, 2022)
- Implementación de un SIEM en el área de TI para identificar y centralizar posibles eventos en la infraestructura critica de la industria gráfica. (Patiño Rosero Wilson Steven, 2023).

- Agradecemos a los pioneros en el campo de la ciberseguridad, cuyos esfuerzos han sentado las bases para el proyecto. Sus investigaciones han sido fundamentales para la comprensión del problema que pretendemos resolver: cómo fortalecer la ciberseguridad mediante el análisis de un ransomware con SIEM y hacking ético.

El estudio se basa en una comprensión sólida de los problemas teóricos e investigativos relacionados con la pregunta de investigación. Se ha revisado y evaluado la literatura existente para asegurar de que estamos bien informados sobre las últimas investigaciones y desarrollos en este campo.

La habilidad para integrar y sintetizar la literatura existente permite desarrollar un marco conceptual sólido para la investigación. Este marco guiará a lo largo del proyecto y ayudará a mantener un enfoque claro.

Finalmente, la investigación ofrece nuevas perspectivas teóricas en el campo de la ciberseguridad. A través del análisis de un ransomware con SIEM, se pretende desarrollar un documento que pueda ser utilizado para fortalecer la ciberseguridad en el futuro. Este documento no sólo contribuirá a la literatura existente, sino que también tendrá implicaciones prácticas para la protección de los sistemas informáticos contra las amenazas de ransomware.

1.4 Justificación del Proyecto

Este proyecto tiene el objetivo de presentar las diferentes etapas que abarca el proceso de ataque de un Ransomware que puede afectar a una PYME, esto se debe a que en la actualidad los ataques con Ransomware son efectuados con más frecuencia, dichos ataques los realizan a diferentes empresas ya sean públicas o privadas. Estos ataques basados en ransomware cada día son más sofisticados, ya que se enfocan en atacar áreas específicas convirtiéndose en una amenaza a su competitividad. Así como existen ataques basados en ransomware existen las tecnologías SIEM las cuales permiten mitigar o salvaguardar la integridad de la empresa SoftwareSystem GC. Este proyecto constará de varias metodologías: De campo, documental-bibliográfica, utilizando las tecnologías SIEM.

Cabe mencionar que los ciberataques se catalogan como un problema para la sociedad porque aumenta el riesgo de pérdida y/o adulteración de la información sensible y la privacidad de países o naciones, personas naturales y jurídicas, por eso las tecnologías SIEM han tenido un impacto favorable ante estas amenazas, ya que son herramientas diseñadas para visibilidad, análisis y respuesta ante incidentes enfocados en la seguridad de entornos informáticos.

1.5 Alcance del Proyecto

Realizar un análisis la implantación e implementación de un SIEM en la empresa SoftwareSystem GC para ver su comportamiento en la infraestructura de la organización, se utilizarán además técnicas de hacking ético y un malware tipo ransomware de manera controlada, para exponer las bondades y efectividad del SIEM.

1.6 Objetivos del Proyecto

General

Implantar la tecnología SIEM, utilizando de manera controlada un ransomware, para detectar de manera prematura, posibles amenazas donde las técnicas de hacking ético determinarán las vulnerabilidades de la infraestructura objeto de estudio.

Específicos

- Analizar el comportamiento del SIEM dentro de la infraestructura de la empresa.
- Crear un ambiente de pruebas para realizar un ataque usando un ransomware desarrollado por nosotros y verificar las bondades del SIEM.
- Establecer mecanismos de prevención mediante la identificación proactiva de amenazas para mitigar el riesgo de ataques de ransomware usando tecnologías SIEM y técnicas de hacking ético

CAPÍTULO II METODOLOGÍA DE LA INVESTIGACIÓN.

2.1 Metodología de la Investigación

Este informe se llevará a cabo siguiendo una metodología mixta que combinará aspectos cualitativos y cuantitativos. En primera instancia, se realizará un análisis y revisión exhaustiva de la información existente sobre ransomware, Security Information and Event Management (SIEM) y prácticas éticas de hacking. Este paso permitirá establecer una base teórica sólida para comprender las características, impacto y métodos de detección y respuesta frente al ransomware, utilizando los siguientes enfoques.

Enfoque Cuantitativo: Se implementará la recolección de datos de casos y eventos de seguridad mediante el uso de SIEM en la infraestructura de determinada empresa, se simularán escenarios de ataques de ransomware para evaluar la efectividad de las herramientas SIEM en la detección temprana, la notificación de eventos sospechosos y las respuestas automatizadas ante posibles incidentes.

Enfoque Cualitativo: Analizando los datos de los eventos de seguridad recopilados por SIEM, registro de casos y patrones de ataques de ransomware centrándose en estudios de casos reales, para comprender la metodología de los ataques, las vulnerabilidades explotadas y las estrategias de recuperación utilizadas. Además, se llevarán a cabo pruebas de penetración ética en una empresa para evaluar la resistencia de los sistemas ante distintos escenarios de ataques de mencionado malware, sin comprometer la integridad de los datos ni la infraestructura.

2.1.1 INVESTIGACIÓN DOCUMENTAL-BIBLIOGRÁFICA.

El empleo de la modalidad de investigación documental- bibliográfica es fundamental en este proyecto de investigación, ya que nos permitirá recopilar, analizar y sintetizar información relevante y existente sobre el uso de ransomware, métodos

utilizados para estos ataques cibernéticos y los efectos que estos poseen en la infraestructura de una empresa así como las soluciones que se emplearon en esos casos por lo cual el conocimiento acumulado previamente por otros investigadores y expertos serán de gran ayuda.

2.1.2 INVESTIGACIÓN EXPERIMENTAL

La investigación experimental puede proporcionar datos valiosos y resultados concretos sobre la efectividad de las herramientas a utilizar en este proyecto por, siendo así que por medio de la ayuda de simulación de ataques controlados, y empleo de enfoques de auditoría de seguridad para evaluar la robustez de los sistemas ante ataques de ransomware nos proporcionará la suficiente información para la realización de planes de respuesta mediante SIEM para mitigar estos ataque en un futuro en las infraestructuras cibernéticas de las empresas.

2.2 Consideraciones Éticas, Sociales, Legales, Profesionales y de Seguridad.

Para realizar este proyecto, ha sido vital contar con el apoyo del principal de la Empresa SoftwareSystem GC, quien gentilmente ha accedido a otorgar el apoyo y el consentimiento para la realización de todas y cada una de las actividades previstas, considerando que el ransomware además de bloquear el acceso a los datos de los clientes, genera una serie de complicaciones de todo orden. La imposibilidad de acceder a los datos, los productos y servicios de la organización intrínsicamente afectan a la imagen y reputación de la organización ante sus stakeholders[4].

Como las actividades previstas se enmarcan en lo establecido en la normativa sobre ese fin, a más de realizar bajo técnicas respetadas y respetables de hacking ético, el enfoque

[4] Públicos de interés.

del proyecto se encamina a proporcionar un producto final que ayude a la organización a proveer estrategias efectivas de mitigación y respuesta para proveer en un futuro, que el impacto de los ataques de malware sean el menor posible, apoyando de esta manera a la continuidad al negocio.

CAPÍTULO III RESULTADOS Y ANÁLISIS

3.1 Evaluación de la efectividad de SIEM en la detección temprana de ataques de ransomware.

Para poder verificar si un SIEM es una herramienta capaz de facilitar la detección de patrones de comportamiento ante un ataque de ransomware en tiempo real, es importante instalarlo dentro de la infraestructura de la persona contratante, es por ello, que es importante y vital, contar con la autorización del representante legal de la organización como se muestra en el Apéndice "A".

En nuestro caso utilizaremos OSSIM5, una tecnología capaz de capturar los logs 6tanto de firewall como IPS, IDS o antivirus para buscar patrones que podrían alertar de un inminente ataque de uno de los malware más peligrosos y destructores como es el caso de ransomware.

No se puede considerar que el SIEM está diseñado solamente para detectar patrones de un vector de ataque específico empleando ransomware, existe una variedad de malware que pueden ser detectados por un SIEM considerando que la función primordial de este es proporcionar un lugar de almacenamiento central de esos volúmenes de datos al equipo de seguridad para establecer a través de patrones de comportamiento, un posible vector de ataque o camino en concreto por donde la estrategia del ataque va a consumarse utilizando malware o técnicas de hacking.

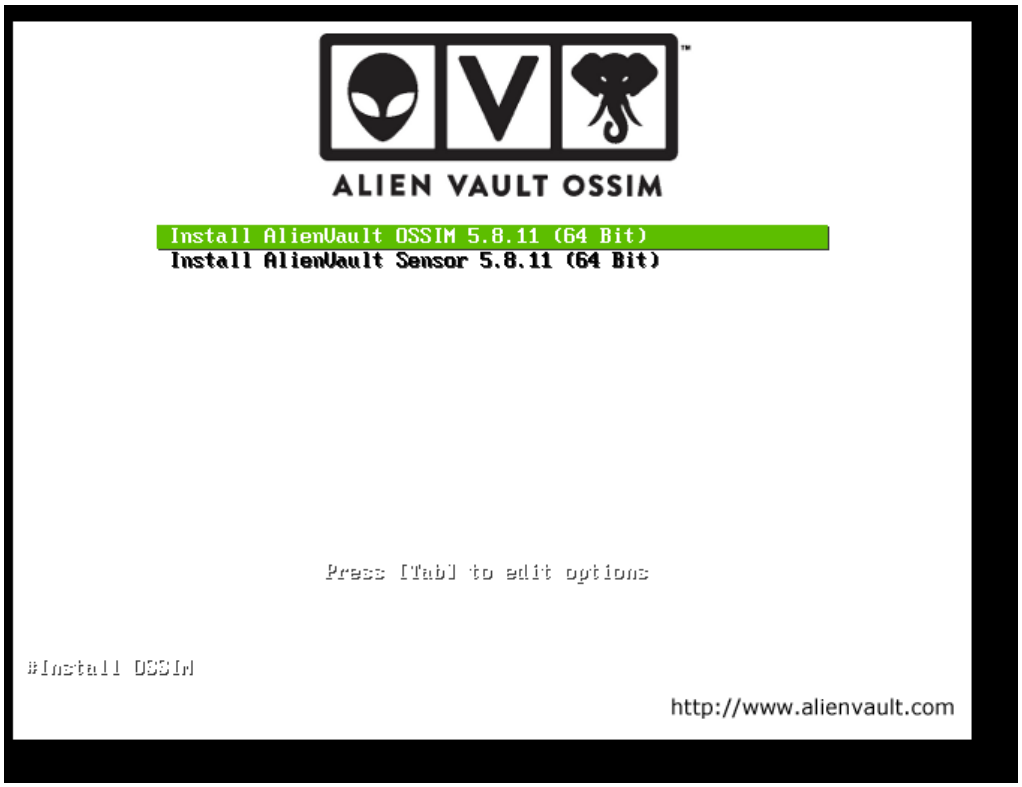
En la ilustración 1, podemos observar el inicio del proceso de instalación del SIEM OSSIM en la infraestructura del contratante.

[5] Open Source Security Information Management, herramienta para recolección de logs de todos los equipos de seguridades como IPD,IDS, firewall.

[6] Archivo de texto donde se graban cronológicamente un evento generado por un servidor o un sistema operativo.

Ilustración 1

Inicio de la instalación del SIEM OSSIM

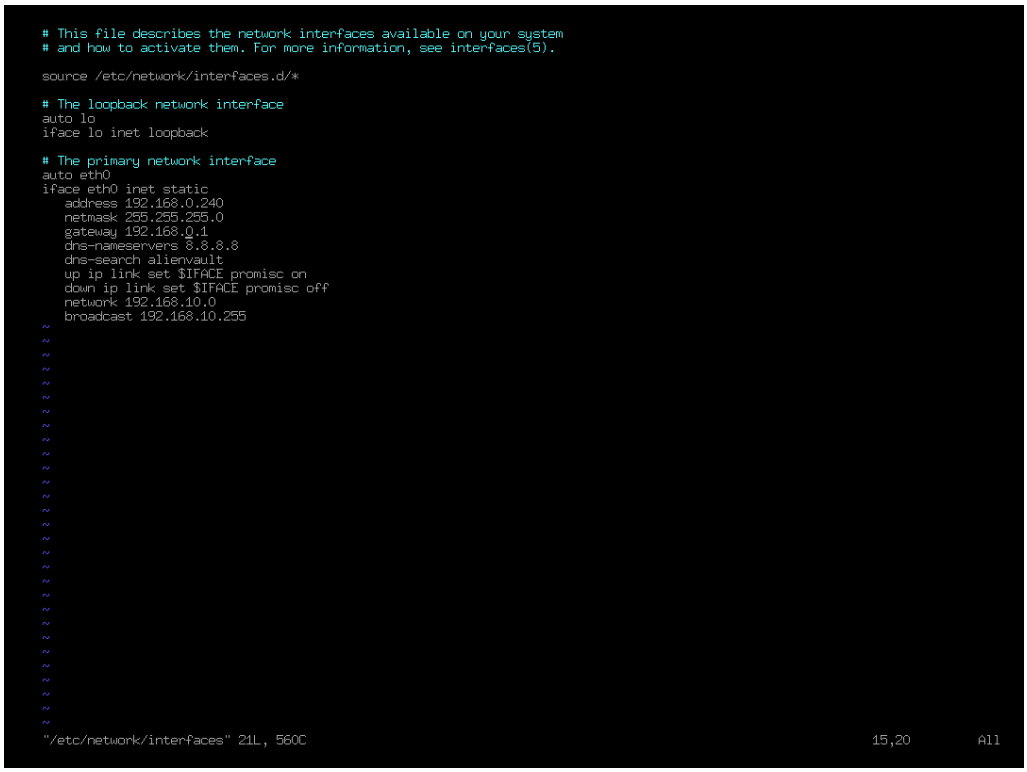


Fuente: De los autores.

Una vez configurada la IP del SIEM, procedemos como cita en la Ilustración 1 a continuar con la instalación.

Ilustración 2

Configuración IP del SIEM

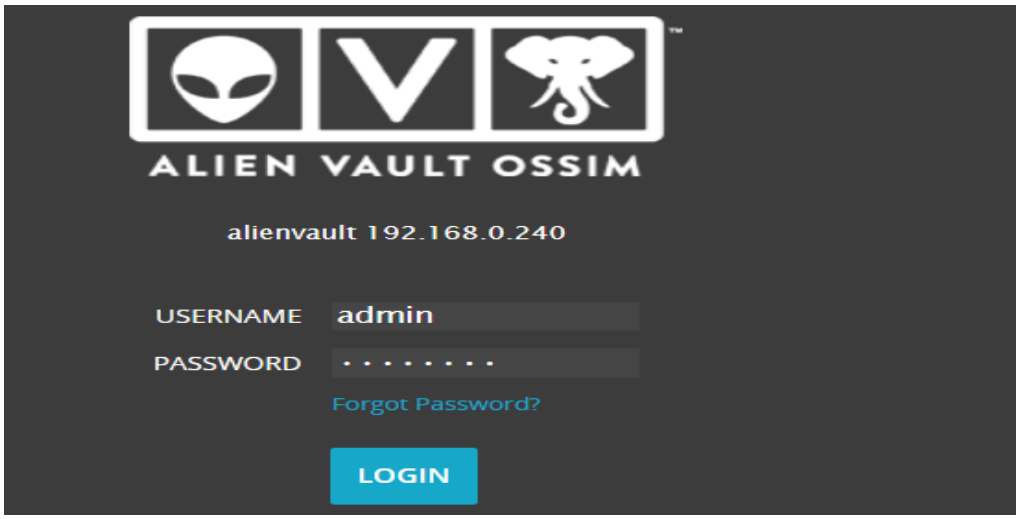


Fuente: De los autores.

Una vez finalizada la configuración de IP en el SIEM, procedemos a ingresar usuario y contraseña para iniciar con la explotación de la herramienta. (Ilustración 3)

Ilustración 3

Ingreso de un usuario y contraseña en el SIEM

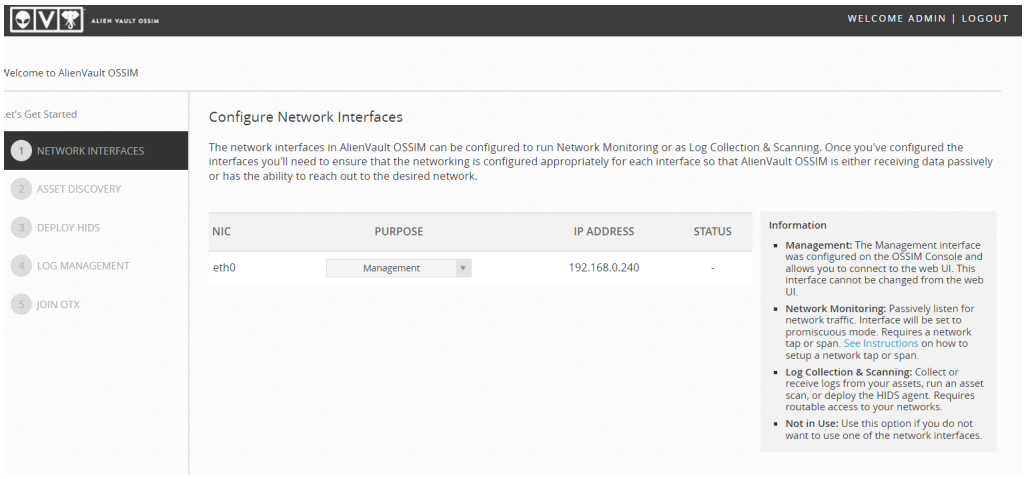


Fuente: De los autores.

Ya iniciado el asistente, el SIEM requiere escanear la red para determinar y establecer su entorno de trabajo, un elemento muy importante de esto se lo puede apreciar en la siguiente Ilustración:

Ilustración 4

SIEM configuración de las interfaces de red.

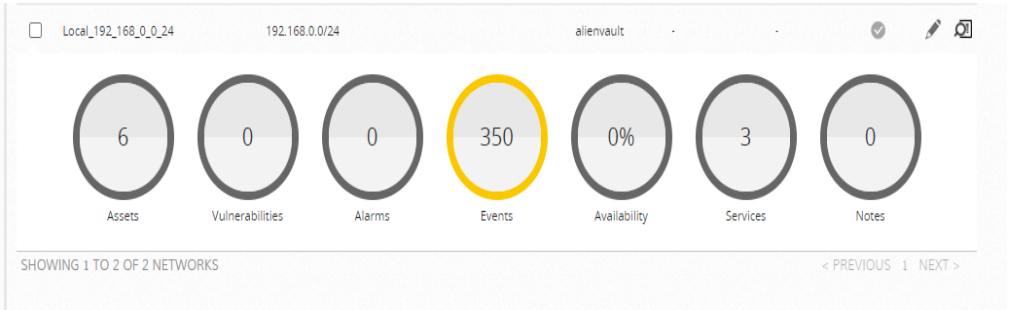


Fuente: De los autores.

Algo interesante de destacar que a medida que la instalación del SIEM va progresando, se puede observar que esta tecnología comienza a capturar de a poco, los logs de los eventos de la red local 192.168.0.1-255 como se observa en la imagen adjunta (Ilustración5).

