Universidad CENFOTEC

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Detección de intrusiones cibernéticas mediante la utilización de sistemas honeypot internos, integrándose con plataformas SIEM gratuitas

Pérez Araya Warren

Agosto de 2022

Declaratoria de derechos de autor

Dedicatoria

Deseo agradecer a mi familia por todo el apoyo durante este proceso. A pesar de haber sido un largo camino, siempre estuvieron pendientes y anuentes a ayudarme.

A mi profesor tutor, el máster Carlos Calvo Muñoz que sin su guía, paciencia y apoyo nada de esto hubiera sido posible.

Universidad CENFOTEC
SOMOS LO QUE SABEMOS

Universidad Cenfotec
Carrera de Postgrado
Maestría Profesional en Ciberseguridad

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Pérez Araya Warren.**

M. Sc. Carlos Calvo Muñoz
Tutor

RANDY GERARDO MORALES MORERA (FIRMA)
Digitally signed by RANDY GERARDO MORALES MORERA (FIRMA)
Date: 2022.08.23 17:35:28 -06'00'

MSEG. Randy Morales Morera
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2022.08.24 21:54:25 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 18 agosto de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Tabla de Contenido

Tabla de tablas

Tabla de ilustraciones

Capítulo 1: Introducción

1.1 Antecedentes del problema

El instituto Ponemon en conjunto con IBM, en su reporte “Cost of a Data Breach” del 2020 indican que, en promedio, una organización puede tardar hasta 280 días en detectar una brecha de seguridad y un total de 315 en detectar y contener la brecha de seguridad. Estos números pueden variar entre diferentes empresas, nichos de negocios y región. Se tiene un promedio global de 207 días para la identificación del incidente y otros 73 días para contener y remediar el incidente, esto para un promedio global de 280 días (IBM, 2020).

Las organizaciones deben cambiar la mentalidad de “si me vulneran” a pensar más bien en “cuando me vulneren”. Pensar en cómo detectar, contener y erradicar un incidente de seguridad proactivamente, es la diferencia entre una organización correctamente preparada y las que no. De los números indicados por IBM en el reporte mencionado anteriormente, es claro que la identificación temprana de un incidente es crucial. Organizaciones grandes a nivel mundial se han visto vulneradas por algún tipo de ataque cibernético, por este motivo la creación de un sistema que permita alertar de manera oportuna y con un alto nivel de confianza es crucial para poder responder ante un incidente de seguridad. La utilización de sistemas honeypots que permitan alertar comportamientos sospechosos dentro de las empresas, podría reducir los días que le toma a una organización detectar, contener y erradicar una brecha de seguridad.

1.2 Definición y Descripción del Problema

Actualmente las organizaciones a nivel mundial cuentan con una amplia gama de productos especializados para la detección y alertamiento de actividades sospechosas. Si bien es cierto, esto es lo ideal y lo que toda organización desea, también tiene sus problemas: a mayor cantidad de información, mayor tiempo va a tomar analizarla y poder tomar una decisión. Aunado a la cantidad de falsos positivos que un sistema de monitoreo tipo SIEM pueda llegar a generar, muchas veces un ataque real puede pasar desapercibido. Cuando se está constantemente monitoreando un equipo que es altamente usado, puede ser más complejo detectar actividades sospechosas.

No importa que tan efectivas sean las políticas y equipos de seguridad, eventualmente, y ante el ataque constante de un adversario, estos controles pueden fallar. El objetivo principal de un atacante no es simplemente obtener acceso a la red de una organización. Los atacantes tienen objetivos que van más allá de obtener acceso a una o más computadoras de la organización, es por este motivo que las organizaciones no pierden esta batalla una vez que un adversario logra entrar a su red de computadoras, esta batalla se pierde una vez que se filtran datos confidenciales de la organización. (Sanders, C. 2020)

1.3 Justificación

Según IBM (2020), el 80% de las brechas de seguridad en donde algún tipo de registro con información personal identificable (Personal Identifiable Information, PII) tiene un costo para la organización de $150 por cada registro fugado. De igual manera se estima un costo total, por cada brecha de seguridad, de $5.52 millones, en empresas de más de 25,000 empleados; y de $2.64 millones para organizaciones con menos de 500 colaboradores.

El uso de herramientas de automatización para la reducción de los días que toma detectar y contener una brecha de seguridad permite reducir y mitigar el daño que pueden sufrir las organizaciones. Según IBM (2020), en un ambiente completamente automatizado, el tiempo total de identificación, contención y erradicación puede pasar de 308 a 234 días. Y en ambientes semi automatizados el tiempo se puede reducir a 275 días.

Por otra parte, IBM (2021) menciona un incremento en el total de días que le toma a una organización detectar y remediar/contener un incidente de seguridad. Para el año 2020 el

promedio era de 280 días. Para el 2021 ese número se incrementó en siete días, para un promedio total de 287 días.

1.5 Objetivos

Para la definición de los objetivos, se utiliza la taxonomía de Benjamin Bloom de 1956, la cual, a través de los años, ha demostrado ser de las más confiables.

1.5.1 Objetivo General

Generar una extensión para la identificación y análisis de intrusiones cibernéticas mediante la utilización de un sistema Honeypot interno integrándose con una plataforma SIEM gratuita.

1.5.2 Objetivos Específicos

- Definir las plataformas honeypot y SIEM a utilizar, que se ajusten a las necesidades del proyecto.
- Realizar la instalación y configurar el servicio de honeypot.
- Elaborar la integración de la plataforma honeypot con el sistema SIEM.
- Crear las reglas de correlación para la detección de intrusiones dentro de una red interna de computadoras.
- Evaluar los resultados obtenidos.
- Optimizar las reglas para una mejor detección y notificación de posibles intrusiones a una red interna de computadoras.
- Crear un paquete o extensión que contenga toda la lógica para la detección de intrusiones dentro de una red interna de computadoras.

1.6 Alcances y Limitaciones

1.6.1 Alcances

El desarrollo de este proyecto tiene como objetivo la detección y análisis de ataques cibernéticos por medio del manejo de sistemas honeypot. Por motivos de tiempo y a modo de prueba de concepto, se pretende utilizar los siguientes servicios o puertos dentro de los sistemas honeypot:

- SSH - Puerto 22
- Web - Puerto 80
- Telnet - Puerto 23
- FTP - Puerto 21

1.6.2 Limitaciones

La detección y análisis de intrusiones cibernéticas se circunscribe a los puertos detallados en el apartado de alcances. Debido a la gran cantidad de plataformas SIEM que existen hoy en día y el tiempo limitado para completar el trabajo, el proyecto está limitado a la utilización de la plataforma IBM QRadar®, ya que cuenta con una versión gratuita (Community Edition) y Gartner ha colocado a esta herramienta dentro del cuadrante de líderes a nivel de plataformas SIEM (Gartner_Inc., 2020).

Capítulo 2: Marco Conceptual

2.1 Honeypot

Según Spitzner, L (2003) en su libro *Honeypots; Tracking Hackers*, define un honeypot como “un recurso de seguridad cuyo valor radica en ser investigado, atacado o comprometido”. Un Honeypot no provee ningún tipo de función principal para el negocio, ni cuenta con información de clientes ni de la compañía ni mucho menos confidencial. Generalmente, un honeypot está inactivo la mayor cantidad de tiempo, lo cual permite que cualquier tipo de interacción con el mismo pueda ser considerada como sospechosa. (Sanders, C. 2020)

Existen tres tipos principales de honeypots: honey systems, honey services, honey tokens.

Un honey system imita la interacción de un sistema operativo y los servicios que provee. Por ejemplo, un sistema utilizando Windows 10 puede actuar como un honey system (Sanders, C. 2020).

Un honey service imita la interacción con un servicio o protocolo específico. Por ejemplo, un servicio de SSH (Secure Shell Protocol) puede ser utilizado para la creación de un honey service (Sanders, C. 2020).

Un honey token imita o simula información legítima. Por ejemplo, un archivo con información falsa de clientes o de la organización, la cual pueda ser usada para atraer la atención de un atacante (Sanders, C. 2020).

Para su correcta implementación, un honeypot debe ser engañoso (deceptive), descubrible (discoverable), interactivo (interactive) y monitoreado (monitored).

2.1.1 Engañoso

El engaño es una distorsión ventajosa de la realidad percibida. (Bell, J. B. 2017) Los honeypots deben presentar alguna forma de falsa realidad. Deben aparentar ser sistemas o servicios o información real, no tienen un propósito fundamental para la organización o el negocio (Sanders, C. 2020).

2.1.2 Descubrible

Si bien es cierto, nadie debería interactuar intencional o legítimamente con un honeypot, estos sistemas deben ser colocados en lugares estratégicos de la red para que puedan ser accedidos en el contexto adecuado. De hecho, el lugar de la red en donde se coloque un honeypot define su funcionalidad primordial. Si un honeypot se configura con acceso desde internet, es muy probable que el mismo sea accedido por escáneres de Internet, bots, etc. Este tipo de honeypot cumpliría un propósito distinto al colocado dentro de una red privada de computadoras. Un honeypot con acceso a Internet permitiría recopilar información de posibles atacantes como IPs, técnicas y tácticas y van a contar con un alto grado de interacción. Por otra parte, si se coloca dentro de la red privada, la interacción con este tipo de sistemas debería de ser mínima o nula, lo cual permite un monitoreo más detallado y reducir los falsos positivos, ya que ningún empleado o plataforma tiene una razón de negocio para interactuar con estos sistemas (Sanders, C. 2020).

2.1.3 Interactivo

El éxito de la misión de un atacante depende de su capacidad para sondear su entorno y aumentar iterativamente su nivel de acceso en pos de un objetivo. Los atacantes confían en el descubrimiento de dispositivos, servicios y datos para que esto suceda.

A pesar de que un honeypot no es una versión real de lo que representa, debería de por lo menos aparentar de esta manera ante un atacante. Un honeypot debe ser interactivo y emitir algún tipo de respuesta ante el estímulo de un atacante para obtener el mayor provecho de este tipo de sistemas (Sanders, C. 2020).

2.1.4 Monitoreado

El aspecto principal de un honeypot es la capacidad de ser monitoreado de manera oportuna y correcta. Sería de poca ayuda tener un honeypot y no poder alertar sobre las interacciones que se estén realizando sobre estos sistemas. Si bien puede que no sea posible registrar todos los comandos emitidos en todos los servidores de una red es posible hacerlo en un honeypot porque el volumen de interacción debe ser bajo o inexistente. (Sanders, C. 2020)

2.1.5 Caso de uso

Existen muchos aplicativos que permiten instalar un sistema honeypot. Existen sistemas que permiten similar un Manejador con Contenido tipo WordPress, simular una base datos o un servicio de red específico (Borges, E. 2021). Si bien estos softwares cuentan con un gran potencial para la detección de una brecha de seguridad, existen otras soluciones un poco más integrales que permiten simular varios servicios de red y hasta aplicaciones. OpenCanary es un proyecto Open Source que permite ejecutar servicios, que activan alertas cuando se usan. Las alertas se pueden enviar a una variedad de fuentes, incluyendo syslog y correos electrónicos. OpenCanary es escalable lo que permite hacerlo crecer junto con las necesidades cambiantes de las organizaciones (OpenCanary. 2018).

2.1.6 OpenCanary

En esencia, OpenCanary crea un honeypot de red que le permite atrapar a los atacantes antes de que comprometan completamente sus sistemas. Como definición técnica, OpenCanary es un demonio (daemon) que ejecuta varias versiones de servicios que alerta cuando un servicio es usado (OpenCanary. 2018).

Por su fácil implementación, escalabilidad, diversidad de servicios (honey services) y ser libre y gratuito, se utilizará OpenCanary como servicio de honeypot para la realización de este proyecto.