Ilustración 5

Captura de logs con el SIEM, mientras se configura en LAN

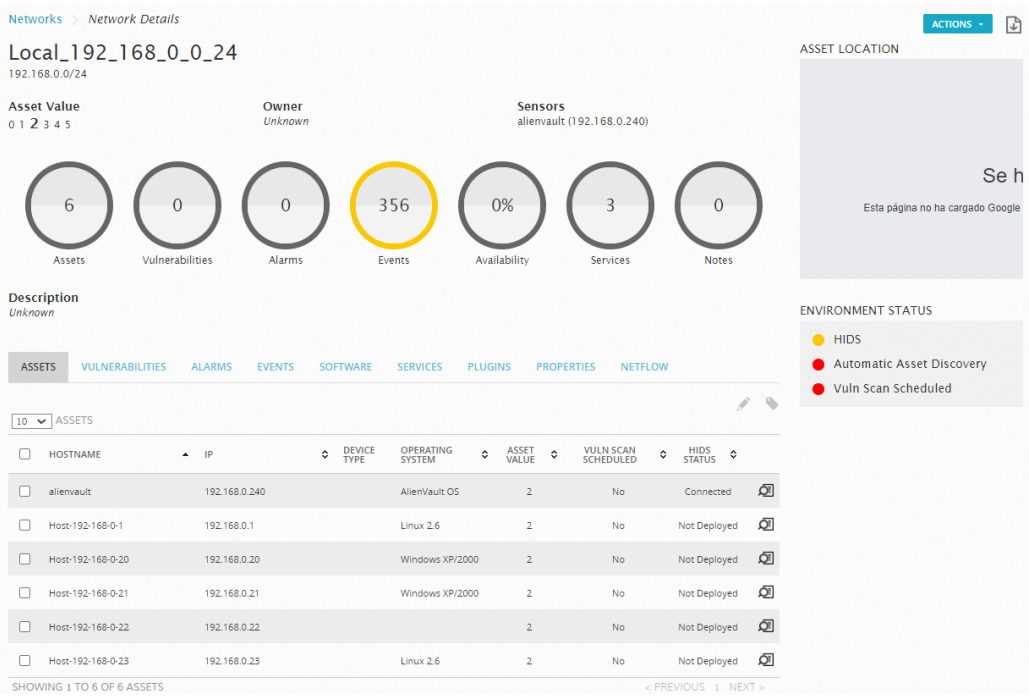


Fuente: De los autores.

En la parte superior izquierda tenemos una lupa, al presionar se obtiene mayores detalles de lo que el SIEM está capturando, donde se puede destacar, que esta tecnología termina siendo una alternativa eficaz para en ese gran volumen de información, lograr detectar patrones que permitan al equipo que administra el SIEM que en un futuro podría ser un SOC, tener una idea de las probabilidades de vectores de ataque en función del comportamiento de las detecciones de los logs, es por ello la importancia de contar con un SIEM en la organización, configurarlo adecuadamente y sobre todo monitorearlo de manera constante para hacer más efectiva y eficiente el trabajo de la Ciberseguridad, tal es así, que en la ilustración posterior a este párrafo, podemos observar lo antes señalado.

Ilustración 6

SIEM comienza a detectar eventos

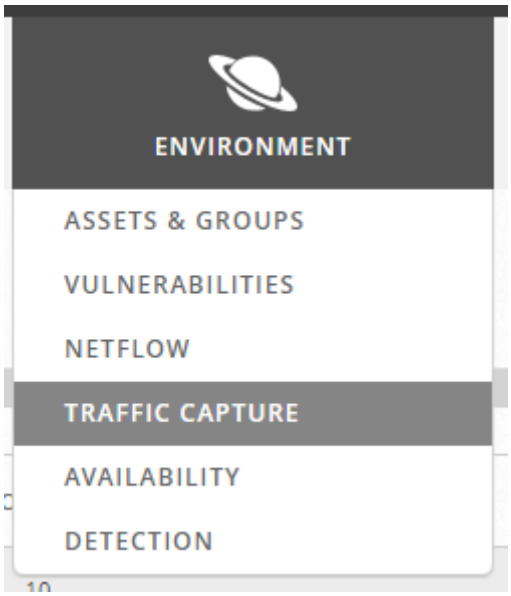


Fuente: De los autores.

Una vez configurado, procedemos a realizar capturas parametrizadas para ello recurrimos al siguiente menú propio del SIEM para iniciar con este requerimiento:

Ilustración 7

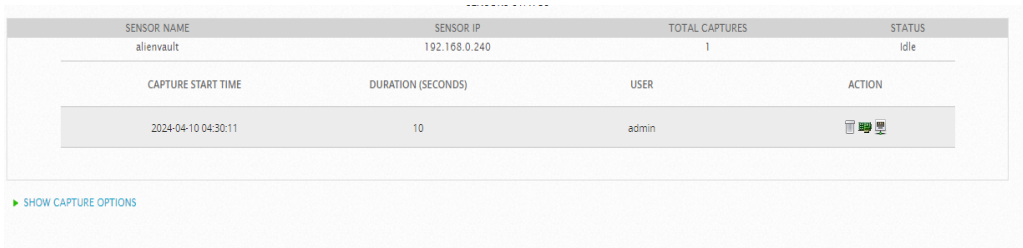
Captura de tráfico.



Fuente: De los autores.

Ilustración 8

Activamos la acción de captura.

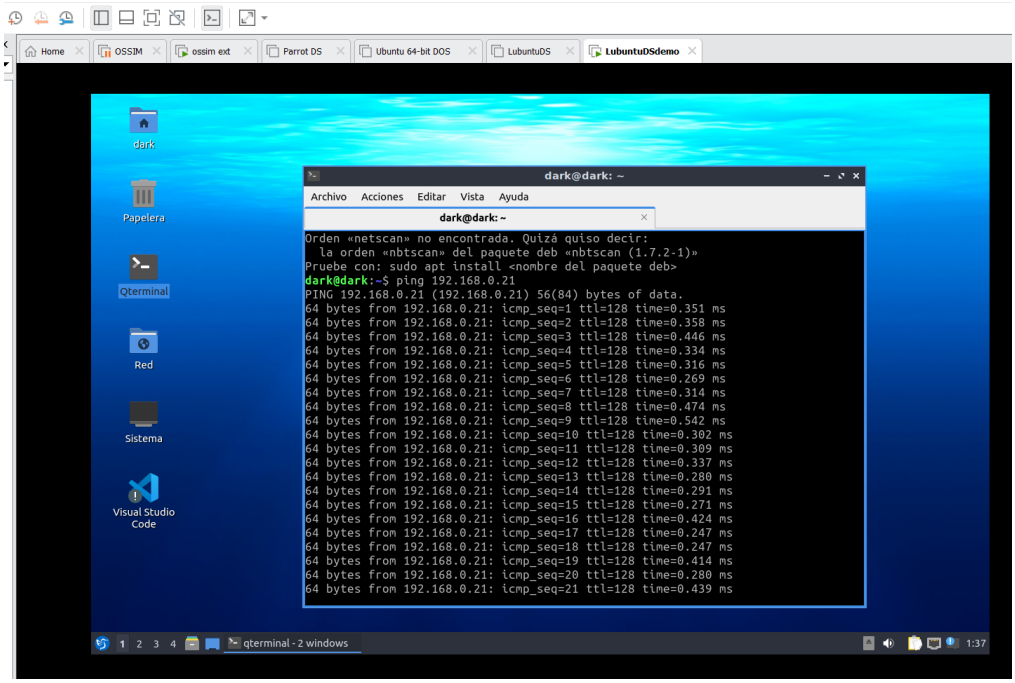


Fuente: De los autores.Nota: Una vez revisado las propiedades y los activos, iniciamos la captura dando click en el payload en la parte derecha de la imagen.

Es muy importante darnos cuenta que apenas realizamos una acción, el SIEM comienza a capturar tráfico y se logra identificar una actividad sospechosa por un ping generado por nosotros.

Ilustración 9

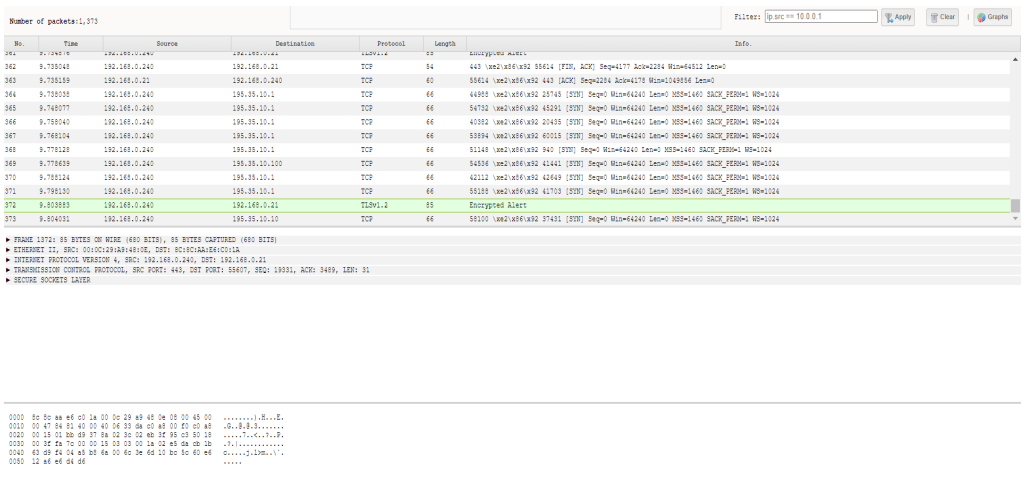
Ping generado para capturar la acción.



Fuente: De los autores.

Ilustración 10

Detección del ping IP 192.168.0.21



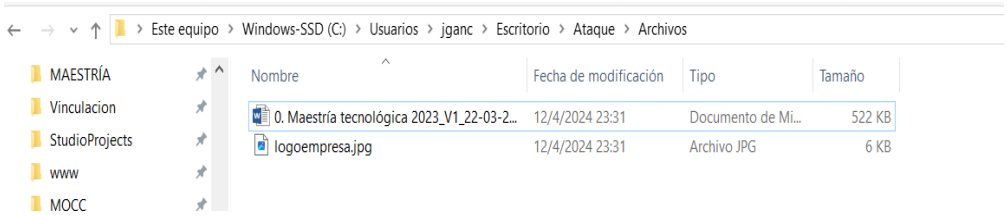
Fuente: De los autores. Nota: En la línea 372 se puede comprobar el ping de la IP 192.168.0.21.

Una vez hecha la prueba que el SIEM está detectando, iniciamos las pruebas con el ransomware desarrollado por nuestro grupo, donde básicamente usaremos 2 librerías, la principal es cryptography, que nos servirá para encriptar y desencriptar los archivos y la siguiente para acceder al sistema operativo.

Como es un entorno de pruebas, vamos a crear una estructura de archivos bien definida en el desktop de Windows llamada Ataque, y dentro de ésta otra carpeta llamada Archivos. A su vez pondremos varios archivos en esta carpeta que serán encriptados, es aquí donde creamos las carpetas para encriptar y desencriptar, es decir usamos un ransomware creado por nosotros, para reducir el impacto y no causar daños en la infraestructura.

Ilustración 11

Creación carpetas de encriptado y des encriptado



Fuente: De los autores.

Dentro de los acuerdos que se realizaron con el Gerente General de la empresa que está auspiciando este proyecto, se acordó que los trabajos a realizar sobre la infraestructura, deben generar el menor impacto sobre esta, considerando que se va a utilizar un ransomware, es decir que para el grupo, la prioridad número uno era probar las debilidades de la infraestructura pero sin afectar a la funcionalidad de la misma, es por ello, que haciendo honor al acuerdo, se decidió generar un ransomware de impacto cero, para mostrar las ventajas de usar un SIEM cuando se producen ataques reales, aun cuando

este estaba encaminado solamente a la detección y no a generar un secuestro de la información contenida en esa infraestructura.

Para comprender mejor nuestro accionar, mostramos a continuación parte del código fuente del ransomware creado por el grupo dos.

Ilustración 12

Código fuente del Ransomware.

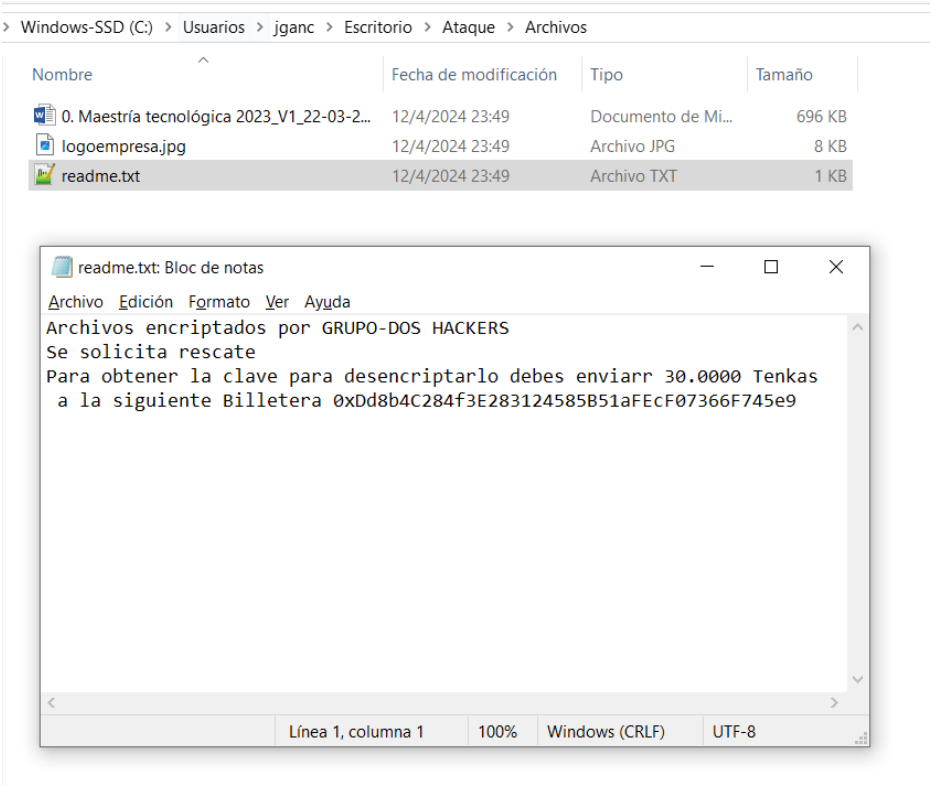
```
from cryptography.fernet import Fernet
import os

def generateKey():
    key = Fernet.generate_key()
    with open("key.key","wb") as key_file:
        key_file.write(key)

def retornarkey():
    return open("key.key","rb").read()

def encryp(items, key):
    i = Fernet(key)
    for x in items:
        with open(x, "rb") as file:
            file_data = file.read()
        data = i.encrypt(file_data)

        with open(x,"wb") as file:
            file.write(data)

if __name__ == "__main__":

    archivos = 'C:\\Users\\jganc\\Desktop\\Ataque\\Archivos'
    items = os.listdir(archivos)
    archivos_2 = [archivos + "\\" + x for x in items ]

generateKey()
key  = retornarkey()

encryp(archivos_2,key)

with open(archivos+"\\"+"readme.txt","w") as file:
    file.write ("Archivos encriptados por GRUPO-DOS HACKERS")
    file.write ("\nSe solicita rescate")
    file.write ("\nPara obtener la clave para desencriptarlo debes enviar 30.0000 Tenkas")
    file.write ("\n a la siguiente Billetera 0xDd8b4C284f3E283124585B51aFEcF07366F745e9")
```

Fuente: De los autores. Nota: El momento que se ejecuta el archivo “readme.txt”, el ransomware inicia su ataque.

En la siguiente ilustración, podemos apreciar el archivo readme.txt que ejecuta el ransomware.

Ilustración 13

Archivo readme. txt con ransomware

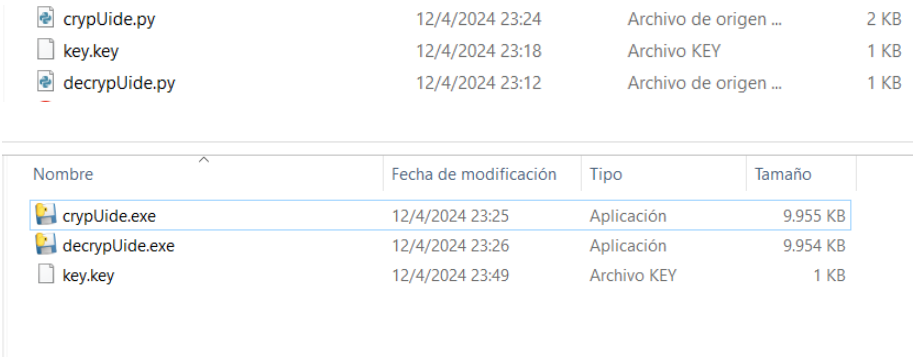


Fuente: De los autores.

Es importante destacar que el archivo original se llama crypUide.py, pero usamos una librería llama Pyinstaller, esta permite generar un archivo .exe para que se ejecute en cualquier sistema Windows (Ilustración 14):

Ilustración 14

Archivos para comprimir y descomprimir los datos



Fuente: De los autores. Nota: Se dos ejecutables creados en Python, uno para encriptar los archivos crypUide.py, y otro para desencriptarlos *descrypUide.py*.

Hechas las pruebas a continuación vamos a ejecutarlos en una máquina virtual con Windows 10, que esta monitorizada por el SIEM AlienVault OSSIM, con esto hemos constatado la funcionalidad del SIEM, por lo que procedemos a establecer y organizar las estrategias de respuesta de incidentes.

3.2 Desarrollo de estrategias de respuesta a incidentes de ransomware utilizando SIEM y técnicas de hacking ético**:**

Como primer punto indicaremos porque es necesario que las organizaciones cuenten con un SIEM para poder prestar una solución, debido a que los ciberataques ya no son algo raro o desconocidos se los puede catalogar hoy en día como algo cotidiano es importante contar con un SIEM con el fin de que cumplan un papel en específico detectando de manera proactiva, las diferentes amenazas de seguridad, una solución efectiva es implantar un monitoreo constante para ver el cambio en la infraestructura de TI, dichas alertas en tiempo real permiten que los analistas de seguridad puedan identificar anomalías para posteriormente proceder a bloquear dichas vulnerabilidades.

Es importante mencionar que actualmente las PYMES optan por el mayor uso de la tecnología. Debido a ello va en aumento es uso de datos que se van generando en la misma se incremente de manera exponencial, debido a dicho crecimiento va a necesitar más sistemas interconectados entre si lo que ocasionaría que se encuentren expuestos, esto va a dar vía libre para que los atacantes corrompan dichos sistemas con mayor facilidad debido a que si no cuentan con un sistema de monitoreo con SIEM puede pasar desapercibido dichos ataques, los cibercriminales aprovechan estos ataques conjuntamente con la ciberseguridad ya que se ha convertido en un negocio liderado por las organizaciones criminales que buscan sustraer cualquier tipo de información para luego reclamar un pago excesivamente alto para la liberación de dicha data que pudieron obtener en el ataque. De este escenario surge la necesidad de centralizar todos estos logs generados por los sistemas con la finalidad de gestionarlos de forma eficiente y aplicar sobre las mismas acciones correctivas que ayuden a un futuro a detectar posibles incidentes de seguridad.

A continuación, se detallará varias ventajas que tiene un SIEM para poder monitorear un ataque de ransomware:

1. Proactividad relacionada con los incidentes de seguridad.
2. Rapidez de respuesta ante incidentes detectados
3. Detección de amenazas previamente desconocidas. Esto se puede lograr el uso de analítica avanzada de eventos.
4. Mayor velocidad a la hora de llevar a cabo la investigación de alertas generadas.
5. Posibilidad de detectar amenazas en logs históricos.
6. Monitorización de las actividades que se lleven a cabo dentro de la red, esto contempla la actividad de los usuarios y dispositivos administrados.
7. Garantiza la protección de los datos.

Evaluación de vulnerabilidades, es decir identificar las vulnerabilidades en los sistemas administrados, realizar pruebas de vulnerabilidades a nivel de red y monitoriza de manera continua para la detección de nuevas amenazas.

Cuando se realiza la instalación de un SIEM debemos considerar diferentes aspectos claves los cuales nos permitirán realizar dicho proceso de manera correcta, entre los puntos que debemos considerar están los siguientes puntos:

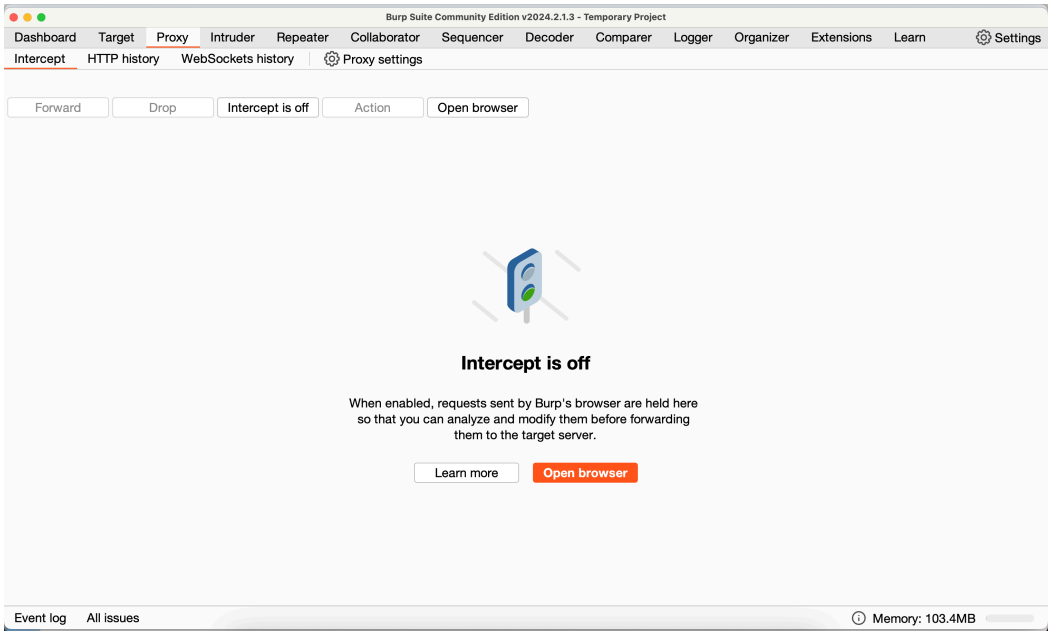
1. Selección de un SIEM adecuado
2. Monitoreo continuo
3. Capacitación y concientización
4. Hacking ético y evaluaciones de vulnerabilidades
5. Respuesta a incidentes
6. Backup y recuperación de información
7. Actualizaciones y parches.

Una de las estrategias sugeridas a la empresa auspiciante de este estudio, fue que los usuarios que se logean para ingresar a la empresa por vía web, deben ser de tipo correo electrónica y no un usuario común solamente, esto con el fin de elevar el grado de dificultad de acceso cuando se utiliza el ataque de fuerza bruta, tomando en cuenta que este tipo de ataque, para cumplir su cometido, requiere de un diccionario de datos con las posibles opciones que podrían dar con el usuario correcto y al incluir dominios de correo al usuario, se busca complicar la consecución del ataque con ese doble factor de búsqueda considerando el número mayor de caracteres, toda vez, que al existir millones de dominios de correo y millones de nombres de usuario, el trabajo para el atacante se complica notablemente.

Una vez analizada y aceptada por la empresa nuestra sugerencia y utilizando la herramienta Burp Suite, comenzamos a comprobar que nuestra teoría y asesoramiento comiencen a dar resultados:

Ilustración 15

Uso de Burp Suite para verificar fuerza bruta

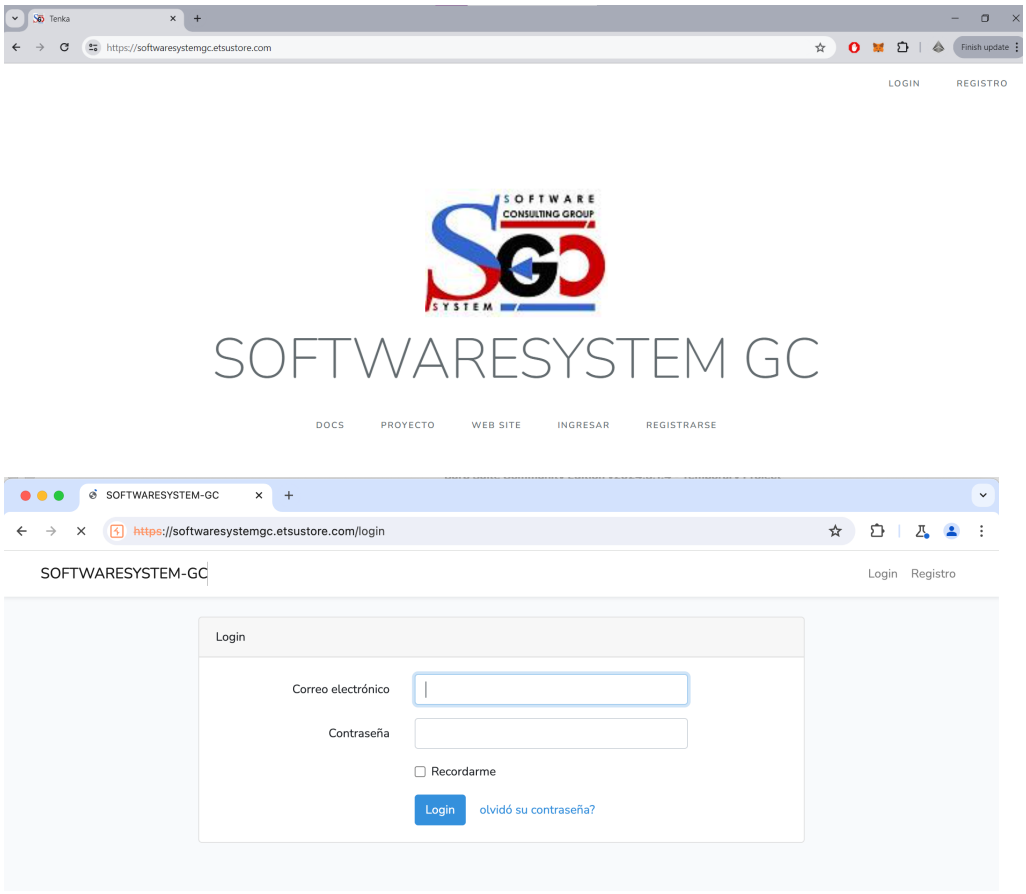


Fuente: De los autores.

Una vez abierta la aplicación, iniciamos el procedimiento para lanzar el ataque de fuerza bruta, para ello abrimos el navegador de Burp Suite y en el browser ingresamos la URL de la Empresa auspiciante:

Ilustración 16

Inicio del ataque de fuerza bruta

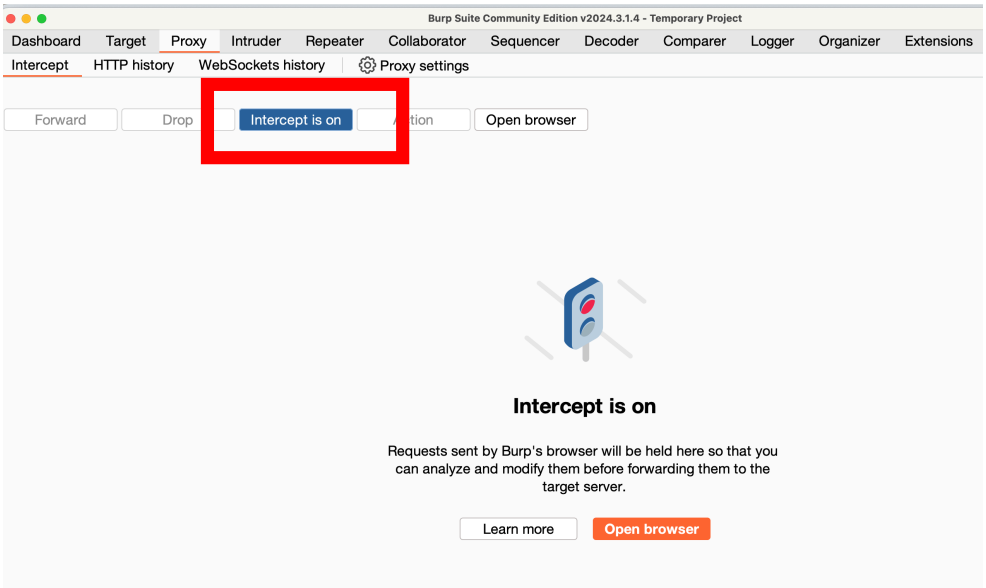


Fuente: De los autores.

Posterior regresamos a la interface de Burp Suite y encendemos el interceptor para iniciar el proceso de ataque por fuerza bruta.

Ilustración 17

Encendido del intereceptor en Burp Suite

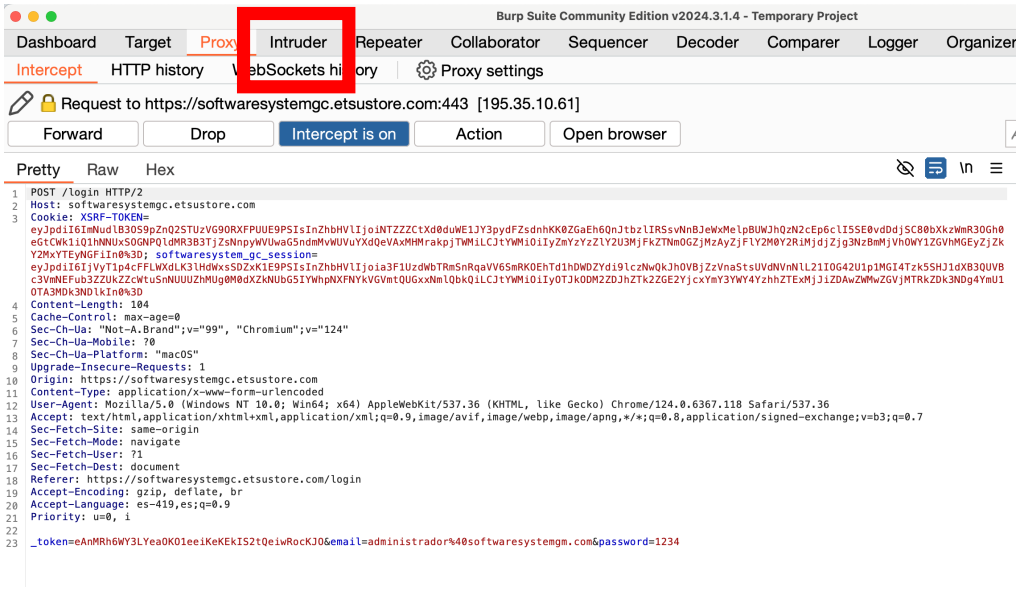


Fuente: De los autores.

Ya con el Intercept encendido como se muestra en la Ilustración 17, regresamos al navegador de Burp Suite y comenzamos a ingresar usuario y contraseña más probable para intentar logearnos de manera normal y que la herramienta capture esa acción para buscar con el diccionario y determinar si logramos alcanzar el cometido.

Ilustración 18

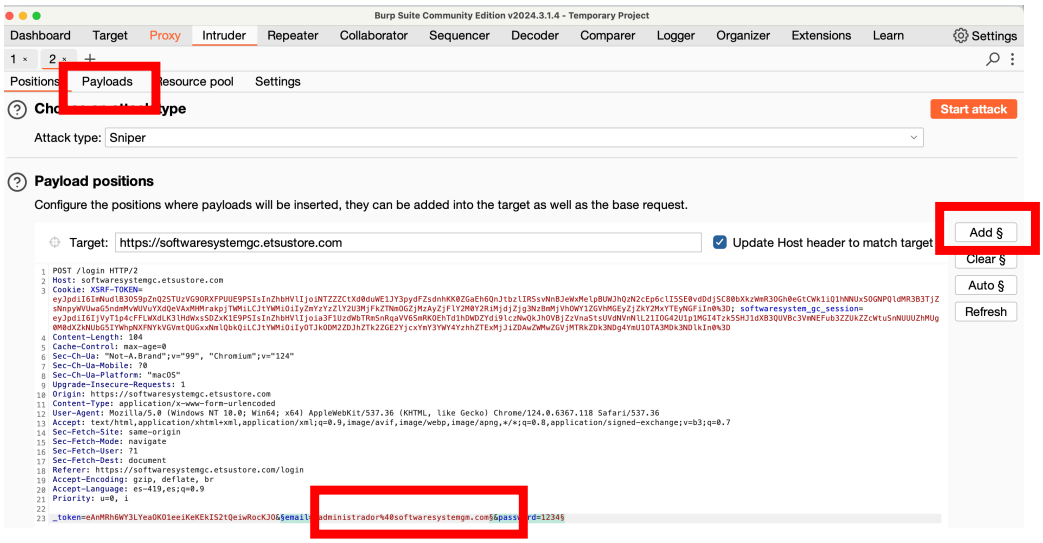
Captura de datos con Burp Suite



Como se muestra en la Ilustración 18, una vez interceptado los datos, comenzamos con el proceso de buscar el o los posibles usuarios para acceder limpiamente a la web de la víctima, para ello elegimos la función *Intruder*, luego seleccionamos en la parte inferior el usuario ingresado y activamos la búsqueda con el botón Add, quedando el usuario activado con un carácter propio de la herramienta § visualizada en la imagen que se muestra a continuación

Ilustración 19

Selección de usuario con botón Add



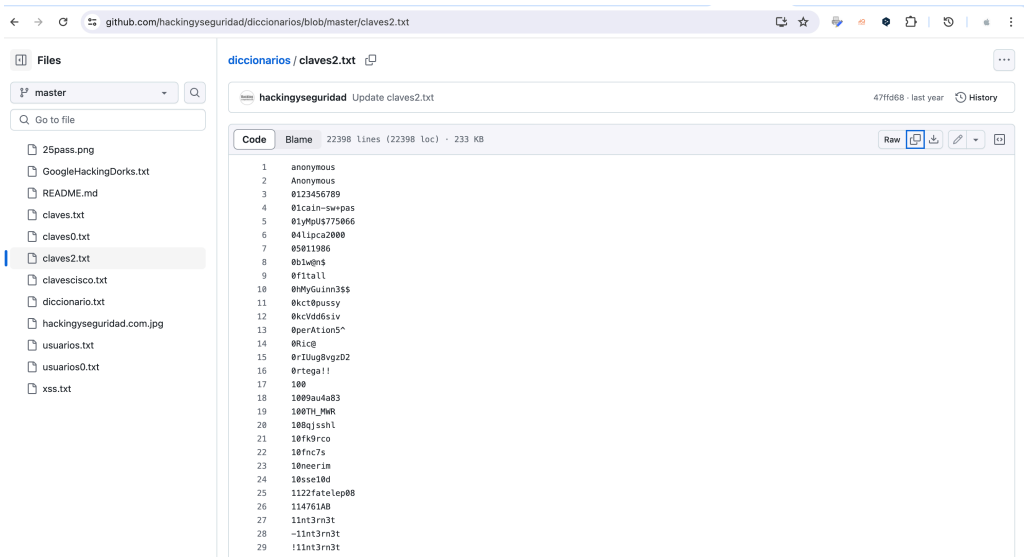
Fuente: De los autores.

Posterior a esto, elegimos la función *Payloads,* cuyo objetivo es ingresar el diccionario requerido para el ataque de fuerza bruta (Ilustración 19).

Para acceder al diccionario de claves, nos apoyamos en repositorios de Github y donde se puede descargar diccionarios de posibles claves como se muestra en la siguiente ilustración, de ahí copiamos el diccionario y pegamos en Burp Suite.

Ilustración 19

Captura de usuarios en github

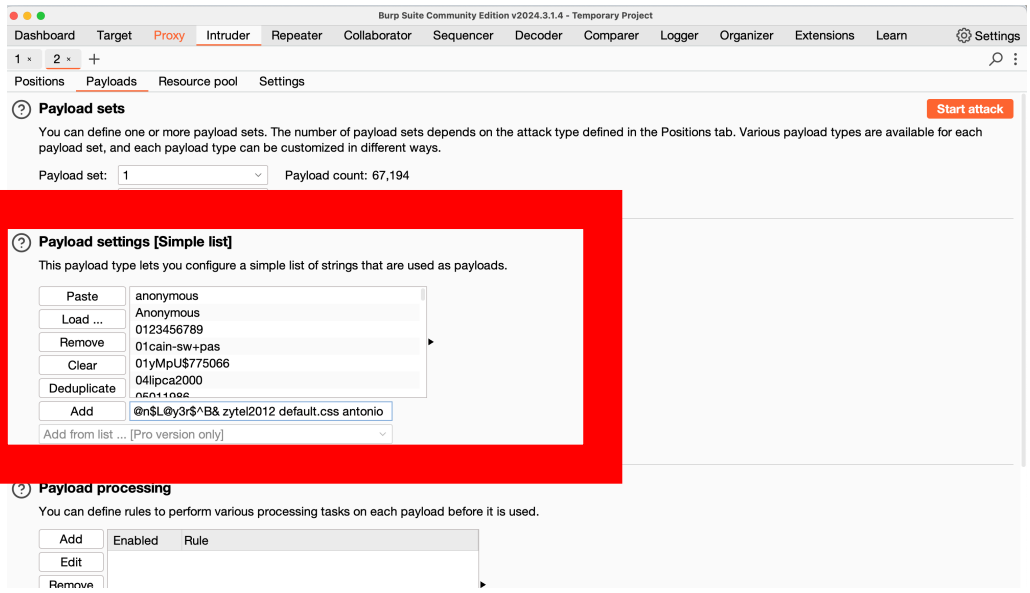


Fuente: De los autores.

Una vez copiados en este caso más de 23000 posibles usuarios, pegamos en ***Payload settings [Siemple list]*** el diccionario donde la herramienta Burp Suite, comenzará a comparar el usuario real con uno a uno de ese diccionario, realizando así el ataque de fuerza bruta como se muestra en la siguiente ilustración.