2.2 SIEM

La tecnología de gestión de eventos e información de seguridad (SIEM) permite la detección de amenazas, el cumplimiento y la gestión de incidentes de seguridad mediante la recopilación y el análisis, tanto en tiempo real como histórico, de eventos de seguridad. Las capacidades principales son un amplio alcance de recopilación y gestión de eventos de registro, la capacidad de analizar eventos de registro y otros datos en fuentes dispares y capacidades operativas, como gestión de incidentes, paneles de control e informes (Gartner_Inc. s.f.).

2.2.1 Caso de uso

Los sistemas SIEM poseen la capacidad de monitorear las redes de computadoras, desde un punto de vista de seguridad. Pero estos sistemas dependen de la calidad de las

fuentes de información que consume y, también, de la correcta implementación y configuración de la herramienta. Muchas veces las alertas generadas por estos sistemas pasan desapercibidas, en muchas ocasiones derivado de la alta cantidad de alertas y falsos positivos que se generan.

Empleando sistemas honey (honeypots) de baja o nula utilización e integrando los logs que esta herramienta genera con un SIEM, permitiría la detección de posibles intrusiones y/o actividades sospechosas de una manera más certera y precisa.

2.2.2 IBM QRadar®

La compañía Gartner, en su análisis de plataformas SIEM del 2020 coloca a IBM QRadar® dentro del cuadrante de líderes a nivel mundial. (Gartner_Inc. 2020)

Por otra parte, IBM hizo pública la versión gratuita de QRadar® (Community Edition) para poder realizar pruebas, experimentar y desarrollar casos de uso sobre esta plataforma, sin ningún costo adicional. Esta plataforma cuenta con una licencia permanente de hasta 50 eventos por segundo, lo cual permite a pequeñas y medianas empresas implementar esta solución sin tener que incurrir en altos costos de instalación y equipo. Por estos motivos, se seleccionó a IBM QRadar® CE como la plataforma SIEM para el desarrollo de la solución propuesta en este trabajo.

En la Ilustración 1, se evidencia la calificación otorgada por la empresa Gartner a los sistemas tipo SIEM. En el cuadrante superior derecho se encuentran los líderes en este tipo de soluciones.

Ilustración 1

Tabla de Gartner referente a sistemas SIEM.

2.4 Sistema Operativo

Un sistema operativo es un programa que controla la ejecución de las aplicaciones y programas. Actúa como una interfaz entre las aplicaciones (software) y los componentes físicos (hardware) del computador. Un sistema operativo tiene los siguientes tres objetivos:

- **Facilidad de uso**: Facilita el uso de un computador.
- **Eficiencia**: Permite que los recursos de un sistema de computación se puedan utilizar de manera eficiente.

- **Capacidad para evolucionar**: Debe permitir el desarrollo, las pruebas y la implementación de nuevas funciones en el sistema, sin interferir con su funcionalidad normal (Stallings, W. 2012).

2.4.1 Kali Linux

Kali Linux es un sistema operativo de código libre y gratuito, enfocado en tareas relacionadas con seguridad de la información. Dentro de las áreas de especialización de este sistema operativo están las pruebas de penetración, investigación de ciberseguridad, computación forense e ingeniería reversa.

Otra gran ventaja de este sistema operativo es que se puede utilizar de diferentes maneras. Se puede instalar en una máquina virtual, dentro de un contenedor, ejecutar desde un dispositivo USB (Live boot) y también soporta los procesadores ARM, como los encontrados en minicomputadoras. Para descargar esta herramienta se puede utilizar el siguiente enlace: https://www.kali.org/get-kali/

2.4.2 Caso de uso

Para la realización de este proyecto, se pretende utilizar Kali Linux dentro de un minicomputador y ejecutar el software honeypot. La implementación de una computadora de tamaño compacto permite incluir portabilidad a la solución y reducir los costos asociados con la adquisición de equipo de cómputo. Al seleccionar un sistema operativo diseñado para realizar tareas de seguridad, la configuración e instalación de herramientas se reduce considerablemente, ya que este sistema operativo cuenta con muchas de las herramientas necesarias para la elaboración de este proyecto.

2.5 Infraestructura física

Para la infraestructura o equipos físicos, se necesita de dos servidores: uno para la herramienta QRadar® y otro para ejecutar el software de honeypots, OpenCanary.

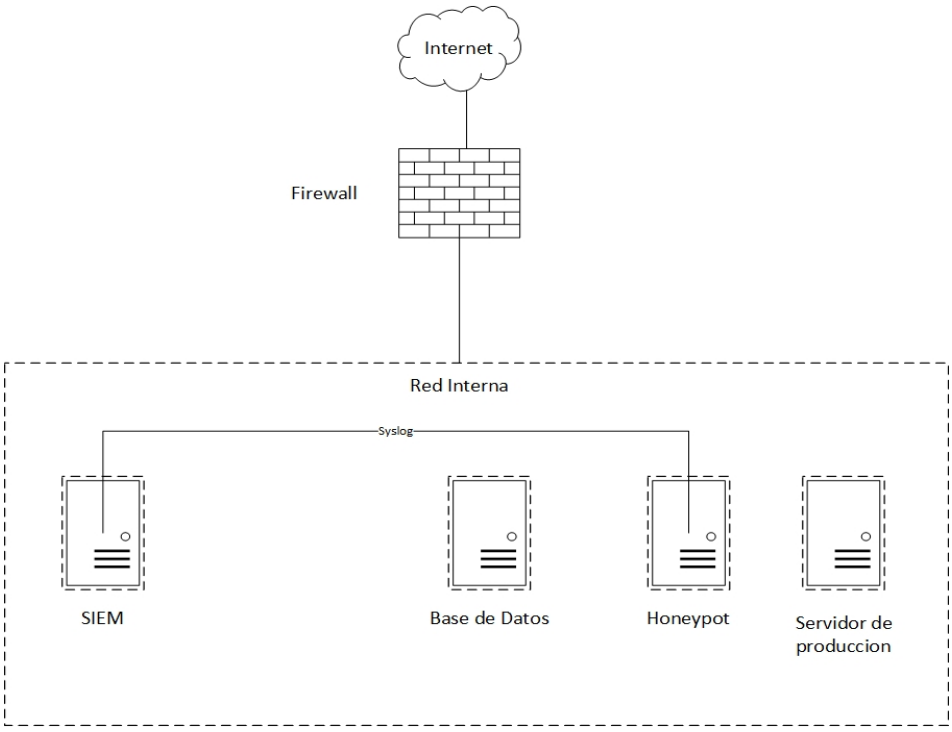
Para la plataforma de QRadar® se debe instalar en un virtualizador de computadores tipo VMWare o VirtualBox. Este sistema viene en formato .ova, el cual es una máquina virtual preconfigurada con todo lo que se necesita para su instalación. La descarga se puede realizar por medio del siguiente enlace: https://www.ibm.com/community/qradar/ce/

Por último, se debe instalar el sistema OpenCanary en una máquina virtual. Este sería el servidor que nos va a permitir detectar y reportar cualquier interacción que exista entre el servidor honey y cualquier otro computador.

En la ilustración 2 se detalla el diagrama de red para la correcta implementación del sistema honeypot y la integración con la plataforma SIEM.

Ilustración 2

Arquitectura propuesta de la solución.



2.5.1 Raspberry Pi

Raspberry Pi es una computadora de bajo costo, alto rendimiento y tamaño reducido, utilizada para aprender y resolver problemas. Para desarrollar este proyecto se va a utilizar el último modelo Raspberry Pi 4, el cual cuenta con un procesador de 1.6GHz de 64 bits y 4 núcleos, chip de red inalámbrica, Bluetooth y 4 GB de memoria RAM.

Los dispositivos de este tipo utilizan una arquitectura distinta a las computadoras de escritorio o portátiles. Los procesadores conocidos como ARM están basados en la arquitectura RISC (reduced instruction set computer) y es muy utilizada por sistemas IoT por su pequeño tamaño (Raspberry Pi Foundation, 2021).

2.5.2 Caso de uso

Estos equipos de bajo costo y tamaño reducido facilitan la instalación de sistemas de una manera fácil y económica. Su costo bajo y su portabilidad permiten la instalación de un sistema honeypot que puede ser portátil y fácilmente colocado en cualquier parte de una red de computadoras, sin tener que pensar en espacio específico para equipos de gran tamaño ni un costo elevado de adquisición.

Para la realización de este proyecto, el Raspberry Pi se usará con Kali Linux como sistema operativo y OpenCanary como sistema de honeypot.

Capítulo 3: Implementación de infraestructura

En el siguiente capítulo se pretende explicar la instalación y configuración de las herramientas a utilizar. Debido a la complejidad en la instalación e implementación de los sistemas a manipular, se pretende realizar una descripción detallada de los pasos requeridos para la correcta implementación de la solución propuesta.

3.1 Instalación del Sistema Operativo

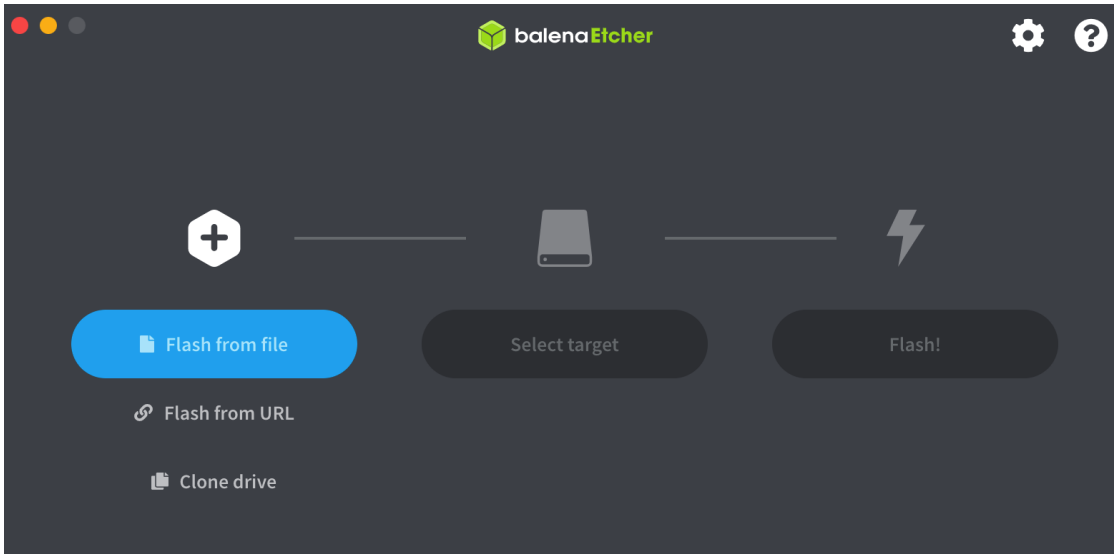
Para la instalación de OpenCanary se va a utilizar Kali Linux como sistema operativo. Para la instalación de Kali Linux en el Raspberry Pi se debe utilizar las versiones para ARM de Kali Linux. La descarga se puede realizar por medio del siguiente enlace: https://www.kali.org/get-kali/#kali-arm

Este tipo de archivo debe ser copiado sobre la tarjeta SD del Raspberry Pi. Para esto se utiliza una herramienta dedicada para estas tareas llamada Etcher. Esta plataforma se puede descargar del siguiente enlace: https://www.balena.io/etcher/.

Una vez se tenga instalada la herramienta y la imagen de Kali Linux descargada, se debe de instalar en la tarjeta de almacenamiento, utilizando Etcher seleccionando la opción Flash from file. Desde aquí se debe de seleccionar la imagen de Kali Linux previamente descargada y el medio de almacenamiento donde se va a copiar la imagen, en este caso la SD se debe a utilizar dentro del Raspberry Pi:

Ilustración 3

Herramienta balena Etcher.



Para realizar la copia de imagen únicamente hace falta seleccionar la opción Flash. Una vez concluido este proceso, se puede insertar la tarjeta SD al Raspberry Pi y prender el computador. Una vez terminado el proceso de inicio por parte del sistema operativo se pueden utilizar las credenciales por defecto de este sistema, las cuales son las siguientes:

- Usuario: kali
- Contraseña: kali

3.2 Instalación de OpenCanary

Para la instalación de OpenCanary, se deben instalar las dependencias.

Para esto se deben de ejecutar los siguientes comandos:

$ sudo apt-get install python3-dev python3-pip python3-virtualenv python3-venv python3-scapy libssl-dev libpcap-dev

Una vez que se tienen instaladas las dependencias, se debe crear un ambiente virtualizado de Python dentro del servidor, para esto se deben ejecutar los siguientes comandos:

```
$ virtualenv env/

$ . env/bin/activate
```

Con el ambiente ya inicializado, se puede instalar OpenCanary, por medio del siguiente comando:

```
$ pip install opencanary
```

Para ejecutar la herramienta, se deben de ejecutar los siguientes comandos:

```
$ . env/bin/activate

$ opencanaryd --start
```

3.3 Instalación de QRadar® Community Edition

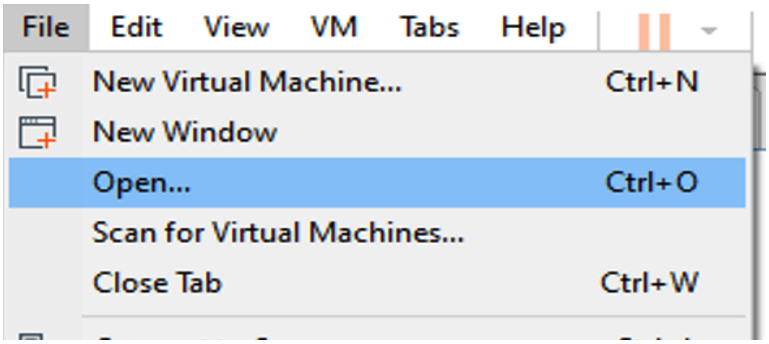
Para la instalación de la herramienta QRadar® Community Edition se debe de contar con un virtualizador (hypervisor) de computadoras. Para efectos del proyecto, se utilizará VMWare Workstation Pro 16. Este sistema permite el despliegue de la máquina virtual de QRadar® CE, la cual se descarga en formato .ova del siguiente enlace: https://www.ibm.com/community/qradar/ce/

Una vez descargada la máquina virtual, se debe realizar la instalación y configuración de QRadar®. A continuación, se detallan los pasos.

El primer paso en la instalación de QRadar® es importar la imagen del sistema. Para esto se usa el menú File y luego la opción Open:

Ilustración 4

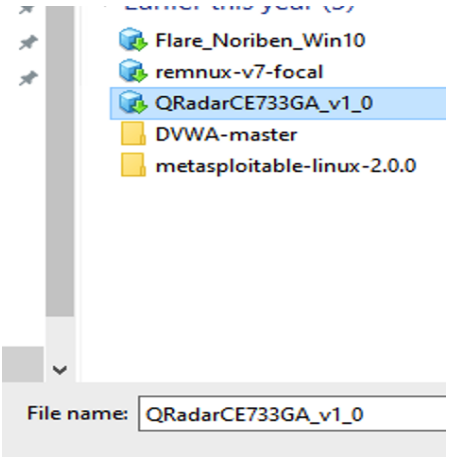
Abrir la máquina virtual.



Se debe seleccionar el archivo OVA descargado:

Ilustración 5

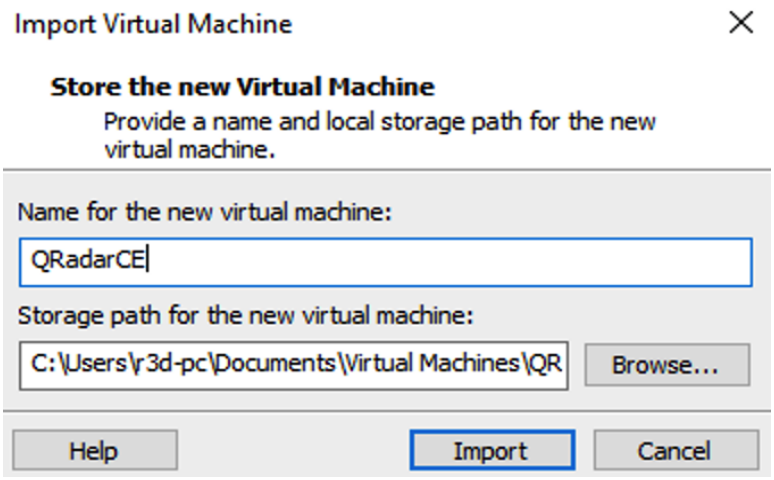
*Archivo OVA del QRadar® CE***.**



Luego de seleccionar la imagen correcta se debe de nombrar la máquina virtual y el lugar en donde se va a guardar el archivo:

Ilustración 6

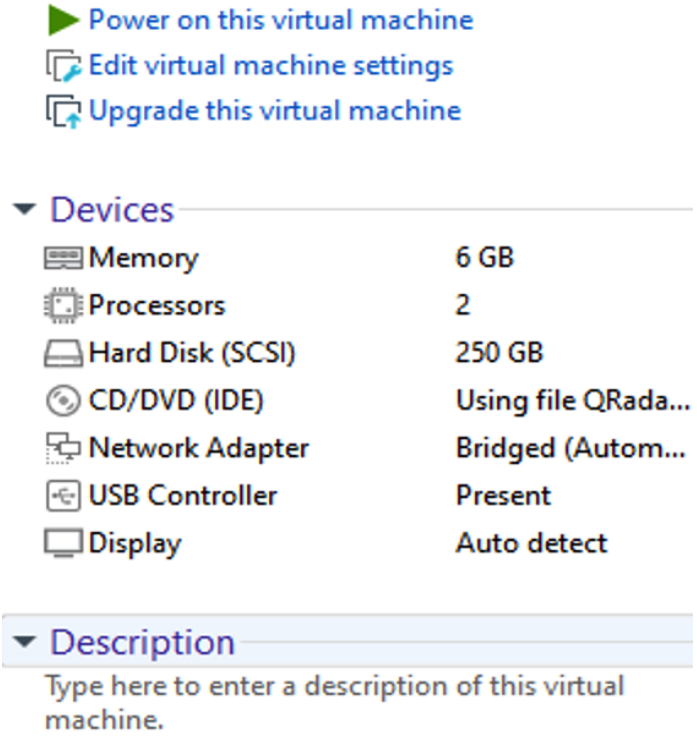
Importación del archivo OVA.



Una vez que la maquina se importa correctamente, se debe visualizar de la siguiente manera:

Ilustración 7

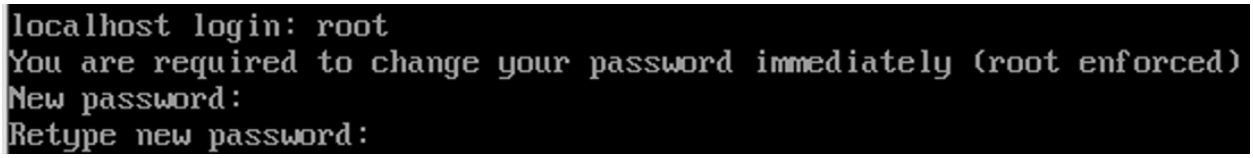
Configuraciones de la máquina virtual.



Luego de iniciar la máquina, utilizando el usuario root se debe realizar un cambio de contraseña:

Ilustración 8

Inicio de sesión en QRadar® CE.



Una vez que se logra entrar al sistema, sobre el directorio /root se puede ver el script llamado setup, el cual es el encargado de realizar todas las configuraciones para el correcto despliegue de QRadar®.

Ilustración 9

Listado de archivos de QRadar® CE.

La ejecución del script se realiza de la siguiente manera:

Ilustración 10

Archivo de instalación de QRadar® CE..

El proceso de instalación realizará verificaciones de licencias, las cuales deben ser aceptadas:

Ilustración 11

Licencia EULA.

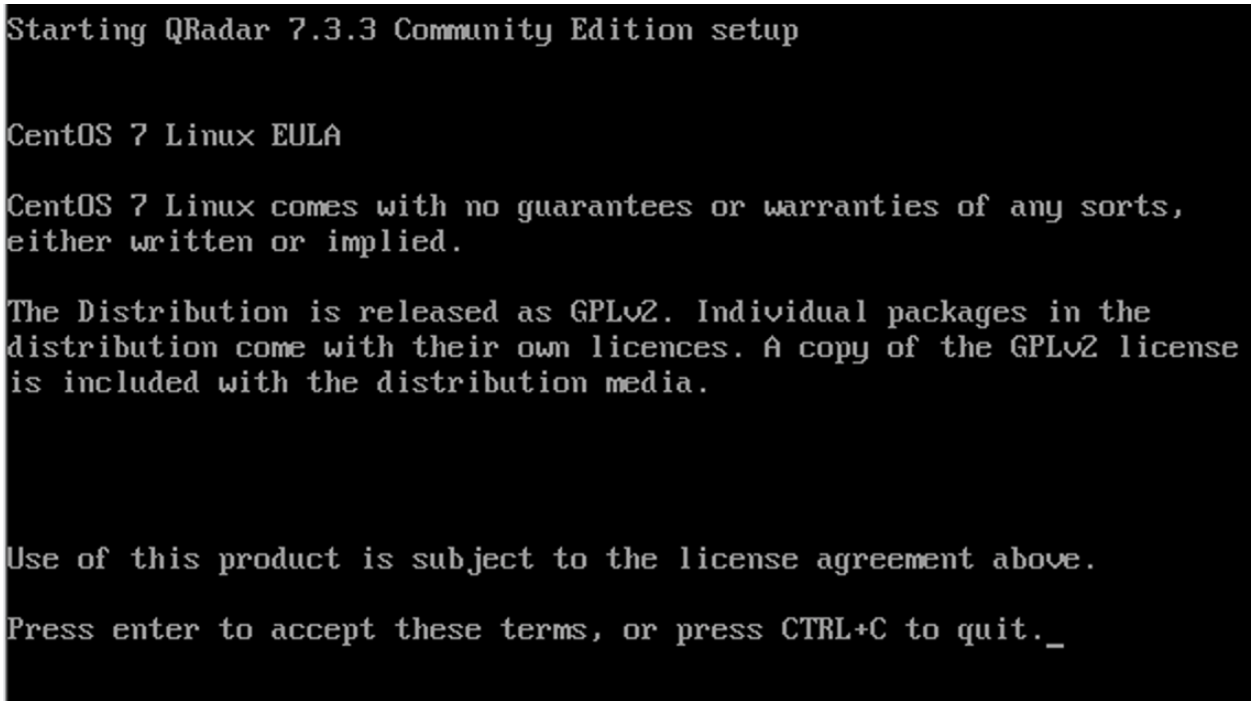
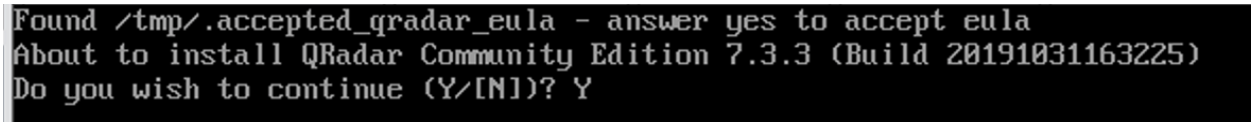


Ilustración 12

Aceptación de los términos y condiciones.