Ilustración 20

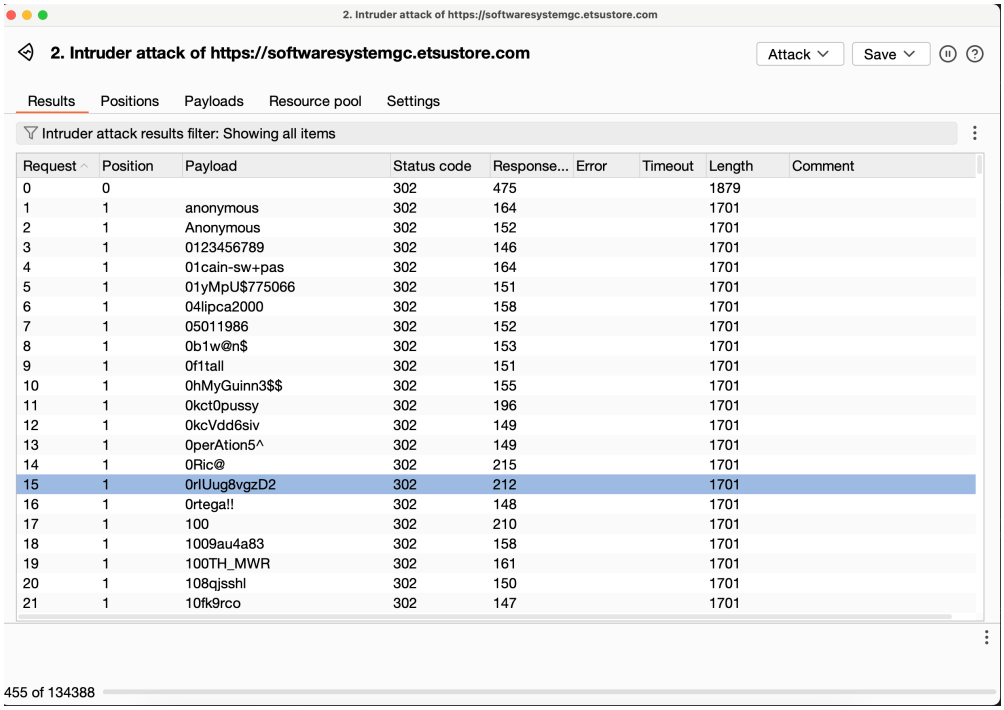
Cargamos el diccionario con más de 23000 opciones de usuario posible



Ya subida la información de claves, se realiza el ataque dando clic en la opción Start attack y esperamos a que la herramienta Burp Suite inicie la comparación del usuario real con los más de 23000 opciones cargadas en el diccionario.

Ilustración 21

Resultado ataque fuerza bruta



Request	Position	Payload	Status code	Response...	Error	Timeout	Length	Comment
0	0		302	475			1879	
1	1	anonymous	302	164			1701	
2	1	Anonymous	302	152			1701	
3	1	0123456789	302	146			1701	
4	1	01cain-sw+pas	302	164			1701	
5	1	01yMpU$775066	302	151			1701	
6	1	04lipca2000	302	158			1701	
7	1	05011986	302	152			1701	
8	1	0b1w@n$	302	153			1701	
9	1	0f1tall	302	151			1701	
10	1	0hMyGuinn3$$	302	155			1701	
11	1	0kct0pussy	302	196			1701	
12	1	0kcVdd6siv	302	149			1701	
13	1	0perAtion5^	302	149			1701	
14	1	0Ric@	302	215			1701	
15	1	0rlUug8vgzD2	302	212			1701	
16	1	0rtega!!	302	148			1701	
17	1	100	302	210			1701	
18	1	1009au4a83	302	158			1701	
19	1	100TH_MWR	302	161			1701	
20	1	108qjsshl	302	150			1701	
21	1	10fk9rco	302	147			1701	

Fuente: De los autores.

En los ataques de fuerza bruta, si fueron detectados como se muestra en las siguientes ilustraciones (22 y 23)

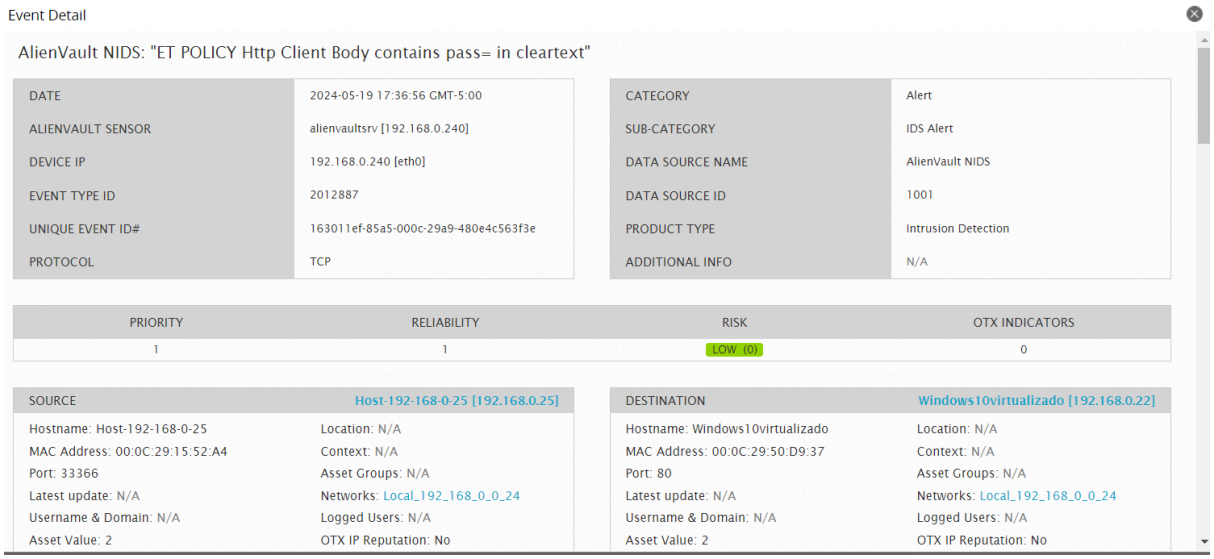
Ilustración 22

Resultado ataque fuerza bruta en SIEM Alienvault

2024-05-19 17:48:18	AlienVault NIDS: "ET SCAN Non-Allowed Host Tried to Connect to MySQL Server"	Windows10virtualizado	alienvaultsrv	alienvaultsrv	0	
2024-05-19 17:48:18	AlienVault NIDS: "ET SCAN Non-Allowed Host Tried to Connect to MySQL Server"	Windows10virtualizado	alienvaultsrv	alienvaultsrv	0	
2024-05-19 17:36:56	AlienVault NIDS: "ET POLICY Http Client Body contains pass= in cleartext"	Host-192-168-0-25	Windows10virtualizado	alienvaultsrv	0	
2024-05-19 17:33:24	AlienVault NIDS: "ET POLICY Http Client Body contains pwd= in cleartext"	Host-192-168-0-25	Windows10virtualizado	alienvaultsrv	0	
2024-05-19 17:11:27	AlienVault NIDS: "ET INFO UPnP Discovery Search Response vulnerable UPnP device 1"	Host-192-168-0-1	Windows10virtualizado	alienvaultsrv	0	
2024-05-19 17:11:27	AlienVault NIDS: "ET INFO UPnP Discovery Search Response vulnerable UPnP device 1"	Host-192-168-0-1	Windows10virtualizado	alienvaultsrv	0	

Ilustración 23

Ataque desde IP 192.168.0.25(atacante) a 192.168.0.22 (servidor web del cliente)



Fuente: De los autores.

Posterior al ataque de fuerza bruta, podemos concluir que no fueron suficientes los posibles usuarios cargados en el diccionario de la herramienta Burp Suite, porque no se pudo dar con el usuario correcto, eso nos da una idea que la estrategia de utilizar usuarios con dominio de correo ralentiza el trabajo de un atacante y dependiendo del atacante, ese vector de ataque podría no ser la opción más viable para dar con el usuario real.

Otra estrategia propuesta fue el uso de honeypot con la herramienta T-Bot, para crear un servidor web fuera de la infraestructura de la organización y confundir a los atacantes para que pareciera que están atacando el servidor verdadero. Con este procedimiento buscábamos distraer la atención de quienes quieran atacar la infraestructura de la empresa auspiciante y complicar más su libre acción sobre esta, considerando que sitios 100% seguros en el mundo no existen, con los conocimientos adquiridos en este master, hemos comprendido lo amplio que es administrar ciberseguridad en ambientes de

desconocimiento total, es por ello y a fin de mejorar sustancialmente la ciberseguridad en la empresa auspiciante, siempre se propuso soluciones en función de las intenciones de los propietarios de esta, así como de sus presupuestos.

3.2.1 Técnicas de hacking ético para la mitigación y recuperación.

Como primer punto indicaremos un concepto fundamental sobre que es hacking ético, antes de ello vamos a dar un concepto corto sobre lo que es un hacker. Desde nuestra perspectiva es un individuo que ha desarrollo ciertas habilidades en cuando al uso de los equipos de computación y en alguno casos equipos electrónicos, con la finalidad de acceder y desafiar las reglas de neutralidad y seguridad de las internet con diferentes objetivos, ya sean individuales, de conocimiento, de retos o simplemente de obtención de dinero.

El hacking ético aborda el análisis y la evaluación de amenazas, identifica diversas vulnerabilidades y busca explotarlas con el propósito de anticipar y subsanar estas deficiencias. Por consiguiente, resulta relevante abordar el concepto de vulnerabilidad en este contexto.

Otro concepto importante es la Vulnerabilidad, normalmente definida por un tipo de fallo ya sea en la programación o en la configuración de un equipo o software que permite acceder a cierto atributos o accesos privilegiados y que puede ser usado regularmente por personas denominadas hackers.

En las siguientes partes, se brinda una explicación clara de las etapas fundamentales del hacking ético.

Fase de reconocimiento

En esta fase se desarrollan los objetivos de ataque y a partir de ello se inicia con la obtención de datos relevantes sobre ese objetivo.

Fase de escaneo.

En esta fase se utiliza la información obtenido de la fase de reconocimiento, su uso será utilizado para halla amenazas a las redes de la institución, lo más común es el escaneo de servicio, escaneo de puertos, entre otros. Finalizado el procedimiento, inicia el escaneo de vulnerabilidades para encontrar huecos, versiones sin actualizar de los sistemas analizados.

Fase de Acceso (Explotación)

Es la fase principal de todo este proceso de hacking ético, también se le denomina fase de explotación, ya que en esta fase se siguen pasos para sacar la información vulnerable e importante de una empresa. Por lo general se usan algunas herramientas, tanto gratuitas como pagadas, y herramientas que los mismos hackers las utilizan, estas pueden ser automatizadas y configuradas en tiempos, dependiendo del tipo de ataque que se realice.

Fase de elaboración de informes

Al finalizar la fase de explotación, se obtienen datos muy importantes de las vulnerabilidades del sistema atacado, pero esto no sirve de nada sin no hay un reporte detallado de los pasos y de las vulnerabilidades encontradas, generalmente se usa una bitácora con datos completos de los ataques y actualmente se realizan dos tipos de informes, uno muy especializado y técnico, y otro de alto nivel para una facilidad de comprensión de las altas gerencias.

Algunas técnicas que se debe considerar para la mitigación y recuperación son:

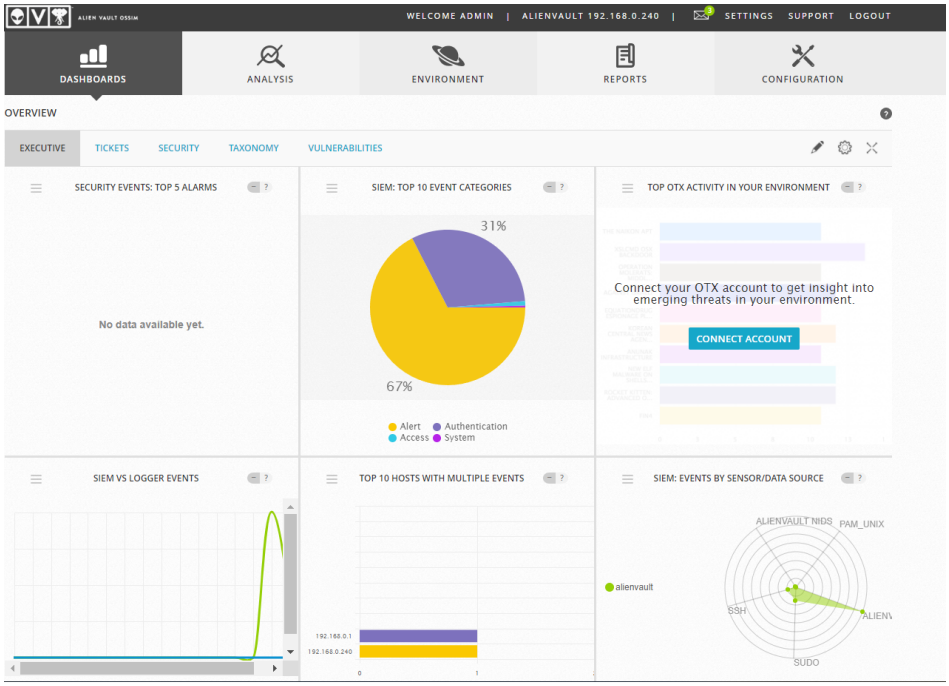
a) Evaluación de vulnerabilidades.

Se centra en la identificación y búsqueda sin abordar la corrección o el aprovechamiento de las mismas. Esta fase es especialmente valiosa en el contexto del hacking ético, ya que muchas empresas clientes inicialmente subestiman su necesidad o relevancia. Realizar un test de vulnerabilidades permite conocer los puntos débiles de una empresa, lo que puede allanar el camino para el consentimiento de servicios de hacking ético más exhaustivos en el futuro.

En la siguiente ilustración, se puede apreciar como el SIEM una vez configurado, comienza a arrojar información que nos permitirá en posterior, evaluar los datos proporcionados para determinar si son falsos positivos, si requieren de evaluación continua o si requieren de elevar a un nivel superior para un análisis más profundo.

Ilustración 23

SIEM al 67% de alertas

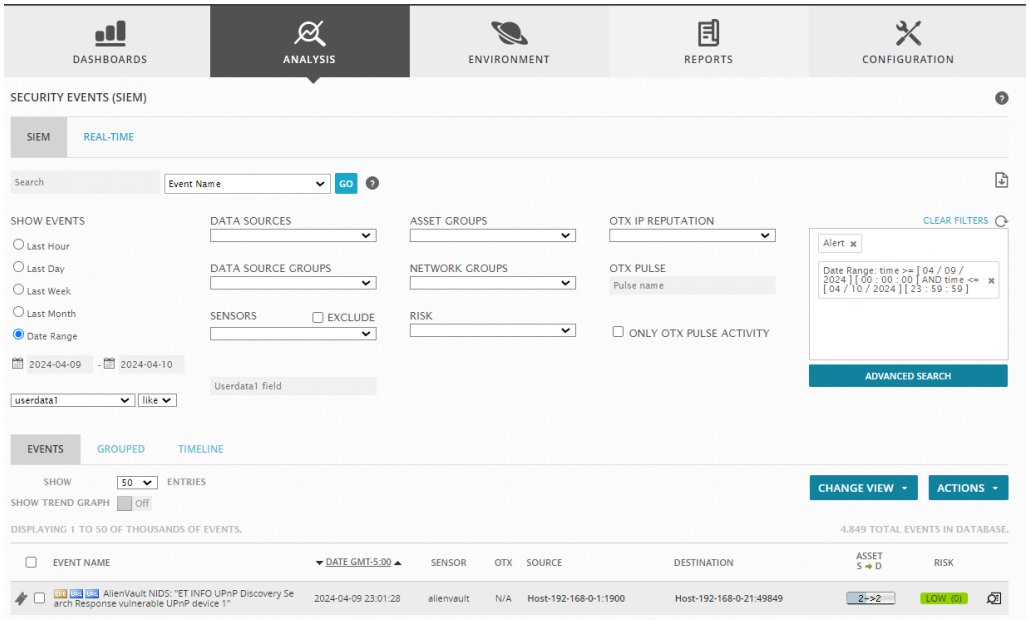


Fuente: De los autores.

Revisando el SIEM, podemos observar que comienzan a aparecer los datos esperados como se muestra en las siguientes ilustraciones, donde ya se aprecian los eventos, en que sensor está detectando, el host, el puerto y el nivel de riesgo, que por más que sea nivel bajo, no debe descartarse sin previa evaluación.

Ilustración 24

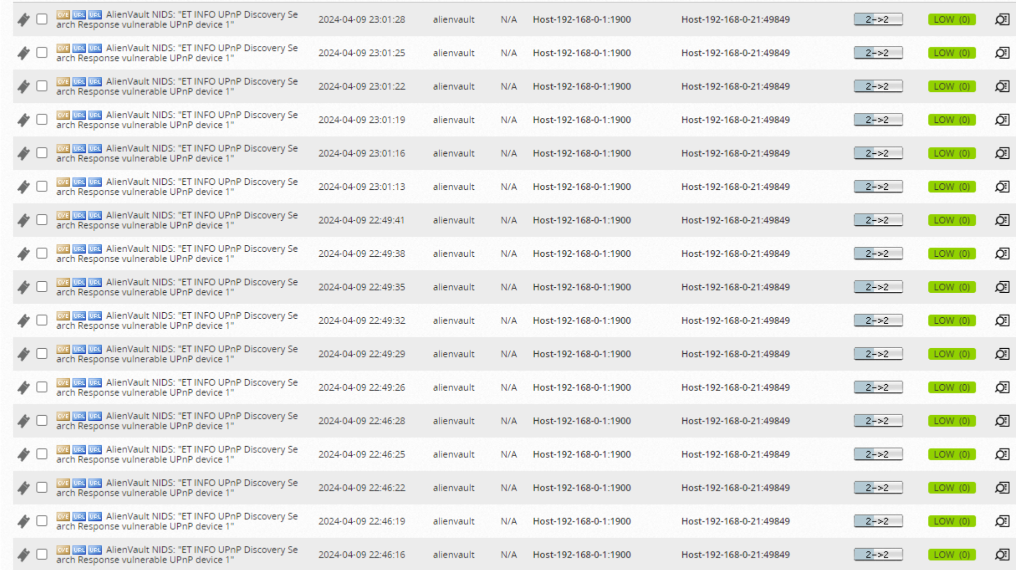
Captura de eventos del SIEM parte I



Fuente: De los autores.

Ilustración 25

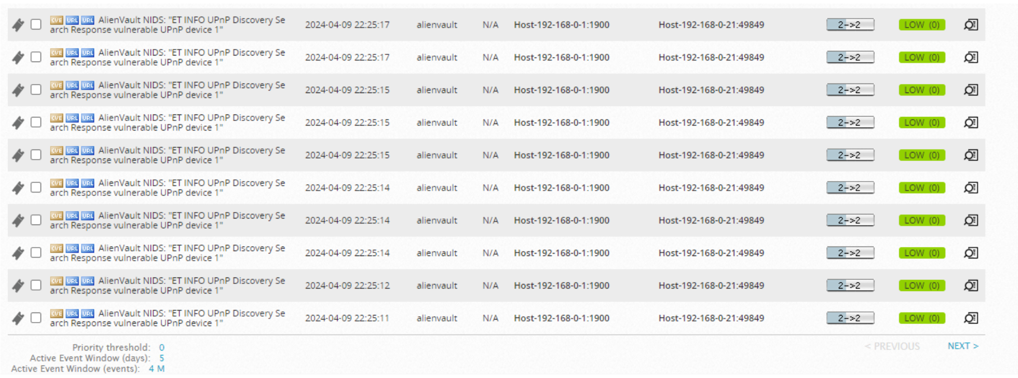
Captura de eventos del SIEM parte 2



Fuente: De los autores.