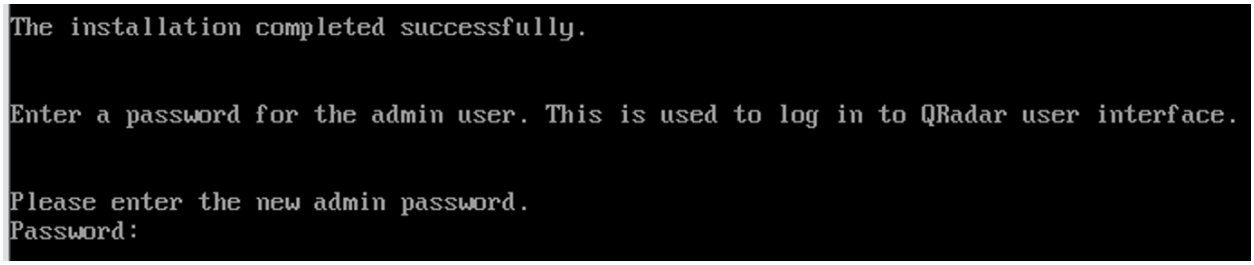


Luego de aceptar las licencias y términos de condiciones, el instalador realizará el proceso de instalación y configuración de la plataforma. Este proceso puede llegar a durar aproximadamente entre 45-60 minutos.

Una vez concluida la instalación, se debe de configurar la contraseña del usuario administrador de la interfaz web:

Ilustración 13

Configuración de contraseña para el usuario web.

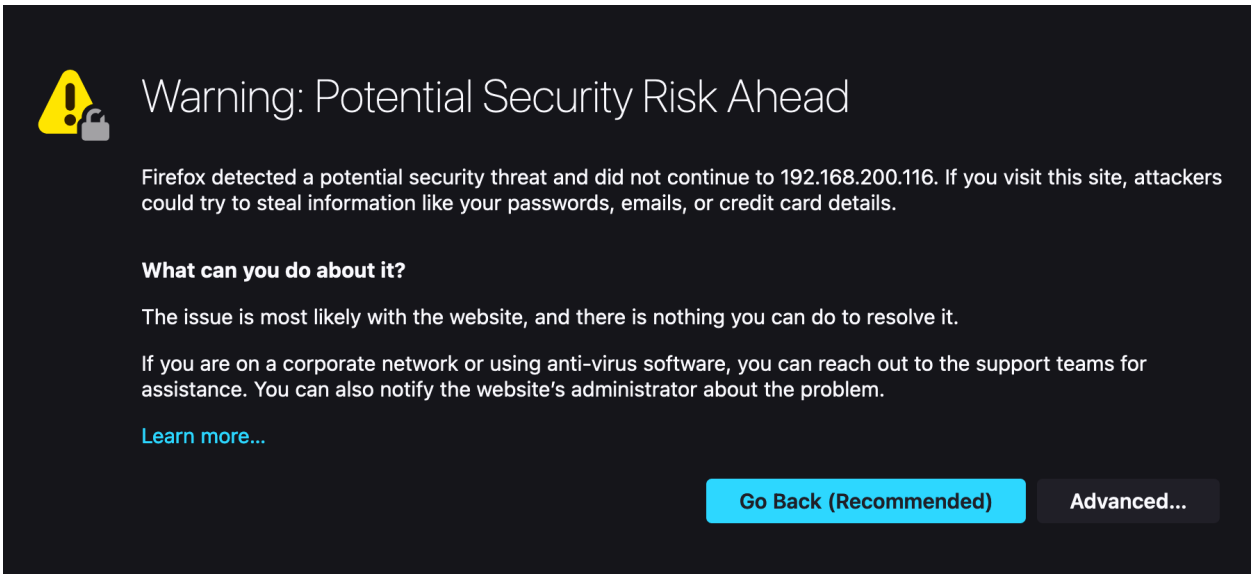


Con la instalación completa, el siguiente paso es ingresar por medio de la página web. Para esto se debe de utilizar la IP del sistema: https://<IP del SIEM>

La primera vez que se ingresa a la página web se presentará una alerta referente al certificado de seguridad auto generado. Para continuar se debe de aceptar esta notificación:

Ilustración 14

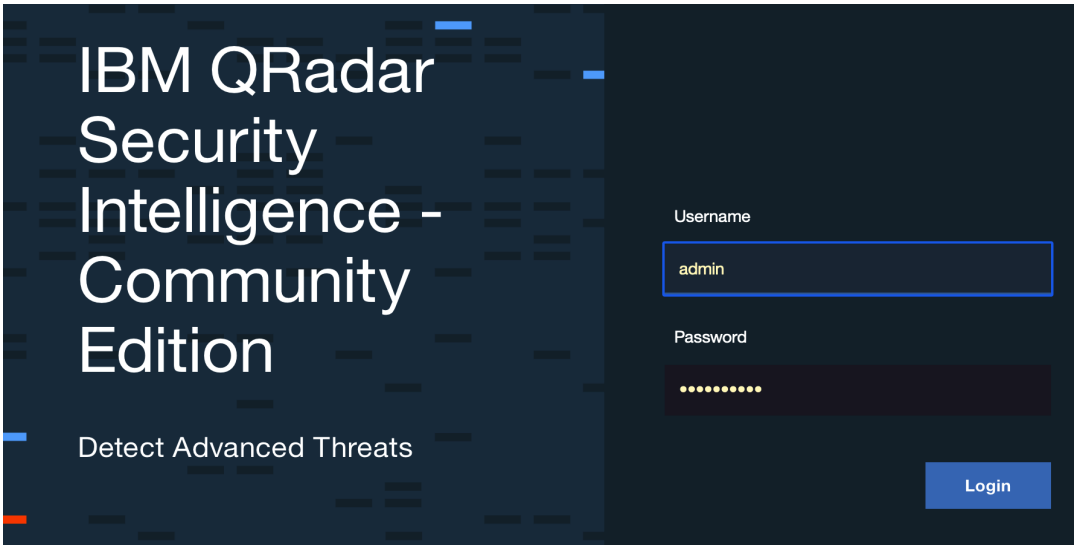
Mensaje de error de certificado SSL.



Para acceder a la interfaz web, se debe de utilizar el usuario admin y la contraseña configurada en pasos anteriores:

Ilustración 15

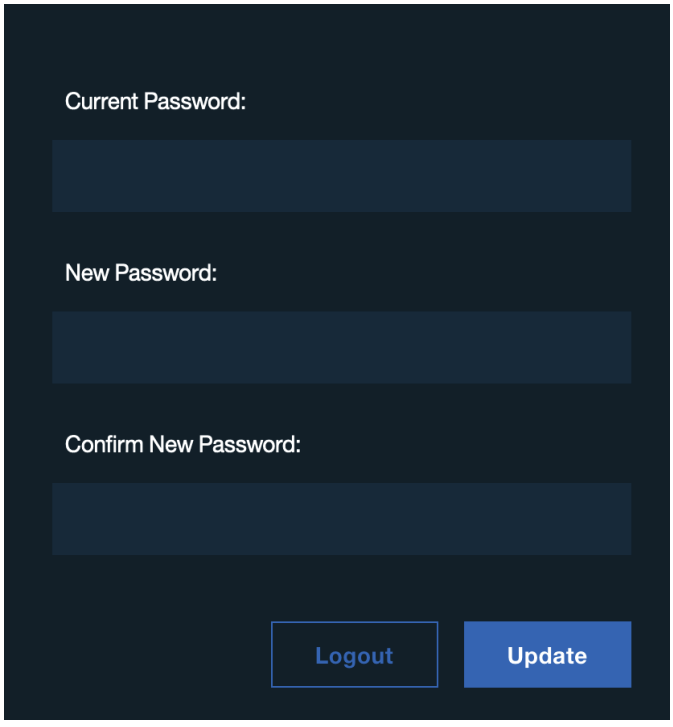
Interfaz web de QRadar®.



El sistema solicitará el cambio de contraseña. Se debe utilizar la contraseña actual y utilizar una contraseña nueva, la cual debe ser ingresada en dos campos:

Ilustración 16

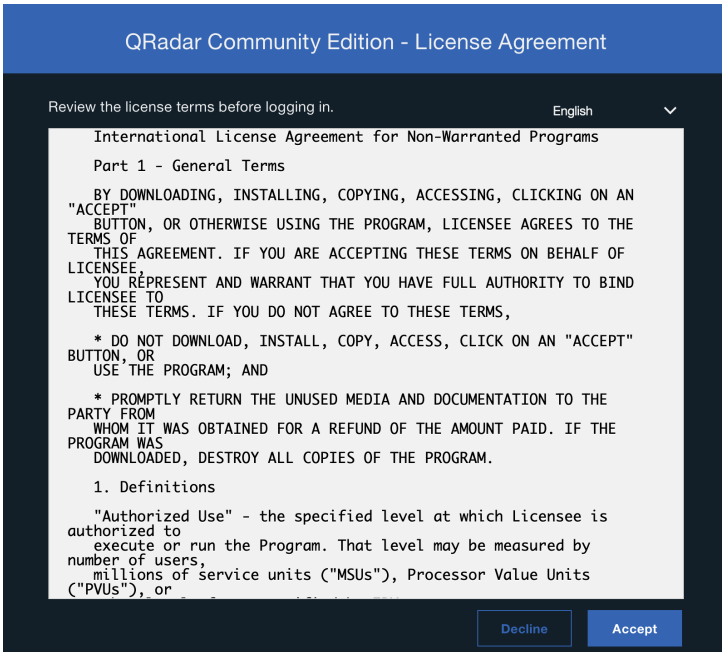
Cambio de contraseña usuario web.



Se presentará la licencia del sistema, la cual debe ser aceptada antes de poder usar la plataforma:

Ilustración 17

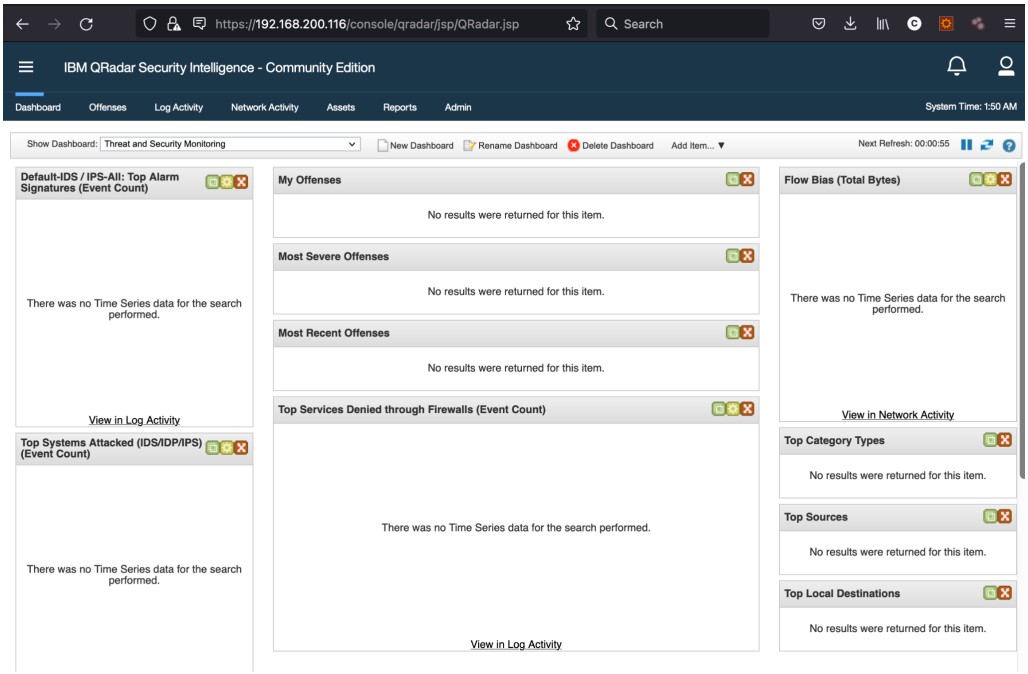
Aceptación de la licencia de QRadar®.