Ilustración 26

Captura de eventos parte 3



Fuente: De los autores.

b) Pentesting**.**

El pentesting viene de la unión de dos palabras en inglés Penetration Testing, y es un proceso por el cual se analiza una o varias vulnerabilidades de una empresa o una organización, con autorización firmada de dicha empresa. En español es denominada como Test de penetración.

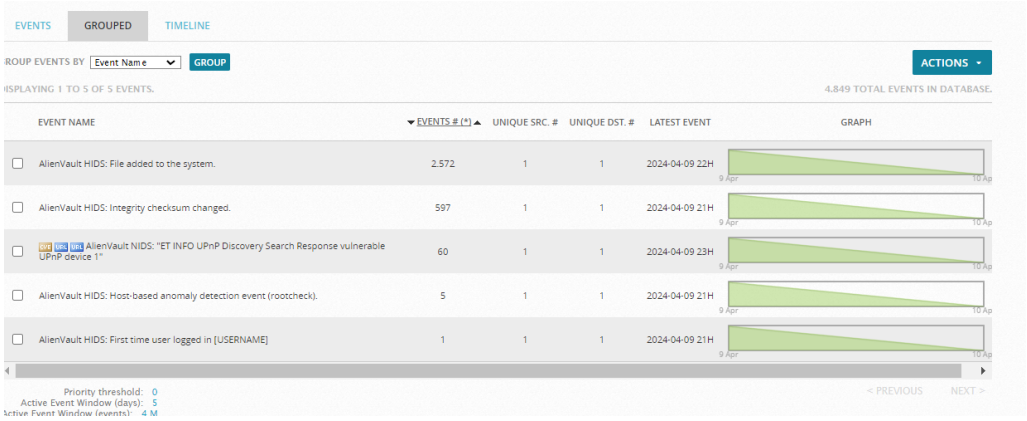
Una diferencia en las fases al analizar vulnerabilidades, es que un pentesting si explota las vulnerabilidades encontradas, su principal finalidad es verificar la viabilidad de dicho problema o vulnerabilidad que puede dañar a los sistemas de computación y así poder arreglarla.

A diferencia de la evaluación de vulnerabilidades, el pentesting si inicia la explotación de vulnerabilidades, su finalidad es verificar la viabilidad de dicho problema o vulnerabilidad que puede dañar a los sistemas de computación y así poder arreglarla.

Una de las ventajas que tiene el SIEM, es que, de manera rápida y gráfica, se puede observar el consolidado de los eventos que nos permitirá inclusive observar las futuras pruebas de pentesting.

Ilustración 27

Consolidación de eventos en el SIEM.



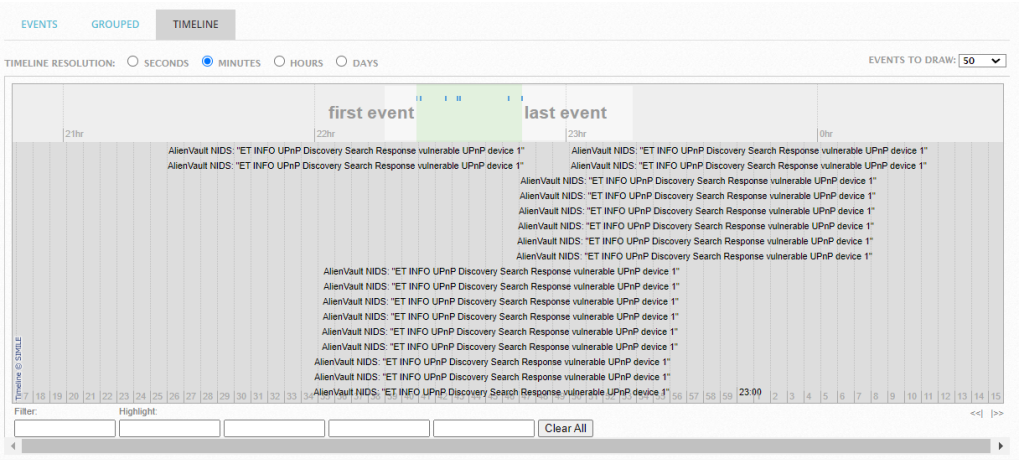
Fuente: De los autores

Otro elemento importante para analizar dentro del SIEM es la línea de tiempo, esto nos otorga una idea global del trabajo para cuando realicemos las pruebas de penetración, sepamos también hacer el seguimiento de esos eventos, para analizarlos dentro del proceso de evaluación e ir tamizando los eventos que

requieren atención y aquellos que podrían escalarse a un análisis mayor o simplemente descartarlos.

Ilustración 28

Línea de tiempo de los eventos del SIEM



Fuente: De los autores

c) Entrenamiento, y concienciación.

Las amenazas más comunes que afecta a las empresas y de acuerdo a los descrito en el capítulo correspondiente, son los Insiders o Filtrador, esto se debe a la falta de capacitación en los temas de ciberseguridad, a pesar de que muchas instituciones tiene grandes infraestructuras, con tecnología de punta, políticas y reglamentos bien definidos, pero si no existe una cultura de la seguridad en todas las áreas y estratos empresariales, pueden colocar en riesgo toda la institución, desde el punto de vista personal como de un punto de vista tecnológico, por ello la importancia de un análisis exhaustivo de sus vulnerabilidades, la concienciación y el uso de hacking ético.

Para poder realizar un monitoreo correcto vamos a ocupar el SIEM de OSSIM el cual nos va a permitir monitorear toda la actividad en tiempo real.

3.3 Análisis de ataques de ransomware utilizando SIEM**.**

Este tema implicaría investigar cómo recopilar y analizar datos forenses de un ataque de ransomware con la ayuda de SIEM y técnicas de hacking ético para identificar al atacante y comprender el alcance del daño.

La recopilación y análisis de datos forenses de un ataque de ransomware con la ayuda de SIEM y técnicas de hacking ético pueden ser una tarea compleja pero crucial para identificar al atacante y comprender el alcance del daño.

Hay que tener en cuenta que para empezar a analizar un ataque de ransomware debemos tener una preparación del entorno, es decir hay que establecer un entorno controlado y aislado para llevar a cabo la investigación forense. Esto podría incluir una red de laboratorio o máquinas virtuales, en las cuales se debe instalar ambientes de seguridad, entre ellos firewalls, IDS, para proteger el entorno de posibles amenazas adicionales durante la investigación, para ello se detallan, los elementos que se deben considerar:

3.3.1 Utilización de SIEM

Primero debemos saber que el SIEM es un sistema de seguridad informática que recopila, correlaciona y analiza registros de eventos y datos de seguridad de múltiples fuentes dentro de una red o sistema informático, el mismo que tiene como objetivo principal detectar amenazas de seguridad de manera activa, facilitando la respuesta a incidentes, proporcionando de esta manera una visión general del cómo se encuentra la seguridad de una empresa.

El SIEM es una herramienta de seguridad cibernética que nos permite detectar varias amenazas sin embargo es la mejor defensa contra el ataque de Ransomware ya que recopilan y analizan los log de eventos de seguridad de diversas fuentes, entre

ellas tenemos servidores, sistemas de detección de intrusos y firewalls. Utilizan algoritmos avanzados y reglas personalizadas para detectar patrones y/o comportamientos poco usuales que podrían indicar actividades maliciosas generando alertas para que los analistas de seguridad investiguen y respondan. Además, facilitan la similitud de eventos para comprender mejor la secuencia de un ataque y el alcance del daño, lo que permite una respuesta rápida y efectiva para mitigar el impacto del incidente.

Con la ayuda de esta herramienta podemos detectar un ataque de ransomware y analizarlo durante las primeras fases.

Tomemos en cuenta que para recopilar y analizar datos forenses de un ataque de ransomware con la ayuda de un SIEM debemos explotar todas las capacidades de este a fin de comprender el alcance y los efectos que tienen en una red el ransomware, empezando por los siguientes pasos.

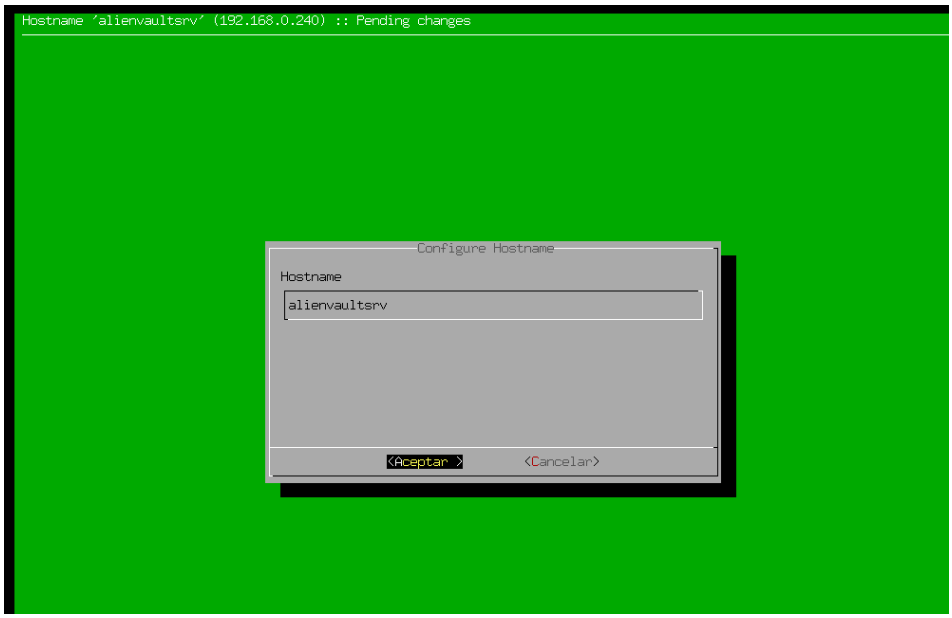
3.3.2. Configuración del SIEM:

El SIEM debe estar configurado correctamente para recopilar registros de eventos de todas las fuentes relevantes en la red, incluidos servidores, estaciones de trabajo, firewalls, sistemas de detección de intrusiones, como ya se mencionó en la parte 3.1 Evaluación del SIEM donde se muestra la instalación y configuración.

Para iniciar configuraremos el sensor, para ello, primero cambiamos el nombre del servidor que por defecto viene el mismo nombre del SENSOR, AlienVault, lo vamos a cambiar a alientvaultsrv, así evitar conflictos con los nombres en el momento de revisar los datos de SIEM AlienVault.

Ilustración 29

Inicio configuración del sensor

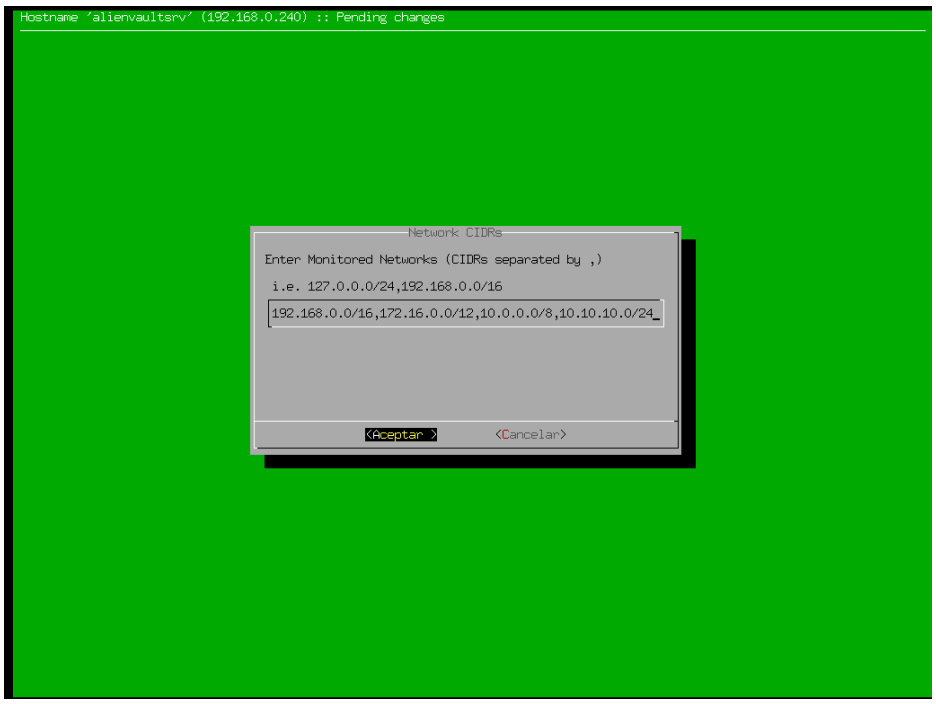


Fuente: De los autores

Es importante citar, que OSSIM Alientvault ya viene con un sensor, pero debemos configurar algunos aspectos, en el momento de instalar el OSSIM agregamos nuestra red la 192.168.0.0/24, pero en el sensor vamos a agregarle la 10.10.10.0/24 para que podamos monitorear la subred que creamos y desde donde pensamos realizar varios ataques y se configura el Data Socurce Plugins para obtener los datos de otros equipos.

Ilustración 30

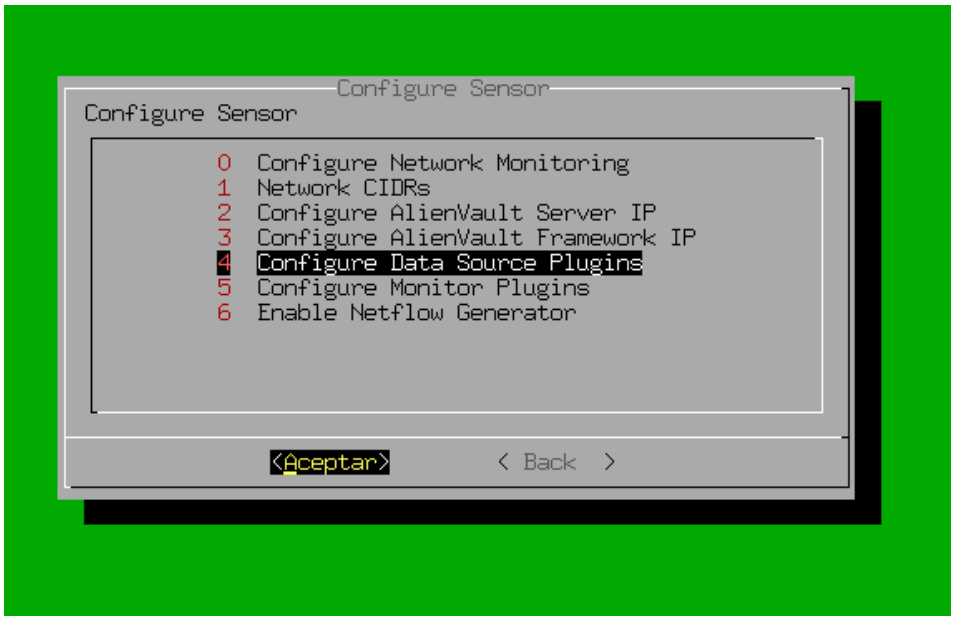
Asignación de la IP al sensor



Fuente: De los autores

Ilustración 31

Configuración del Data Socurce Plugins, para que reciba información de otros equipos

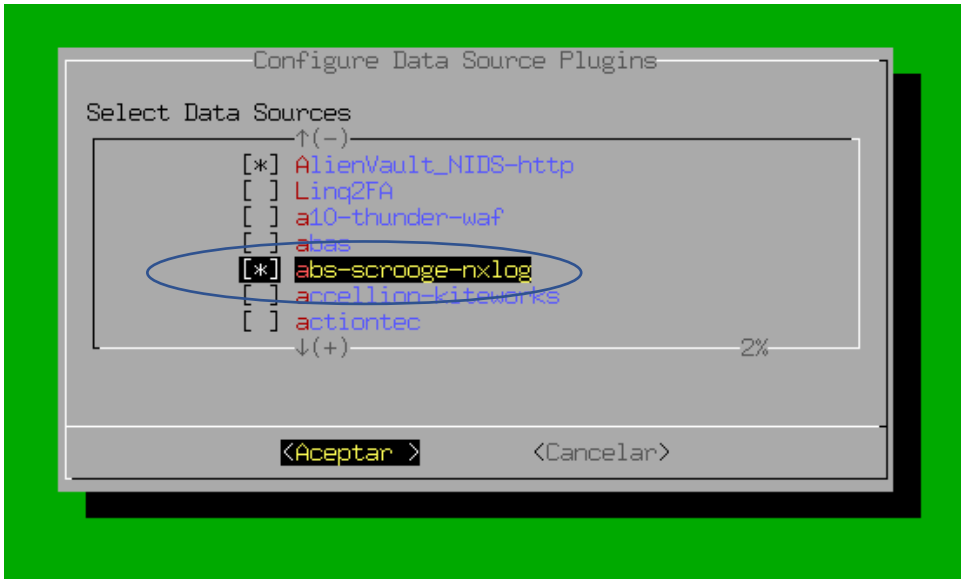


Fuente: De los autores

Como vamos a utilizar el complemento NXLog para Windows, buscaremos uno que podamos usarlo, además de seleccionar todos los que vienen incluidos en el AlienVault y los relacionados a NXLog y también los de Apache, que allí estará instalado nuestro sistema que será atacado.

Ilustración 32

Configuración de NXlog para Windows

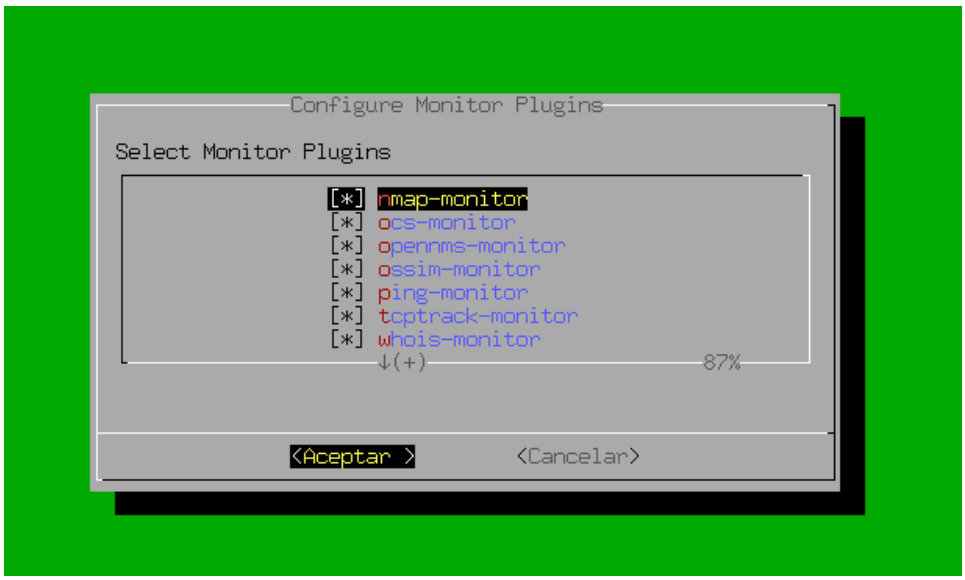


Fuente: De los autores

Luego procedemos a configurar el Monitor Plugins que nos permite instalar programas para obtener los registros de otros equipos, seleccionando todos los Plugins con la barra espaciadora.

Ilustración 33

Configuración de los plugins del nmap-monitor.



Fuente: De los autores

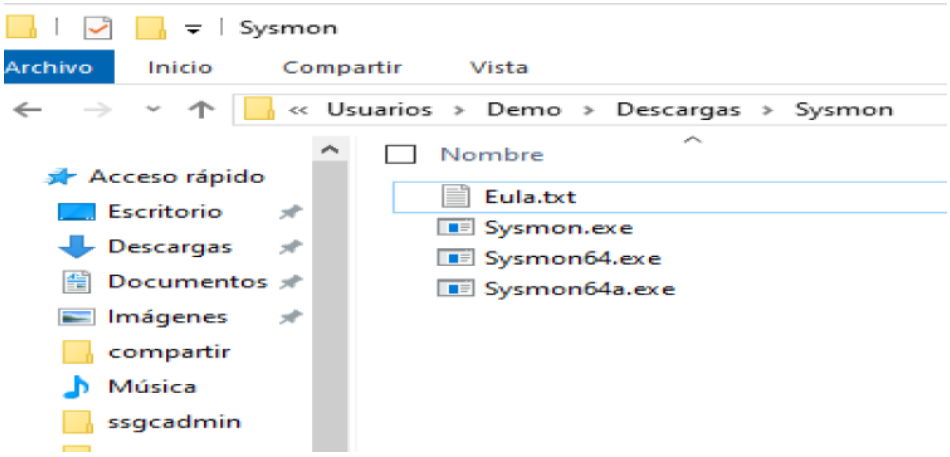
3.3.3 Monitoreo en tiempo real.

Utilizar la capacidad para monitorear en rela-time la SIEM para detectar proceso inusuales, especialmente aquellos que detectan los antivirus, o aquellos que crean procesos de apertura de puertos y que son un indicio de un ataque de ransomware. Esto incluye patrones de comportamiento anormal, como cambios inesperados en los archivos, ingresos sin autorización, o movimientos inusuales de la red.

El proceso inicial del monitoreo, empieza con descargamos la versión más actual desde los servidores de Microsoft de, Sysmon v15.14 cuya herramienta permite registrar toda la actividad que sucede en un equipo Windows, para ello, descargamos el archivo comprimido en zip que contiene los siguientes archivos:

Ilustración 34

Archivos descomprimidos de Sysmon

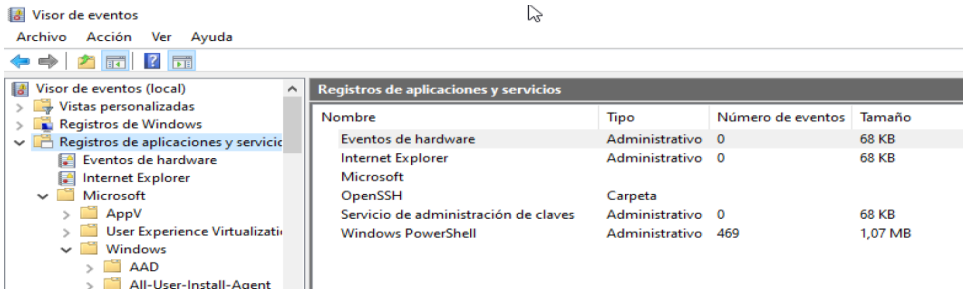


Fuente: De los autores

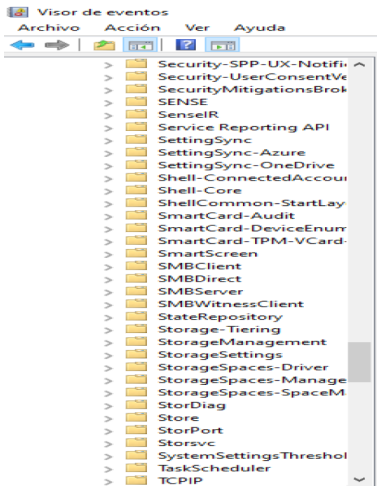
Posterior a la descarga, procedemos a abrir el visor de eventos del Windows y verificamos si tenemos instalado SYSMON, verificamos que no hay e iniciamos la instalación:

Ilustración 35

Verificación de instalación SYSMON



Fuente: De los autores

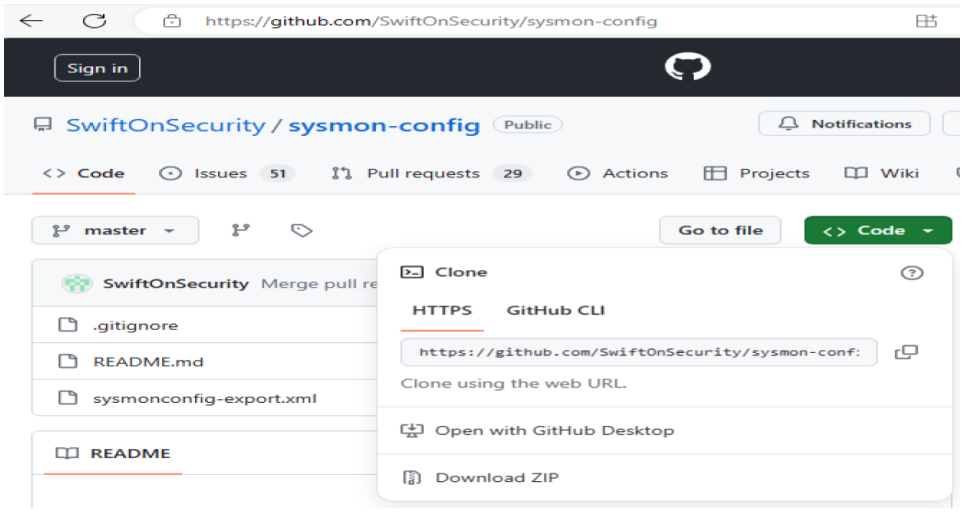


Fuente: De los autores

Antes de instalar SYSMON, necesitamos un archivo de configuración, que lo descargamos en Github para ello, buscamos Swiftonsecurity Sysmon github y descargamos los archivos como zip.

Ilustración 36

Descarga de archivo de configuración en github

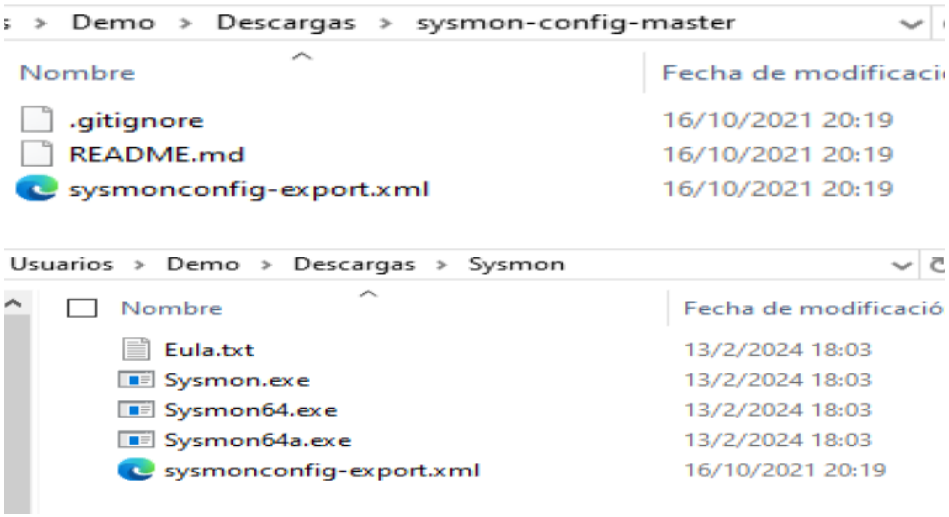


Fuente: De los autores

Una vez verificado en github, procedemos a copiar el archivo XML que está en el archivo zip y lo pegamos en la carpeta de instalación de SYSMON.

Ilustración 37

Copiamos y pegamos el archivo XML de github en carpeta SYSMON

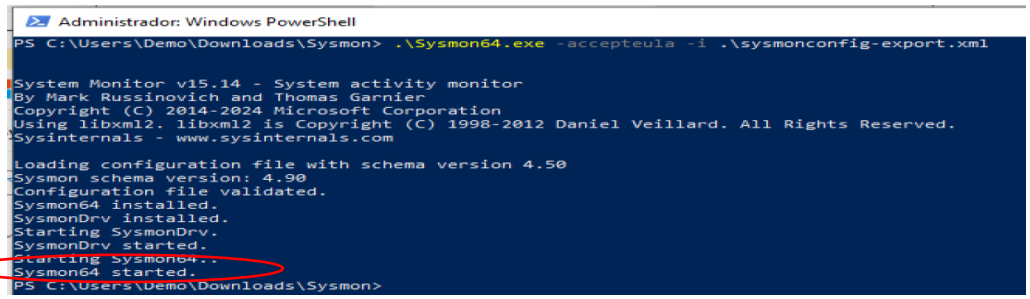


Fuente: De los autores

Una vez realizado esa tarea, es importante considerar que para instalarlo lo hacemos desde un terminal, normalmente Power Shell de Windows, luego para instalarlo ejecutamos el siguiente comando, [Sysmon64.ex –accepteula –i sysmonconfig-export.xml], con eso podemos ver que ya tenemos instalado e iniciado el agente de Logs, Sysmon.

Ilustración 38

Verificación SYSMON started.

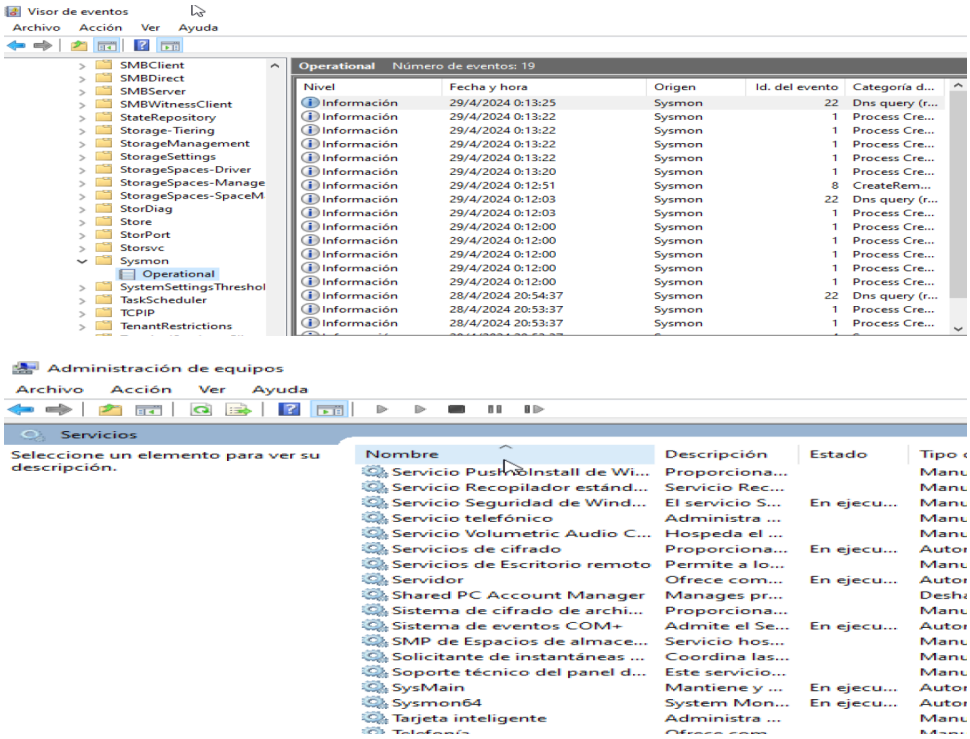


Fuente: De los autores

Podemos verificar en el visor de eventos que ya está ejecutándose SYSMON y de la misma manera en el administrador de servicios.

Ilustración 39

Ejecución de SYSMON confirmada



Fuente: De los autores

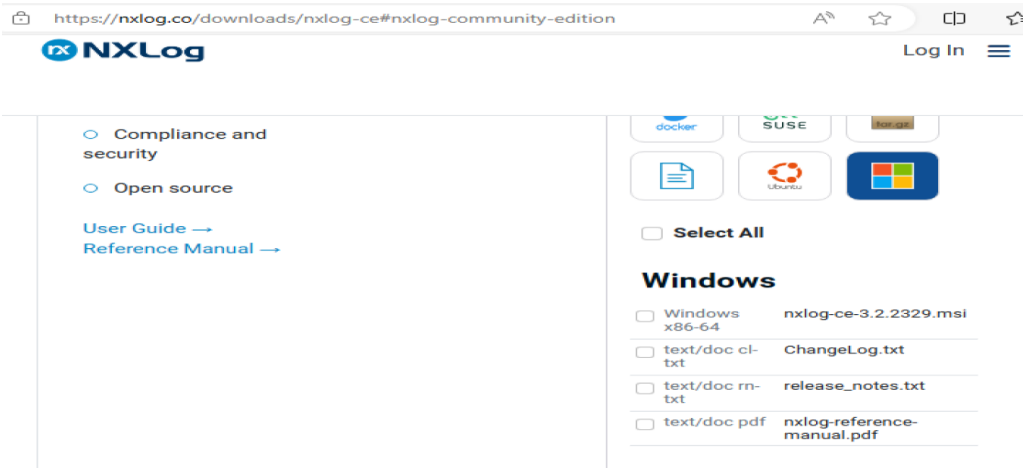
3.3.4 Recopilación de evidencia.

Utilizar las capacidades de almacenamiento de registros del SIEM para recopilar y almacenar evidencia forense relevante, como registros de eventos, registros de tráfico de red, registros de cambios de archivos y otros datos pertinentes relacionados con el ataque.

Para realizar esta actividad, es importante realizar la configuración del agente de reenvío de registros NXLOG (SYSMON), para ello, procedemos a descargar NXLOG comunity edition y seleccionamos la versión para Windows.

Ilustración 40

Instalación de NXlog comunity edition para Windows



Fuente: De los autores

Una vez que verificamos que están corriendo en los servicios de Windows, procedemos a detenerlo porque falta instalar los archivos de configuración, para ello descargamos del link https://mrksecurity.medium.com/alien-vault-ossim-nxlog-conf-3d8c703f0573 la configuración y la pegamos en un archivo llamado **nxlog.conf,** y realizamos los siguientes cambios:

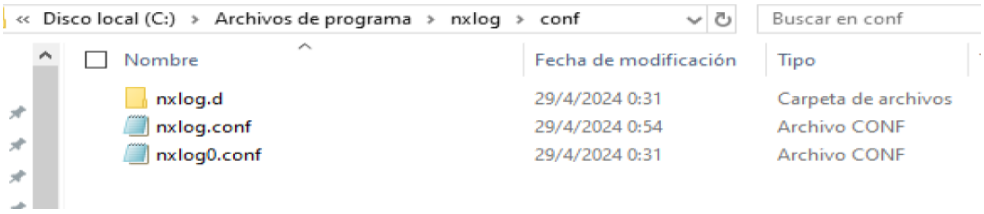
1. Verificamos si el path de nxlog en Windows es el adecuado y descomentarlo

2. Cambiamos la IP `por la IP de nuestro servidor OSSIM.

Una vez realizado aquello, procedemos a cargarlo en la carpeta **C:/program Files/nxlog/conf/**

Ilustración 41

Configuración NXlog para enrutar log al SIEM OSSIM

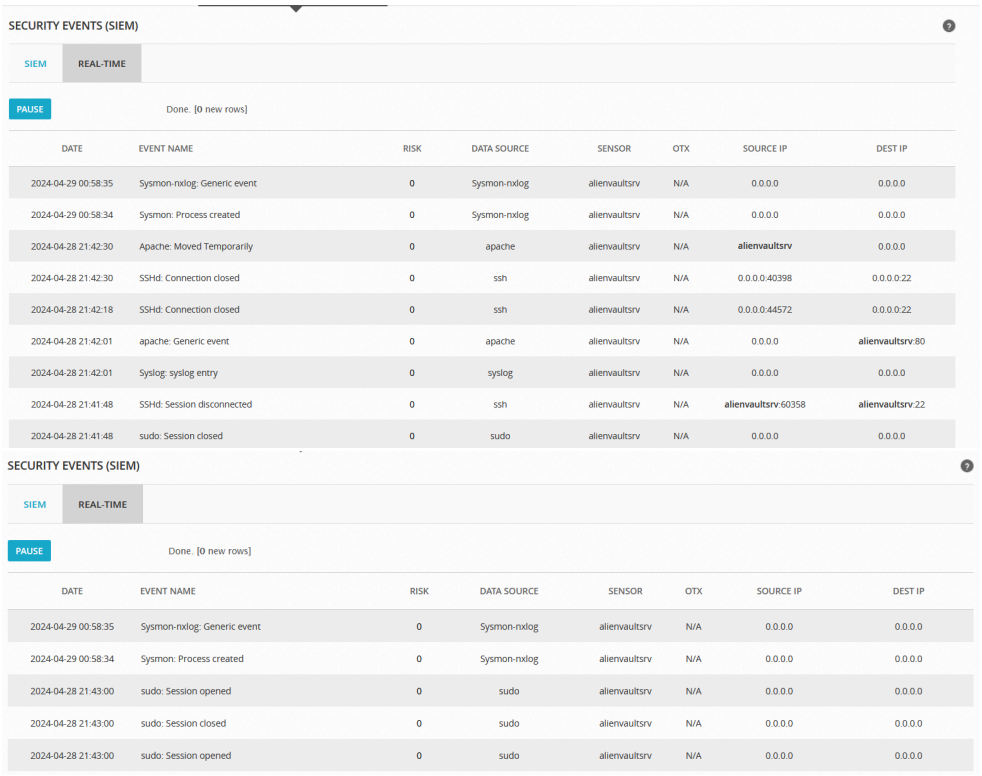


Fuente: De los autores

Una vez realizado este trabajo, se puede observar que el SIEM comienza a detectar y al actualizarlo, este cambia.

Ilustración 42

Captura de logs en el SIEM.

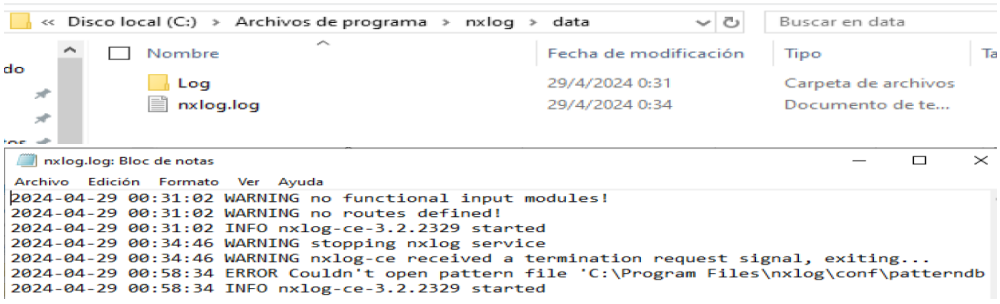


Fuente: De los autores

Podemos verificar los logs que se crea en la máquina instalada comienzan a enviar datos al SIEM, se lo verifica en la siguiente ilustración:

Ilustración 43

Envío de logs en el SIEM.