Una vez se completen estos pasos, el sistema podrá ser utilizado con normalidad:

Ilustración 18

Interfaz web de QRadar®.

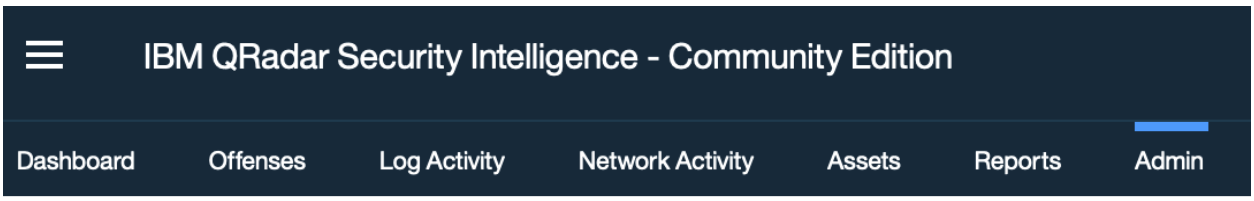


Debido a que se está utilizando una herramienta libre (Community Edition) ya preconfigurada, el espacio en disco es limitado (250GB). De ser requerido, se pueden enviar los logs a una solución centralizada de mayor espacio. Para esto se deben de realizar dos configuraciones: Routing rules y Forwarding Destinations, desde el admin tab:

Seleccionar el menú Admin:

Ilustración 19

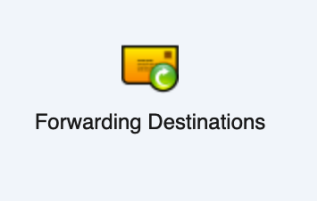
Menú QRadar®.



Primeramente, configurar el destino a donde se desean enviar los eventos desde el menú de Forwarding Destination:

Ilustración 20

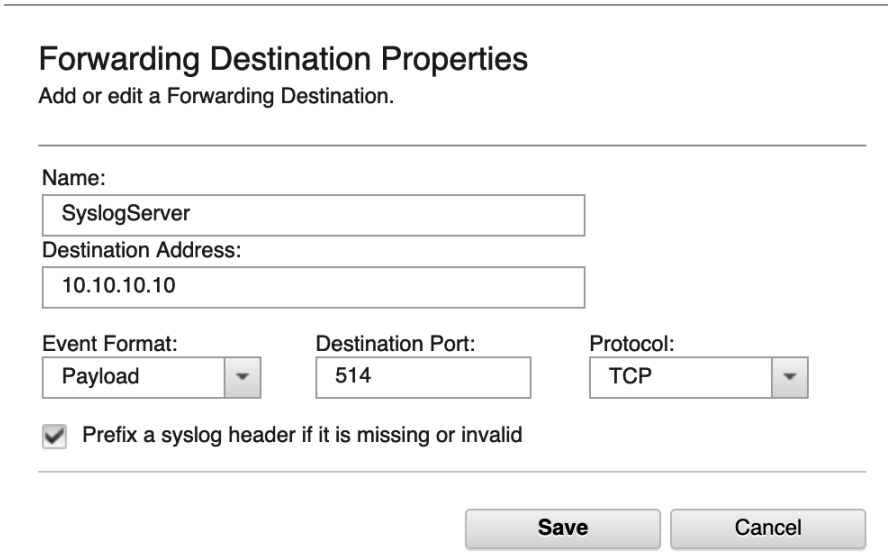
Destinos de reenvío de logs.



Ingresar la información necesaria como la IP del destino y asignarle un nombre:

Ilustración 21

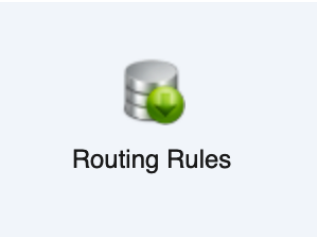
Configuración de los destinos de reenvío.



Una vez configurada esta opción, ingresar al menú de Routing Rules:

Ilustración 22

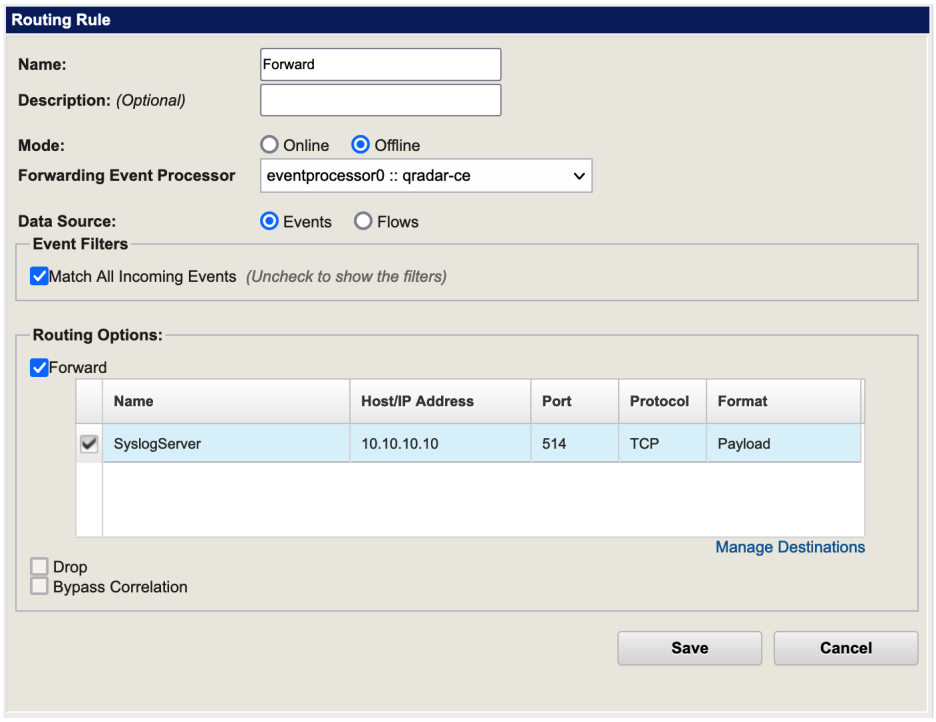
Reglas de enrutamiento para el reenvío de paquetes.



Desde esta opción se configura el reenvío de eventos al destino previamente configurado. Por motivos de rendimiento, se recomienda utilizar la opción de offline, para realizar el reenvío de eventos en el momento que el sistema tenga la capacidad de realizarlo.

Ilustración 23

Configuración de las reglas de reenvío.



Capítulo 4: Propuesta de solución

En el siguiente capítulo se explicará la solución propuesta y todas las configuraciones necesarias para integrar las plataformas anteriormente configuradas.

4.1 Integración de OpenCanary con QRadar®

Para la integración de OpenCanary con la plataforma SIEM primero se deben de configurar los servicios a utilizar y/o simular. Para esto, OpenCanary cuenta con un archivo de configuración localizado en /etc/opencanaryd/opencanary.conf.

Desde este archivo se configuran los servicios y puertos que el honeypot va a simular. Seguidamente se detallan las configuraciones para la solución de este proyecto:

"device.node_id": "opencanary-1",

"ftp.enabled": true,

"ftp.port": 21,

"ftp.banner": "FTP server ready",

"http.banner": "Apache/2.2.22 (Ubuntu)",

"http.enabled": true,

"http.port": 80,

"mysql.enabled": true,

"mysql.port": 3306,

"mysql.banner": "5.5.43-0ubuntu0.14.04.1",

"ssh.enabled": true,

"ssh.port": 22,

"ssh.version": "SSH-2.0-OpenSSH_5.1p1 Debian-4",

"telnet.enabled": true,

"snmp.enabled": true,

"snmp.port": 161,

"telnet.port": 23,

"telnet.banner": "",

"telnet.banner": "",

"telnet.honeycreds": [

{

"username": "admin",

"password": "$pbkdf2-sha512$19000$bG1NaY3xvjdGyBlj7N37Xw$dGrmBqqWa1okTCpN3QEmeo9j5DuV2u1EuVFD8Di0GxNiM64To5O/Y66f7UASvnQr8.LCzqTm6awC8Kj/aGKvwA"

},

{

"username": "admin",

"password": "admin1"

}

Para esta solución específica y a modo de prueba de concepto, los servicios configurados son:

- FTP
- Web (HTTP)
- MySQL
- SSH

- SNMP
- Telnet

4.1.1 Envío de logs a QRadar®

Una vez configurados los puertos y servicios a utilizar por la herramienta de OpenCanary, es necesario configurar el envío de estos logs a la plataforma SIEM para su análisis y detección automatizada. Si bien es cierto OpenCanary va a generar los eventos relacionados con el escaneo y enumeración de puertos, el SIEM es el encargado de generar las alertas necesarias para la detección de actividades sospechosas, posiblemente relacionada con brechas de seguridad. Esta configuración se realiza desde el mismo archivo: /etc/opencanaryd/opencanary.conf.

Dentro del apartado llamado Handlers se lleva a cabo la configuración:

```
"handlers": {
        "json-tcp": {
        "class": "opencanary.logger.SocketJSONHandler",
        "host": "<Ingresar IP del SIEM>",
        "port": 514
        },
        "console": {
        "class": "logging.StreamHandler",
        "stream": "ext://sys.stdout"
        },
        "file": {
        "class": "logging.FileHandler",
```

```
            "filename": "/var/tmp/opencanary.log"
        }
    }
```

Esta configuración envía los logs generados por OpenCanary, a través del protocolo de syslog (puerto 514), al SIEM. La plataforma de QRadar®, por defecto, no puede interpretar correctamente los logs de OpenCanary, ya que no son soportados por defecto en QRadar®. Para esto, los eventos deben ser indexados por medio de las utilidades propias del SIEM.

4.2 Interpretación de logs de OpenCanary en QRadar

Los logs de OpenCanar no son interpretados por defecto en QRadar. Esto imposibilita a la plataforma a utilizar estos eventos en la generación de ofensas, ya que al no poder interpretar los eventos correctamente no pueden pasar por lo motores de correlación y generación de ofensas propias de la herramienta.

Para solucionar este problema, QRadar® cuenta con una herramienta que permite interpretar correctamente los eventos que no sean identificados por defecto. Desde el menú de Admin, bajo la opción de DSM Editor, se puede crear la lógica, utilizando expresiones regulares, para ayudar a la plataforma en la interpretación de los eventos de QRadar®. Como se detalla a continuación, por defecto los logs de OpenCanary se visualizan de la siguiente manera:

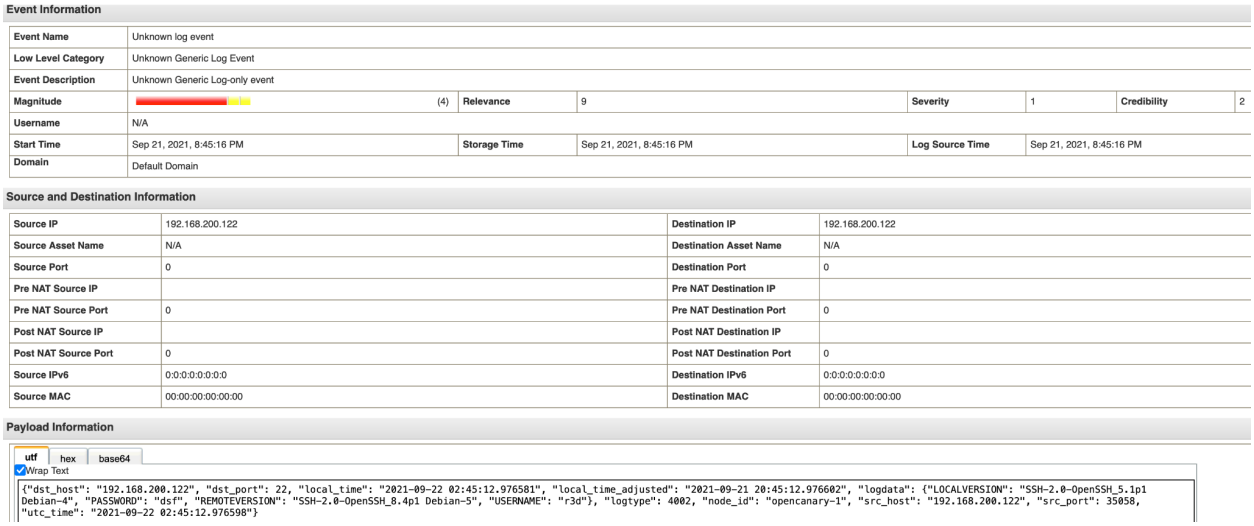
Ilustración 24

Eventos recibidos por QRadar®.

Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP
Unknown log event	SIM Generic Log DSM-7 :: qradar-ce	1	Sep 21, 2021, 8:45:16 PM	Unknown Generic Log Event	192.168.200.122	0	192.168.200.122
Unknown log event	SIM Generic Log DSM-7 :: qradar-ce	1	Sep 21, 2021, 8:45:14 PM	Unknown Generic Log Event	192.168.200.122	0	192.168.200.122
Unknown log event	SIM Generic Log DSM-7 :: qradar-ce	1	Sep 21, 2021, 8:45:12 PM	Unknown Generic Log Event	192.168.200.122	0	192.168.200.122
Unknown log event	SIM Generic Log DSM-7 :: qradar-ce	1	Sep 21, 2021, 8:45:10 PM	Unknown Generic Log Event	192.168.200.122	0	192.168.200.122
Unknown log event	SIM Generic Log DSM-7 :: qradar-ce	1	Sep 21, 2021, 8:45:08 PM	Unknown Generic Log Event	192.168.200.122	0	192.168.200.122
Unknown log event	SIM Generic Log DSM-7 :: qradar-ce	1	Sep 21, 2021, 8:45:04 PM	Unknown Generic Log Event	192.168.200.122	0	192.168.200.122

Ilustración 25

Detalle de los eventos recibidos por QRadar®.



Event Information

Event Name	Unknown log event						
Low Level Category	Unknown Generic Log Event						
Event Description	Unknown Generic Log-only event						
Magnitude	(4)	Relevance	9	Severity	1	Credibility	2
Username	N/A						
Start Time	Sep 21, 2021, 8:45:16 PM	Storage Time	Sep 21, 2021, 8:45:16 PM	Log Source Time	Sep 21, 2021, 8:45:16 PM		
Domain	Default Domain						

Source and Destination Information

Source IP	192.168.200.122	Destination IP	192.168.200.122
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf hex base64

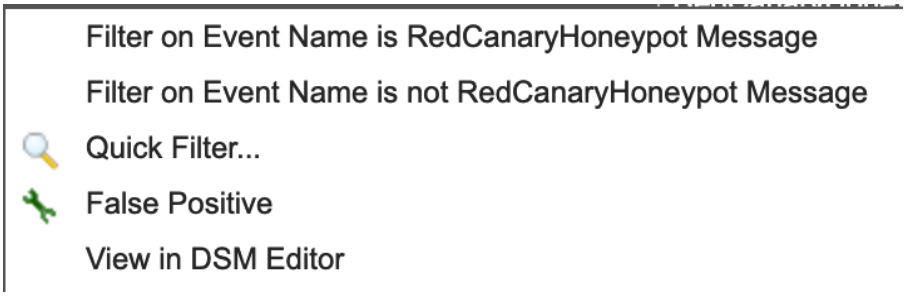
Wrap Text

{"dst_host": "192.168.200.122", "dst_port": 22, "local_time": "2021-09-22 02:45:12.976581", "local_time_adjusted": "2021-09-21 20:45:12.976602", "logdata": {"LOCALVERSION": "SSH-2.0-OpenSSH_5.1p1 Debian-4", "PASSWORD": "dsf", "REMOTEVERSION": "SSH-2.0-OpenSSH_8.4p1 Debian-5", "USERNAME": "r3d"}, "logtype": 4002, "node_id": "opencanary-1", "src_host": "192.168.200.122", "src_port": 35058, "utc_time": "2021-09-22 02:45:12.976598"}

Una vez que se identifiquen los logs de OpenCanary en QRadar®, desde el menú de Log Activity, se pueden seleccionar varios eventos, luego dar click derecho y seleccionar la opción de ver en el Editor de DSM:

Ilustración 26

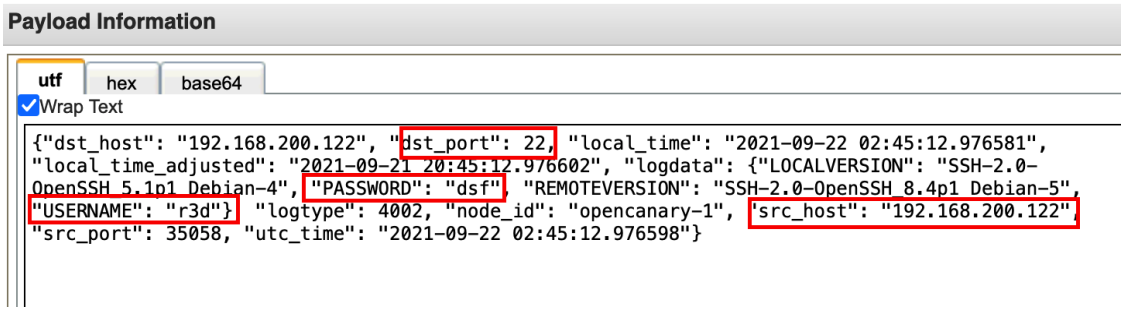
Filtros de búsqueda en QRadar®.



Dentro del DSM Editor se utilizan expresiones regulares para poder extraer la información relevante del payload del evento, como: IP origen, IP destino, puerto, entre otros. Algunos de los campos más relevantes se detallan a continuación:

Ilustración 27

Detalle del payload de los eventos en QRadar®.



Para realizar la extracción (parseo) de la información desde el editor de DSM se debe crear una fuente de información nueva (Log Source), para esto se puede utilizar el nombre de la herramienta, en este proyecto va a ser llamado OpenCanary.

Ilustración 28

Tipos de fuentes de información en QRadar®.

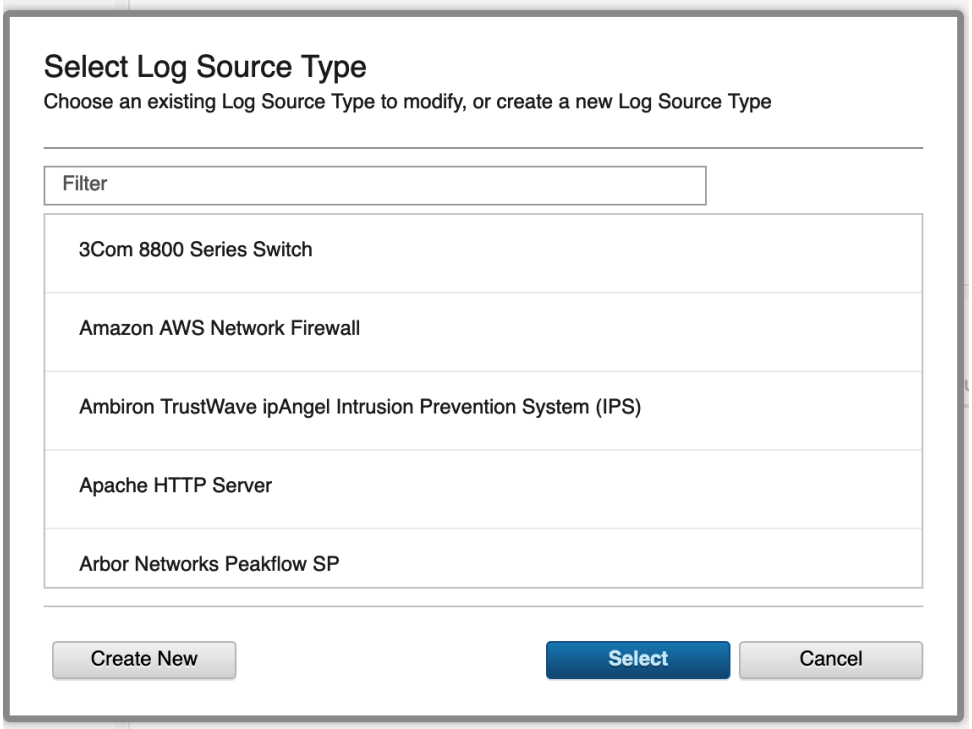
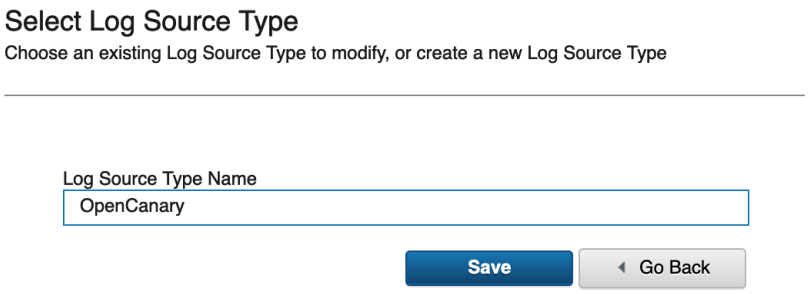


Ilustración 29

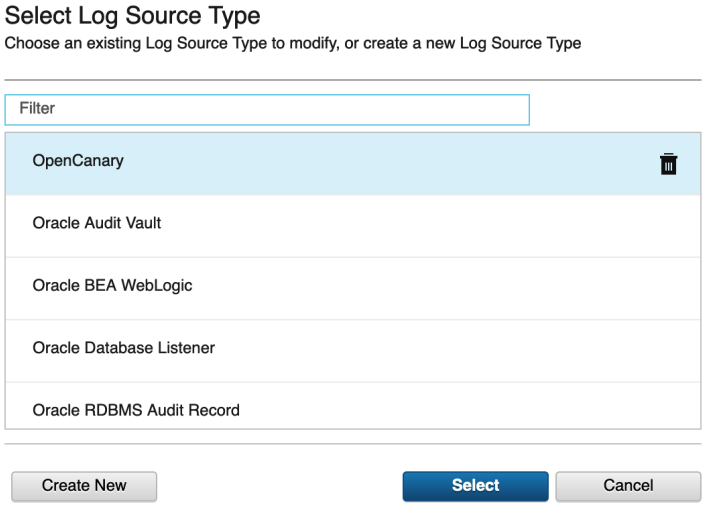
Nueva fuente de información en QRadar®.