Fuente: De los autores

3.3.5 Análisis forense.

Utilizar herramientas de análisis forense junto con los datos recopilados por el SIEM para investigar el ataque en profundidad. Esto incluye analizar los registros de eventos en busca de patrones de comportamiento malicioso, identificar la cadena de eventos que condujo al ataque y determinar el alcance del daño.

3.3.6 Correlación de eventos.

Utilizar las capacidades de correlación de eventos del SIEM para identificar relaciones entre diferentes eventos y actividades en la red, lo que puede ayudar a comprender cómo se propagó el ransomware y qué sistemas o usuarios se vieron afectados.

3.3.7 Generación de informes.

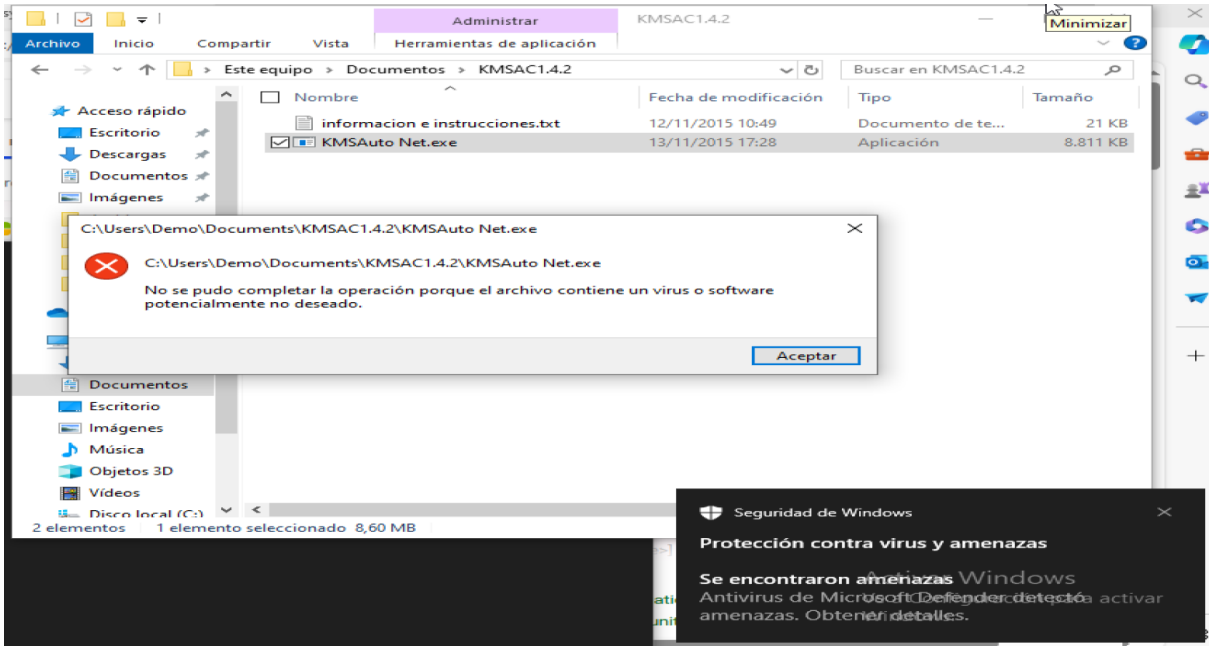
Utilizar el SIEM para generar informes detallados sobre el ataque de ransomware, incluida una cronología de eventos, IOC identificados, análisis de impacto y recomendaciones de mitigación.

Podremos ver como el SIEM va analizando y encontrando las irregularidades creadas por el ransomware, realizando un testeo con ransomware crypUide, sin ataque a archivo o servicios sensibles de Windows.

Para analizar si el SIEM tiene un correcto funcionamiento, este debería ser capaz de detectar la actividad relacionada con el virus que estás ejecutando. Si el antivirus de Windows detecta el virus, pero el SIEM no registra esta detección o no genera alertas adecuadas, podría indicar un problema en la configuración o en la efectividad del SIEM.

Ilustración 44

Reporte de detección de virus en Windows

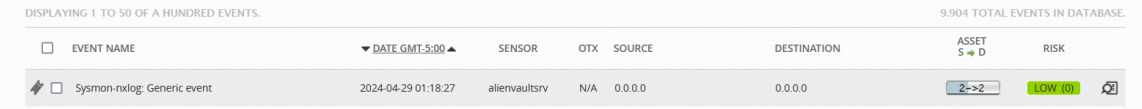


Fuente: De los autores

Procedemos a identificar el problema mostrando el siguiente evento:

Ilustración 45

Evento generado por el SIEM.

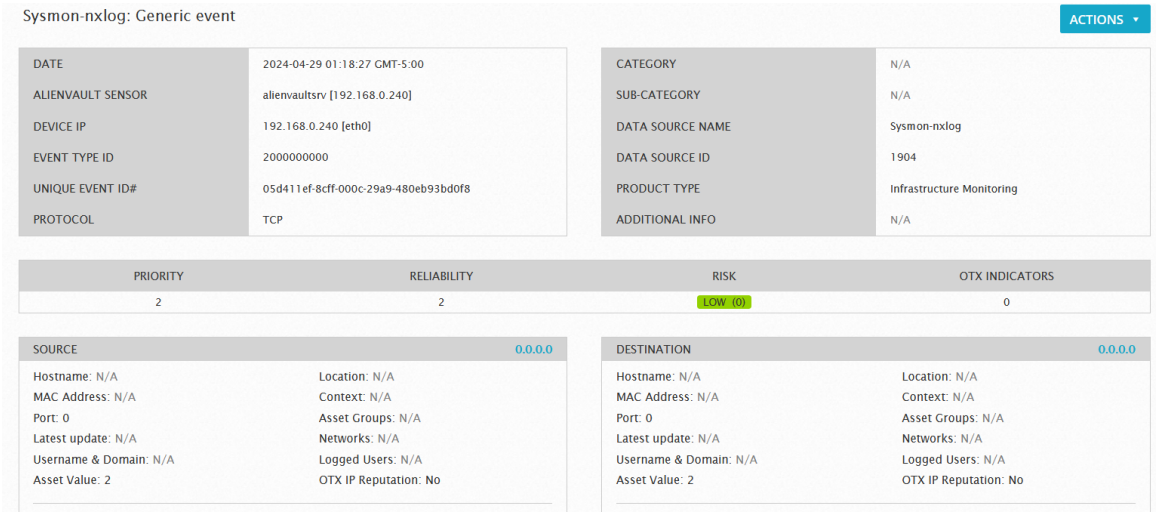


Fuente: De los autores

Cuando nos permitimos analizar en su totalidad los detalles del evento, el cual nos proporciona información exhaustiva sobre el incidente registrado, incluyendo datos recopilados, indicadores relevantes y la evaluación de la reputación de la dirección IP involucrada, incluyendo niveles de riesgo y confiabilidad calculados. Esencialmente, estos detalles brindan una visión completa del evento, su contexto y su nivel de amenaza asociado.

Ilustración 46

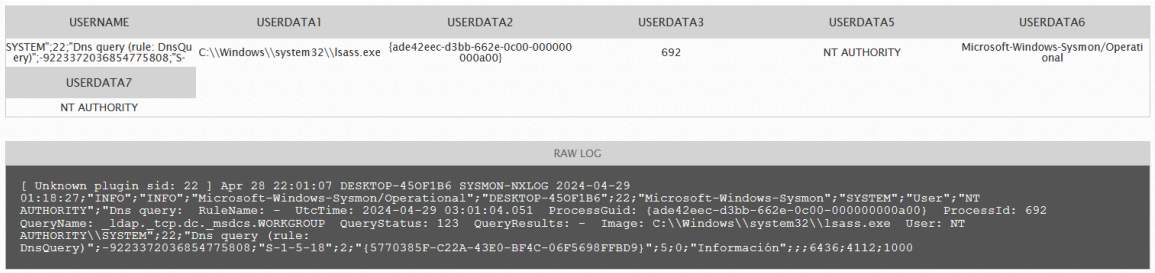
Detalle del evento detectado por el SIEM parte 1.



Fuente: De los autores

Ilustración 47

Detalle del evento detectado por el SIEM parte 2.



USERNAME	USERDATA1	USERDATA2	USERDATA3	USERDATA5	USERDATA6
SYSTEM";22;"Dns query (rule: DnsQuery)";-9223372036854775808;"S-	C:\\Windows\\system32\\lsass.exe	{ade42eec-d3bb-662e-0c00-000000000a00}	692	NT AUTHORITY	Microsoft-Windows-Sysmon/Operational

USERDATA7
NT AUTHORITY

RAW LOG

```
[ Unknown plugin sid: 22 ] Apr 28 22:01:07 DESKTOP-45OF1B6 SYSMON-NXLOG 2024-04-29
01:18:27;"INFO";"INFO";"Microsoft-Windows-Sysmon/Operational";"DESKTOP-45OF1B6";22;"Microsoft-Windows-Sysmon";"SYSTEM";"User";"NT
AUTHORITY";"Dns query:  RuleName: -  UtcTime: 2024-04-29 03:01:04.051  ProcessGuid: {ade42eec-d3bb-662e-0c00-000000000a00}  ProcessId: 692
QueryName: _ldap._tcp.dc._msdcs.WORKGROUP  QueryStatus: 123  QueryResults: -  Image: C:\\Windows\\system32\\lsass.exe  User: NT
AUTHORITY\\SYSTEM";22;"Dns query (rule:
DnsQuery)";-9223372036854775808;"S-1-5-18";2;"{5770385F-C22A-43E0-BF4C-06F5698FFBD9}";5;0;"Información";;;6436;4112;1000
```

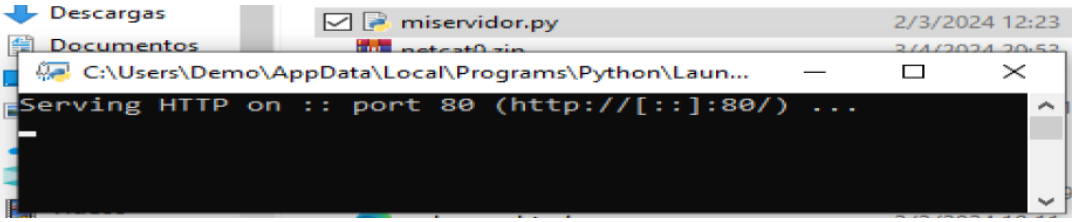
Fuente: De los autores

En otro Testeo con miservidor.exe va a implicar ejecutar un programa (miservidor.exe) que crea un backdoor, que viene a ser un acceso no autorizado al sistema. Al crear este backdoor, simularemos un escenario de ataque donde un actor malintencionado podría explotar esa vulnerabilidad para acceder al sistema sin permiso.

Si el SIEM detecta la apertura de este puerto causada por el backdoor, significa que está funcionando correctamente al identificar y registrar actividades sospechosas o maliciosas en el sistema. Esto indica que el SIEM está monitoreando adecuadamente la seguridad del sistema y proporciona alertas para que los administradores puedan tomar medidas correctivas para mitigar cualquier riesgo de seguridad. En resumen, la detección de la apertura del puerto causada por el backdoor indica una capacidad efectiva del SIEM para detectar amenazas y proteger el sistema contra intrusiones no autorizadas.

Ilustración 48

Muestra del backdoor del Ransomware



Fuente: De los autores

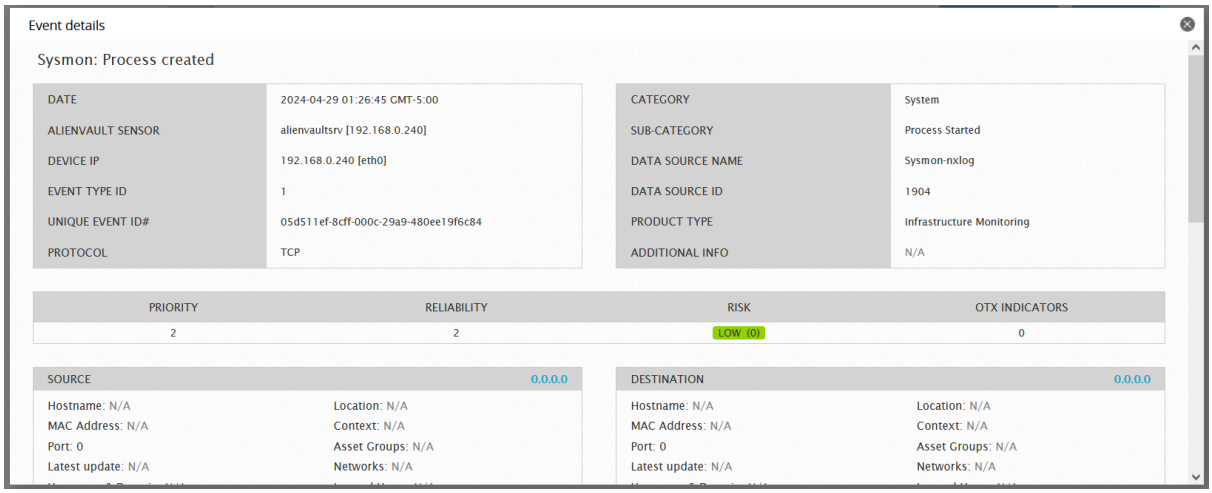
Una vez detectado por el SIEM, a pesar que lo muestra como un riesgo bajo, lo que puede significar que el SIEM está evaluando la amenaza como menos crítica o menos urgente en comparación con otras amenazas más severas. Esto podría deberse a varios factores, como la configuración de la política de seguridad, la evaluación de la amenaza o la priorización de los eventos.

Sin embargo, la capacidad de acceder al equipo comprometido desde una máquina virtual en otra subred y descargar archivos significa que la vulnerabilidad explotada por el backdoor es significativa y puede ser explotada por atacantes para realizar acciones maliciosas, como robo de datos, ejecución de código arbitrario o compromiso del sistema.

Aunque el SIEM pueda clasificar la amenaza como baja, sigue siendo importante abordar y remediar la vulnerabilidad del backdoor lo antes posible para evitar posibles consecuencias negativas, como pérdida de datos, interrupción del servicio o daños a la infraestructura de la organización y peor aún, afectar la reputación de la misma, es por ello, que el análisis del evanto a través del SIEM es primoridial.

Ilustración 49

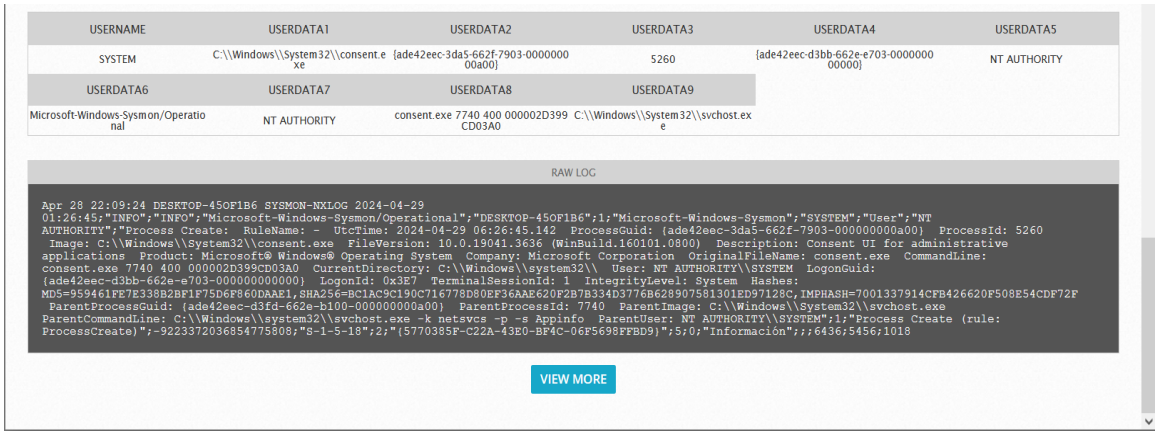
Análisis del evento en el SIEM, producido por el ransomware parte 1.



Fuente: De los autores

Ilustración 50

Análisis del evento en el SIEM, producido por el ransomware parte 2.



Fuente: De los autores

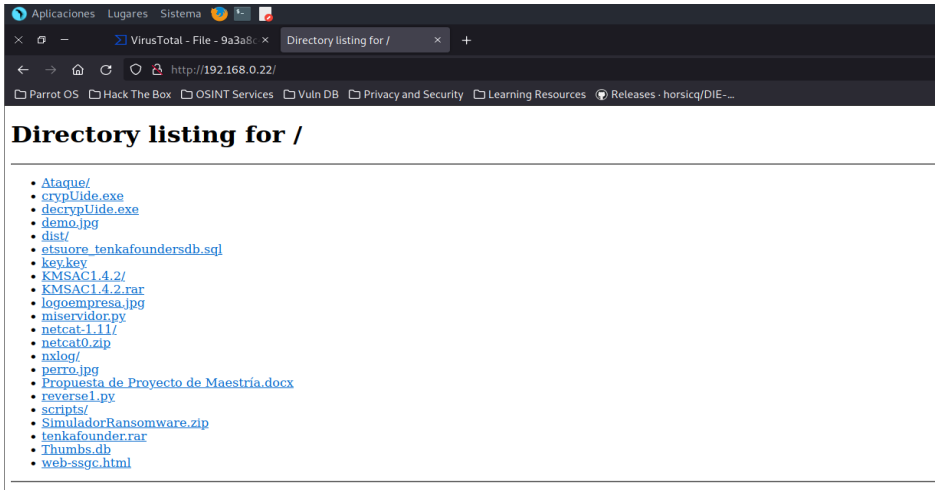
Sin embargo, de acuerdo a la imagen la capacidad de acceder al equipo comprometido desde un navegador web desde la máquina virtual de Parrot que esta en otra subred y poder descargar archivos significa que la vulnerabilidad explotada por el backdoor es significativa y puede ser explotada por atacantes para realizar acciones

maliciosas, como robo de datos, ejecución de código arbitrario o compromiso del sistema.

Aunque el SIEM pueda clasificar la amenaza como baja, sigue siendo importante abordar y remediar la vulnerabilidad del backdoor lo antes posible para evitar posibles consecuencias negativas, como pérdida de datos, interrupción del servicio o daños a la reputación de la empresa.

Ilustración 51

Muestra el acceso del backdoor a la información del servidor.



Fuente: De los autores

Si la amenaza en el SIEM puede mostrarse como baja, esta no se puede descartar, porque como se visualiza en la Ilustración anterior a este párrafo, el back door low risk , muestra ya que existe una vulnerabilidad que requiere ser atendida por los diferentes niveles de análisis técnico y/o inclusive procesos de reversing, para analizar el script y su posible vextor de ataque.

En el Dashboard del SIEM, tiene registrado el acceso de forma gráfica de los indicidentes que a través del enturamiento de los logs, permite tener una idea general de los eventos de ciberseguridad ocurridos en la organización, lo que demuestra la

importancia de contar con una tecnología de esta envergadura para soportar las acciones y respuesta a incidentes que se podría presentar contra la infraestructura pero lo importante de todo es que se presenta de manera previa como indicios.