Una vez creado, se debe de seleccionar la fuente:

Ilustración 30

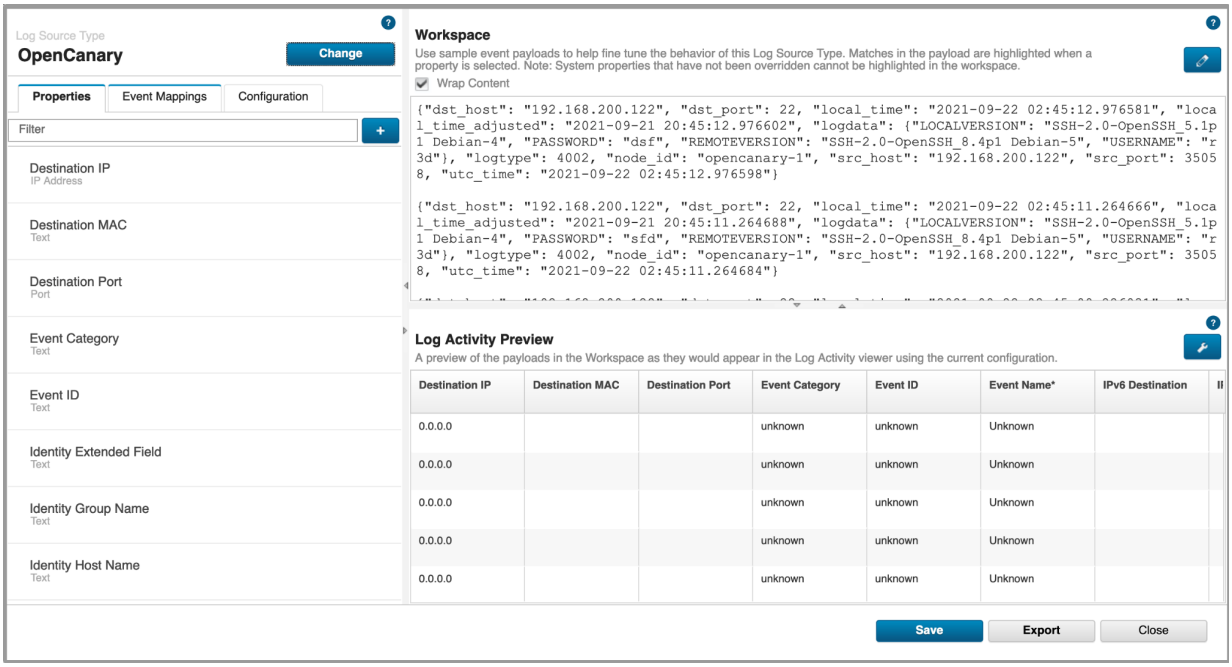
Selección de la fuente de información a utilizar.



Una vez que se selecciona la fuente deseada, QRadar® presenta una interfaz desde donde se debe realizar la indexación de la información.

Ilustración 31

Interfaz para el mapeo de los eventos en QRadar®.

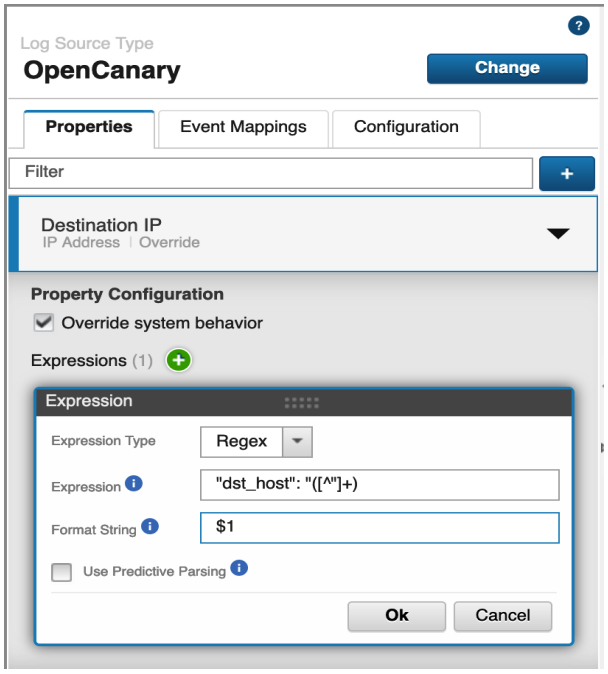


A modo de ejemplificación se detalla cómo realizar esta tarea para la IP de destino y el puerto destino. Para los demás campos se detalla la expresión regular y los pasos son los mismos para cualquier propiedad que desea ser extraída.

Para realizar la indexación de la IP de destino (Destination IP), se busca dicha propiedad utilizando el filtro de búsquedas. Una vez identificada se da clic sobre la propiedad. Dentro del menú desplegado se selecciona la opción de sobreescribir el comportamiento del sistema (Override system behavior). Dentro de la opción de expresión (Expression) se ingresa la expresión regular, en este caso se utilizará la siguiente: "dst_host": "([^"]+). Por último, en el campo de formato del texto (Format String) se debe especificar el campo a indexar, para esto se utiliza la sintaxis: $1; esto le indica a la herramienta que tiene que indexar el primer campo extraído utilizando la expresión regular.

Ilustración 32

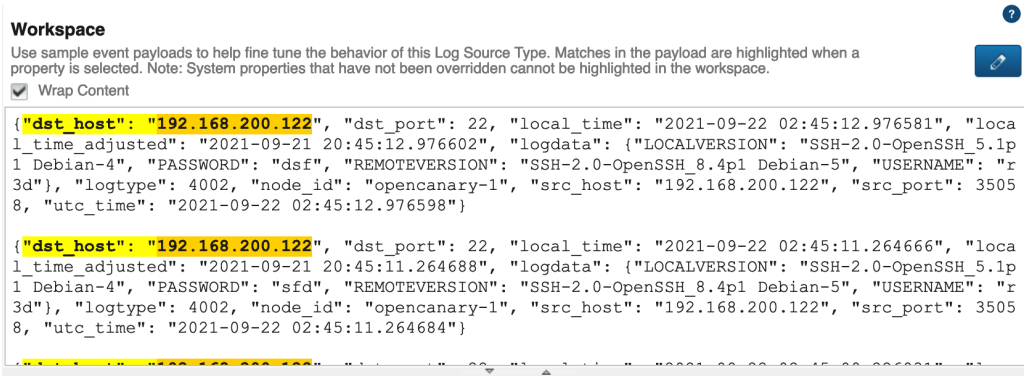
Mapeo de los eventos en QRadar®.



A medida que se va realizando esta configuración, la interfaz gráfica señala, con colores, el o los campos que la expresión regular extrae:

Ilustración 33

Resultado del mapeo utilizado en QRadar®.

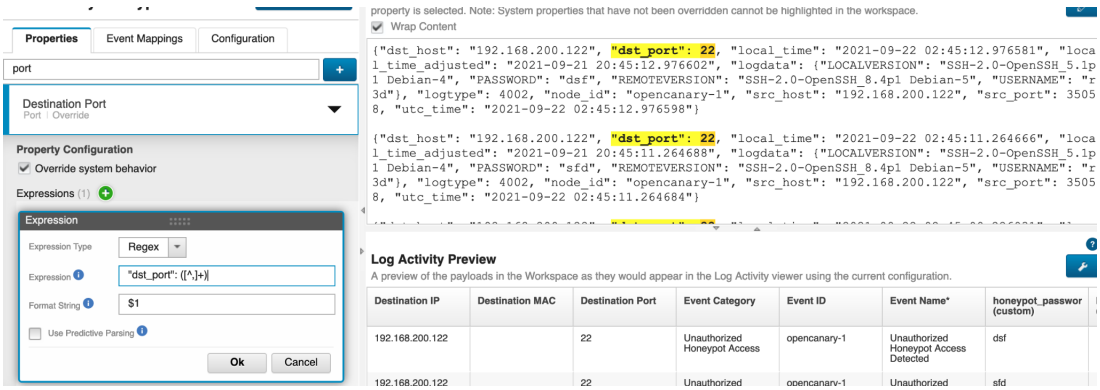


El color naranja detalla el campo extraído por la expresión regular ingresada en el campo Expresión.

Para el campo de Puerto destino, se siguen los mismos pasos detallados anteriormente, pero se utiliza la siguiente expresión regular: "dst_port": [\D]*([^\D]+).

Ilustración 34

Mapeo del campo Puerto Destino en QRadar®.



El resto de las expresiones regulares se detallan a continuación:

Tabla 1

Expresiones regulares de los campos a mapear en QRadar®.

Campo	Expresión regular
IP Destino	"dst_host": "([^"]+)
Puerto Destino	"dst_port": [\D]*([^\D]+)
Número de Evento (Event ID)	node_id": "([^"]+)
Event Category	Expression: () String Format: Acceso no autorizado a Honeypot
Contraseña (Password)	"PASSWORD": "([^"]+)
User Agent	"USERAGENT": "([^"]+)
IP Origen (Source IP)	"src_host": "([^"]+)
Puerto Origen (Source Port)	"src_port": [\D]*([^\D]+)
Usuario (Username)	"USERNAME": "([^"]+)

Una vez configuradas y extraídas las propiedades de los eventos de Opencanary, QRadar® se muestra la información relevante en la descripción del evento, como aparece en la siguiente imagen:

Ilustración 35

Eventos correctamente identificados por QRadar®.

Event Name	Log Source	Event Count	Start Time	Source IP	Source Port	Destination IP	Destination Port	honeypot_logtype (custom)
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	1	Oct 3, 2021, 12:02:28 AM	192.168.200.127	34562	192.168.200.122	23	6001
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	1	Oct 3, 2021, 12:02:24 AM	192.168.200.127	34562	192.168.200.122	23	6001
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	1	Oct 3, 2021, 12:02:21 AM	192.168.200.127	34562	192.168.200.122	23	6001
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	1	Oct 3, 2021, 12:02:17 AM	192.168.200.127	34562	192.168.200.122	23	6001
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	3	Oct 3, 2021, 12:00:39 AM	192.168.200.127	54123	192.168.200.122	22	4002
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	1	Oct 3, 2021, 12:00:36 AM	192.168.200.127	54122	192.168.200.122	22	4002
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	1	Oct 3, 2021, 12:00:35 AM	192.168.200.127	54122	192.168.200.122	22	4002
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	1	Oct 3, 2021, 12:00:32 AM	192.168.200.127	54122	192.168.200.122	22	4002
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	4	Oct 3, 2021, 12:00:30 AM	192.168.200.127	54123	192.168.200.122	22	4001
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	3	Oct 3, 2021, 12:00:03 AM	192.168.200.127	45648	192.168.200.122	80	3001
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ ...	2	Oct 2, 2021, 11:59:49 PM	192.168.200.127	45648	192.168.200.122	80	3001

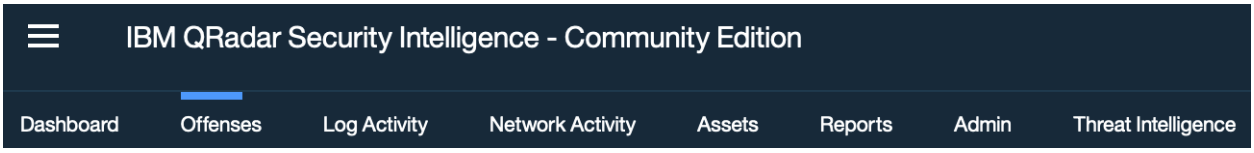
4.3 Creación de reglas

Una vez que los eventos de OpenCanary estén correctamente indexados, QRadar® puede generar alertas (Ofensas) basadas en dichos eventos. Este paso es fundamental, ya que permite poder realizar un monitoreo centralizado de las actividades detectadas por el SIEM. Como parte fundamental de los sistemas honey, el monitoreo es una de estas. La plataforma SIEM permite centralizar este monitoreo consumiendo los eventos del OpenCanary, indexando, correlacionando y generando alertas de seguridad que permitan identificar acciones posiblemente maliciosas.