Ilustración 52

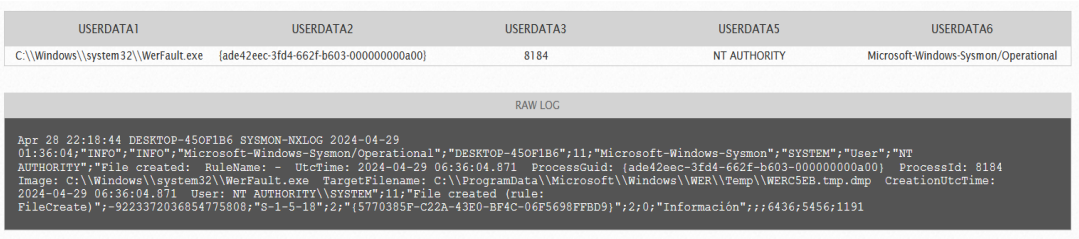
SIEM configurado y funcionando

Fuente: De los autores

Cuando damos click en Access, nos muestra el último acceso a la máquina de Windows, en nuestro caso, el Testeo 3, que es un ataque con crypUideS.exe, versión modificada de nuestro ransomware, pero con un ataque directo a un servicio de Windows.

Ilustración 53

Prueba de detección del ataque en el SIEM.



USERDATA1	USERDATA2	USERDATA3	USERDATA5	USERDATA6
C:\\Windows\\system32\\WerFault.exe	{ade42eec-3fd4-662f-b603-000000000a00}	8184	NT AUTHORITY	Microsoft-Windows-Sysmon/Operational

RAW LOG

```
Apr 28 22:18:44 DESKTOP-45OF1B6 SYSMON-NXLOG 2024-04-29
01:36:04;"INFO";"INFO";"Microsoft-Windows-Sysmon/Operational";"DESKTOP-45OF1B6";11;"Microsoft-Windows-Sysmon";"SYSTEM";"User";"NT
AUTHORITY";"File created:  RuleName: -  UtcTime: 2024-04-29 06:36:04.871  ProcessGuid: {ade42eec-3fd4-662f-b603-000000000a00}  ProcessId: 8184
Image: C:\\Windows\\system32\\WerFault.exe  TargetFilename: C:\\ProgramData\\Microsoft\\Windows\\WER\\Temp\\WERC5EB.tmp.dmp  CreationUtcTime:
2024-04-29 06:36:04.871  User: NT AUTHORITY\\SYSTEM";11;"File created (rule:
FileCreate)";-9223372036854775808;"S-1-5-18";2;"{5770385F-C22A-43E0-BF4C-06F5698FFBD9}";2;0;"Información";;;6436;5456;1191
```

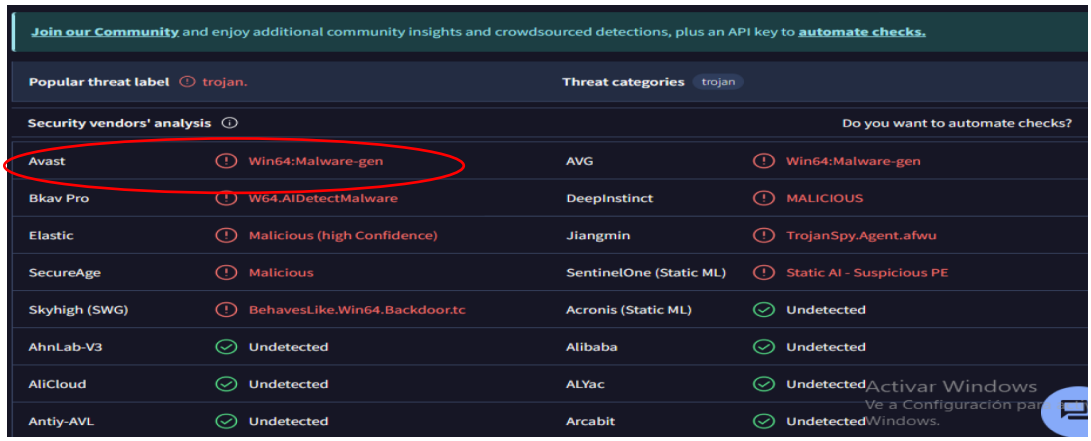
Fuente: De los autores

3.3.8 Evaluación de ataque usando cripuide.exe (ransomware propietario)

Al iniciar le ataque inicialmente los antivirus no detectaban el ransomware, por lo que usamos varias estrategias entre ellas modificar el código para que sea más específico en un ataque a un registro de Windows, pero lo que logramos es simplemente que no ejecutaba esas instrucciones porque Windows pedía certificado digital, no pasaba de ese detalle y no saltaba una alarma, así que probamos otra estrategia, es subirlo y revisarlo varias veces en **virus total** hasta que sea detectado como una potencial amenaza, y lo logramos como se muestra en la siguiente ilustración.

Ilustración 54

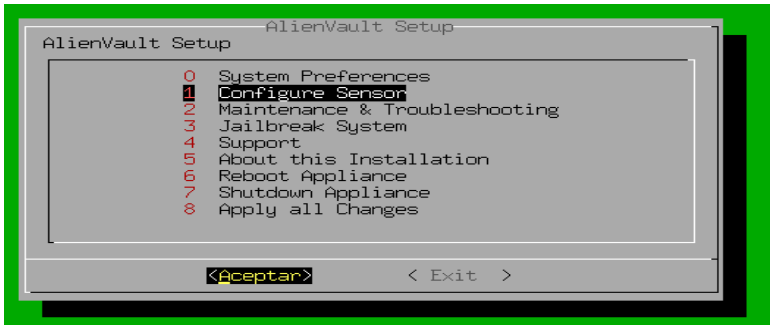
Detección de malware por parte de virus total



Con ello ya podemos descargarnos un antivirus que lo detecte, y al ejecutarse se muestre en el SIEM, pero no podemos descargar cualquier antivirus, necesitamos de uno que el SIEM Alienvault tenga dentro de su base de datos de plugins para que se conecte con el sensor, y en este caso buscando en el servidor encontramos que soporta **Avast** (Ilustración 55 y 56).

Ilustración 55

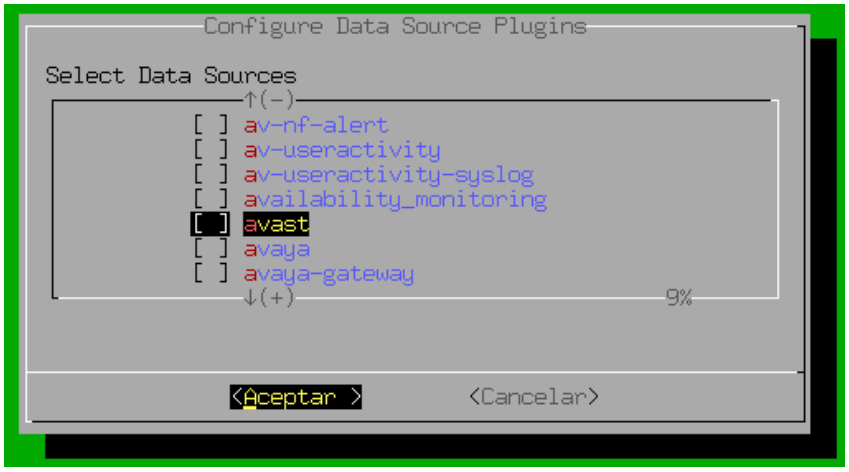
Actualización de sensor



Fuente: De los autores

Ilustración 56

Selección de plugin AVAST

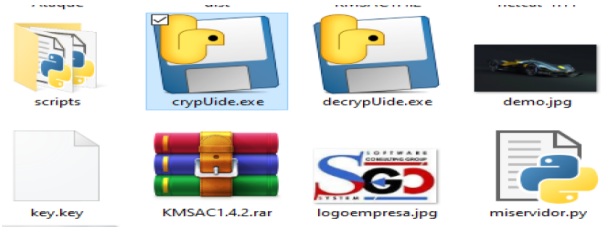


Fuente: De los autores

Ahora configurado el plugin de avast podemos instalar el avast y luego de ello ejecutaremos nuestro ransonware cripUide.exe

Ilustración 57

Ejecución del ransomware cripUide.exe

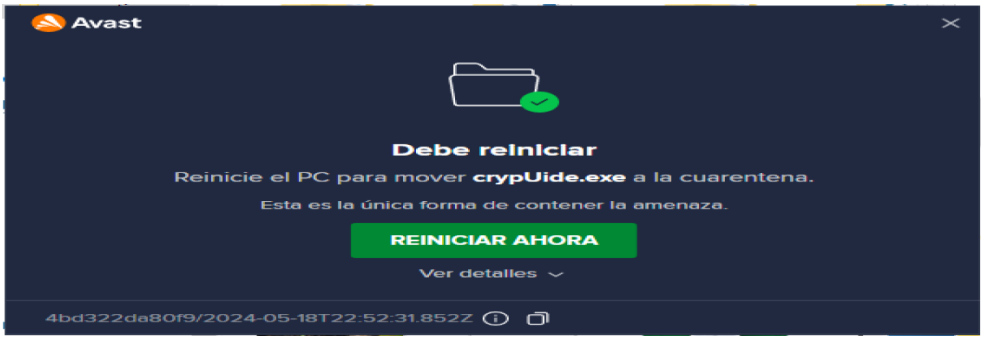


Fuente: De los autores

Inmediatamente el Avast le reconoce como amenaza y lo manda a cuarentena como lo muestra la Ilustración 58.

Ilustración 58

Detección del ransomware cripUide.exe por parte de Avast



Fuente: De los autores

Ahora veamos como se muestra esa detección en el SIEM, que lo ha detectado como un evento como se puede apreciar en las ilustraciones 59 y 60.

Ilustración 59

Evento detectado en el SIEM

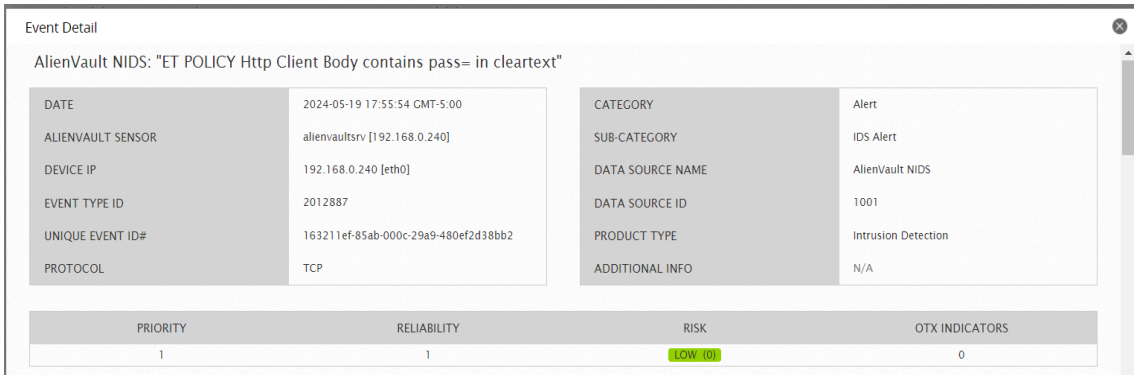
DATE	SIGNATURE	SOURCE	DESTINATION	SENSOR	RIS
2024-05-19 17:55:54	AlienVault NIDS: "ET POLICY Http Client Body contains pass= in cleartext"	Host-192-168-0-25	Windows10virtualizado	alienvaultsrv	

Fuente: De los autores

Nota: Podemos observar más información sobre el evento dando clic sobre el ícono de lupa

Ilustración 60

Mayor información detectada en el SIEM.



Fuente: De los autores

Aunque es un ataque muy potente, no se entiende por qué el SIEM coloca este evento como LOW, imaginamos porque se pudo detectar a tiempo el ataque.

CAPÍTULO IV CONCLUSIONES Y RECOMENDACIONES

Como se ha podido evidenciar, el SIEM es una excelente herramienta de apoyo a las operaciones, procedimientos y procesos de ciberseguridad que se busca implantar e implementar en una organización, a través de la integración de los logs que emiten los sensores como firewall, IPS, IDS, web, etc para consolidad esa información y poderla analizar para bien sea escalarla a un nivel superior de análisis técnico pormenorizado o simplemente descartar como falsos positivos.

Dentro de este estudio pudimos verificar la efectividd de la herramienta SIEM y lo importante que es para una organización por más pequeña que esta fuere, explotar esa bondad tecnológica en pos de un manejo saludable de la ciberseguridad, más aún conociendo que los diferentes procesos de hacking que dependiendo del tipo de ataque que se busque consolidar, también pueden generar alertas en el SIEM demostrando así sus beneficios en ciberseguridad.

Si nos enfocamos en cambio en el ransomware y conocedores de lo que este malware dependiendo de su configuración pueda hacer no solo con encriptar la información sino que a sus creadores otorgarles la potestad una vez secuestrados los datos, hacerlos públicos o en el peor de los escenarios atacar a las infraestructuras de los clientes cuyos datos fueron esncriptados por un rescate, habren las puertas para que el SIEM permita detectar a tiempo, cualesquier posible vector de ataque sobre la infraestructura de la organización explotando obviamente las vulnerabilidades que esta tiene.

El SIEM por ende pasa a ser en la actualidad, una importante herramienta de prevención y detección temprana a posibles sucesos de vulneración seguridad, siendo la base en un futuro, para la implmenentación de un SOC[7] en la medida que la infraestructura crezca.

Considerando la utilización para este estudio de un ransomware bajo un entorno controlado, ayudó mayoritariamente a desarrollar estrategias que permitan visualizar de manera temprana una posible amenaza, la fama que tiene este tipo de malware, motivó a realizar este estudio, en una infraestructura de reducido impacto en caso que el ransomware se saliera de control, por ello, el grupo tomó la decisión de utilizar su propio ransomware que incluía solamente un código para aperturar un back door, si bien en otra parte de este script también estaba activada la opción de encriptar datos, de igual forma incluímos el desencriptador para tranquilidad del CEO de la empresa auspiciante.

Con todo esto, las pruebas realizadas con la tecnología SIEM sobre la infraestructura de la organización, permitieron cubrier las espectativas del representante legal, se pudo demostrar que los beneficios son mayores cuando existen herramientas como OSSIM que siendo un Open Source, se puede realizar un trabajo SIEM muy respetable, pues Alient Vault. OSSIM pasa a ser una alternativa SIEM muy fiable y de bajo costo para organizaciones como la auspiciante.

[7] Security Operations Center

Referencias bibliográficas.

Acuña Paredes Yesenia de las Mercedes, A. S. (2022). *Implementación de un SIEM para la identificación de posibles ciberataques en la empresa Torres & Torres.* Obtenido de Repositorio Digital UIDE: https://repositorio.uide.edu.ec/handle/37000/5603

Agudelo Castro Bryan Adrián, Á. Y. (2022). *Elaboración de 5 Casos de Uso para Plataforma SIEM Institucional en el Sector Financiero a ser implementado por la empresa de Seguridad Informática Secure Soft.* Conseguido del Repositorio Digital de la Universidad Internacional del Ecuador https://repositorio.uide.edu.ec/handle/37000/5610

Gómez Prado Sandra Patricia, S. B. (2023). *Propuesta de implementación de SIEM en un centro de capacitación, con tres casos de usos, utilizando Mitre attack.* Conseguido del Repositorio Digital de la Universidad Internacional del Ecuador https://repositorio.uide.edu.ec/handle/37000/6615

Patiño Rosero Wilson Steven, P. Y. (2023). *Implementación de un SIEM en el área de TI para identificar y centralizar posibles eventos en la infraestructura critica de la industria gráfica.* Conseguido del Repositorio Digital de la Universidad Internacional del Ecuador https://repositorio.uide.edu.ec/handle/37000/6613

Kaspersky. (01 de 01 de 2024). *CIBERAMENAZA MAPA EN TIEMPO REAL*. Recuperado el 01 de 01 de 2024, de Kaspersky: https://cybermap.kaspersky.com/es

García Merino, J. (2018). *Ventajas e Implementación de un sistema SIEM*. Recuperado el 02 de 04 de 2024, de Universitat Oberta de Catalunya https://openaccess.uoc.edu/handle/10609/107546

Guevara Jurado, L. A. *El hacking ético como servicio conexo de consultoría en seguridad por parte de las empresas de seguridad privada*. Recuperado el 02 de 04 de 2024, de Universidad Militar Nueva Granada: https://repository.unimilitar.edu.co/handle/10654/40525

Astudillo, K. (2013). *HACKING ÉTICO 101 Cómo hackear profesionalmente*.

Benchimol, D. (2011). *Hacking desde Cero. Buenos Aires, Argentina: Fox Andina en coedición con Gradi S.A.*

Borghello, C. (2001). Tesis "*Seguridad Informática: Sus Implicancias e Implementación"*

Check Point Software Technologies Ltd.(2022) *Técnicas de detección de ransomware* https://checkpoint.com/es/cyber-hub/threat-prevention/ransomware/ransomware-detection-techniques/

Pure Storage *Ejemplos de amenazas que puede detectar una solución SIEM* de Pure Storage: https://www.purestorage.com/la/knowledge/what-is-siem.html

Equipo Qumulo (2021) *Cómo detectar patrones de acceso de ransomware* https://qumulo.com/es/blog/how-to-detect-ransomware-access-patterns/

APÉNDICE “A”

Autorización de trabajos sobre la infraestructura de la Empresa SOFTWARESYSTEM GC

SOFTWARESYSTEM GC
CONSULTING GROUP
AUDITORIA, CONSULTORIA, DESARROLLO DE SOFTWARE, ETHICAL HACKING, INFORMATICA FORENSE, INSTALACION DE REDES, VENTA DE EQUIPOS Y CAPACITACION
RUC: 1713306627001

AUTORIZACIÓN

Quito 10 de mayo de 2024

Yo, Gerardo Cajamarca Méndez CEO de la Empresa SOFTWARESYSTEM GC., autorizo a los ciudadanos Julio Gancino C.I. 1714626270, Bryan Jaya C.I. 1718322777, Yadira García C.I. 1718294281 y Robert Granda C.I. 1709693855, estudiantes de Maestría en Ciberseguridad de la Universidad Internacional del Ecuador, a realizar las pruebas SIEM y Hacking Ético sobre la infraestructura de mi organización, a fin de obtener los resultados requeridos para la obtención de su grado en Maestría, es por ello, que se les otorgará todas las facilidades para ese cometido, mismos que garantizan que utilizarán amenazas demo y/o de riesgo mínimo en ambientes controlados para garantizar que no exista afectación alguna.

Los interesados pueden hacer uso del presente como a bien tuviese sin responsabilidad para SOFTWARESYSTEM GC, ni para ninguno de sus funcionarios.

Atentamente

Firmado electrónicamente por:
GERARDO IVAN CAJAMARCA MENDEZ
Razón:
Localización:
Fecha: 2024-05-10T21:17:45.839329-05:00

Ing. Gerardo Cajamarca Méndez Mgs.
CEO

Dirección: Conocoto - Los Alamos **Teléfonos:** 4521 203 / 0995341444 M
E-mail : gerardocim@softwaresystem-gc.com **Web :** www.softwaresystem-gc.com
Quito - Ecuador