QRadar® permite crear estas reglas por medio de una interfaz gráfica muy sencilla de usar. Desde el menú de Ofensas (Offenses) se selecciona la opción de reglas (Rules)

Ilustración 36

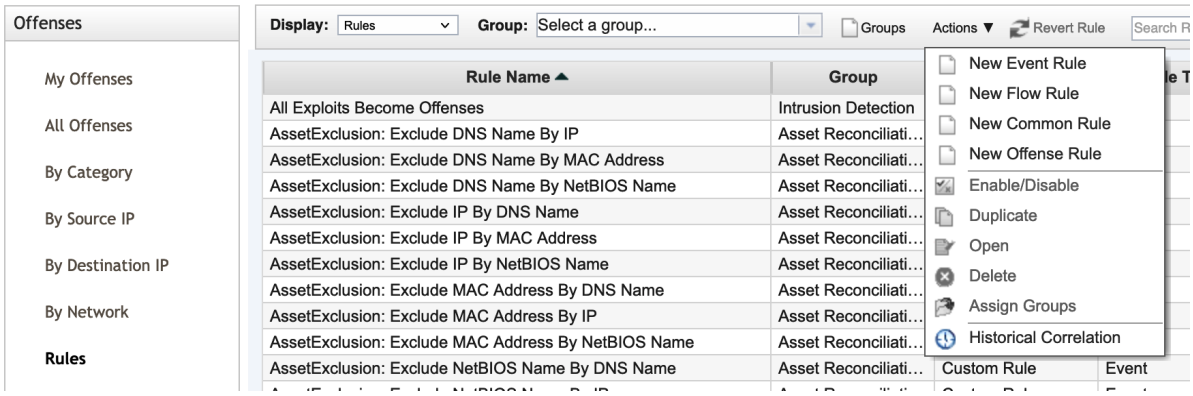
Menú de QRadar®.



Desde esta opción se selecciona el menú de acciones (Actions) y luego se crea una nueva regla de eventos (New Event Rule).

Ilustración 37

Menú para la creación de reglas en QRadar®.



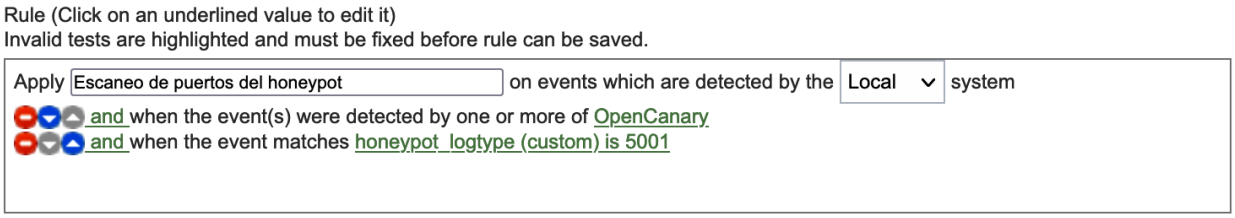
La interfaz para la creación de las reglas es bastante amigable con el usuario al igual que la creación de la lógica de la regla. Para este proyecto y a modo de prueba de concepto, se van a realizar reglas para tres casos de uso, los cuales son los siguientes:

1. Detección de escaneo de puertos sobre el honeypot
2. Fuerza bruta sobre los servicios del honeypot
3. Intento de conexión a la base de datos del honeypot

Para la creación de la regla se debe dar un nombre que permita identificarla seguido de la lógica, utilizando las opciones en la parte superior de la interfaz.

Ilustración 38

Definición de la lógica de las reglas en QRadar®.



Una vez que se tiene la lógica creada, se deben de configurar tres secciones más: acciones de la regla, respuestas de la regla y límites de la regla. Para este caso específico, estas fueron las configuraciones realizadas:

Ilustración 39

Acciones de las reglas.

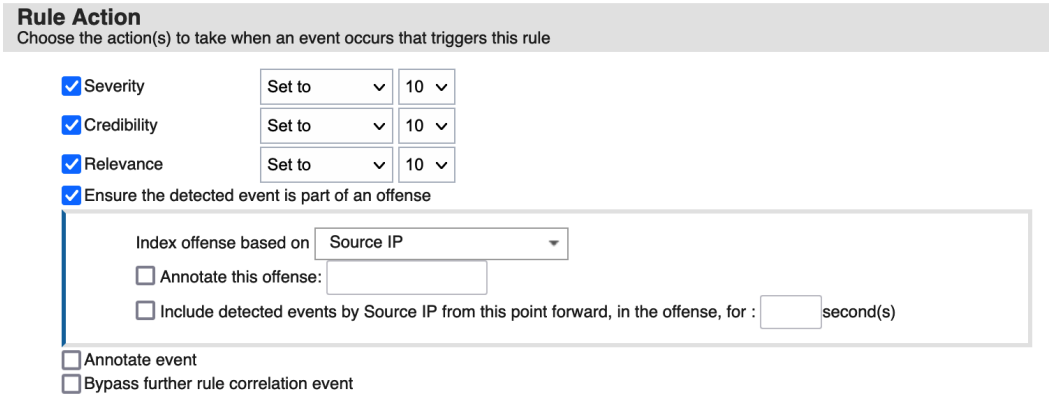


Ilustración 40

Respuesta a la reglas.

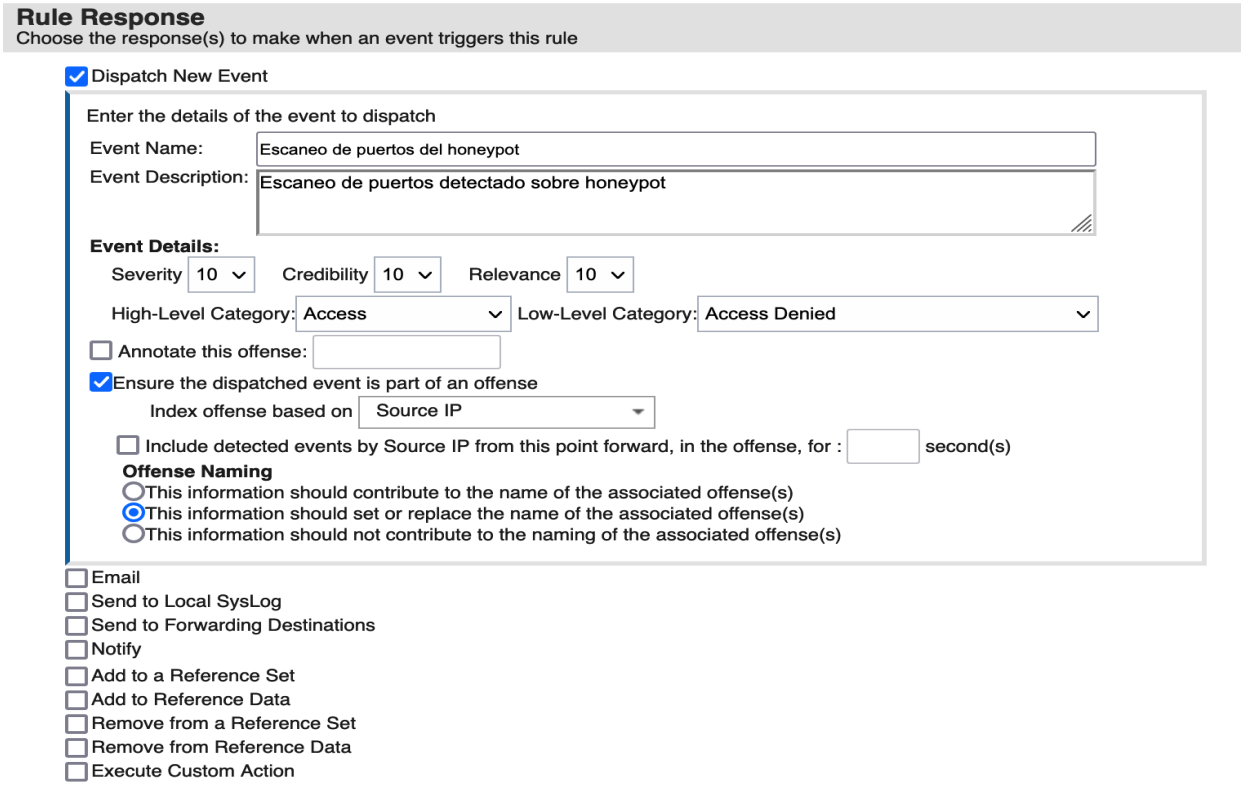


Ilustración 41

Limitador de las reglas.

Las configuraciones descritas anteriormente permiten crear la lógica dentro del SIEM para alertar las actividades detectadas por el honeypot. Las interacciones notificadas por el sistema honeypot van a generar una ofensa dentro de la plataforma SIEM, esto facilita el proceso de respuesta a un posible incidente de seguridad.

Para los otros dos casos de uso esta es la lógica de las reglas:

4.3.1 Fuerza bruta

Ilustración 42

Resumen de la lógica de las reglas de detección.

Rule Description

Apply Fuerza bruta detectada sobre honeypot on events which are detected by the Local system
and when the event(s) were detected by one or more of OpenCanary
and when at least 3 events are seen with the same Destination IP and different honeypot_password (custom) in 5 minutes

Rule Actions

- Set Severity to 10
- Set Credibility to 10
- Set Relevance to 10
- Force the detected Event to create a NEW offense, select the offense using Source IP

Rule Responses

- Dispatch New Event
  - Event Name: Fuerza Bruta detectada en honeypot
  - Event Description: intentos de fuerza bruta detectados por el honeypot
  - Severity: 10 Credibility: 10 Relevance: 10
  - High-Level Category: Control System
  - Low-Level Category: Billing Event
  - Force the dispatched event to create a NEW offense, select the offense using Source IP

This Rule will be: Enabled

4.3.2 Intentos de acceso a la base de datos

Ilustración 43

Resumen de la lógica de la regla para identificar accesos no autorizados a la base de datos.

Rule Description

Apply Intento de acceso a la BD honeypot on events which are detected by the Local system
and when the event(s) were detected by one or more of OpenCanary
and when the destination port is one of the following 3306
and when the event matches honeypot_logtype (custom) is any of 8001
and when the event matches Username is not N/A

Rule Actions

- Set Severity to 10
- Set Credibility to 10
- Set Relevance to 10
- Force the detected Event to create a NEW offense, select the offense using Source IP

Rule Responses

- Dispatch New Event
  - Event Name: Intento de conexión a la BD honeypot
  - Event Description: Intento de conexión a la BD del honeypot
  - Severity: 10 Credibility: 10 Relevance: 10
  - High-Level Category: Authentication
  - Low-Level Category: User Login Attempt
  - Force the dispatched event to create a NEW offense, select the offense using Source IP

This Rule will be: Enabled

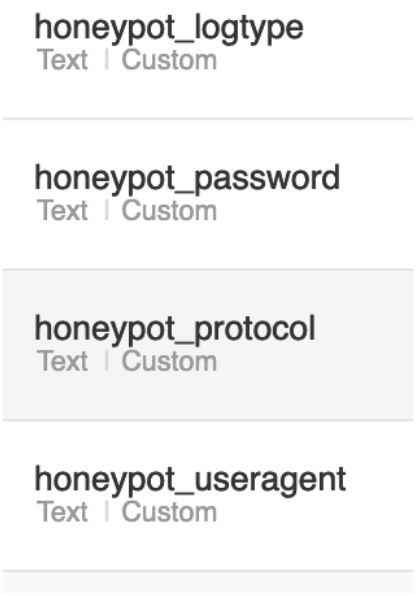
4.4 Optimización de las reglas

Cada una de las reglas desarrolladas dentro del proyecto fueron puestas a prueba para optimizar la detección y la lógica detrás de las reglas de detección. Dentro de las tareas de optimización de las reglas, se lograron identificar áreas de perfeccionamiento para una mejor detección y generación de alertas dentro de la plataforma de QRadar®.

Por medio del análisis y las pruebas realizadas, se lograron identificar nuevos campos dentro de los eventos del honeypot, los cuales son de interés para el proyecto. Estos campos se mapearon e indexaron como parte de la correcta identificación de dichos eventos por parte del SIEM. Estos se mencionan a continuación en la ilustración 44:

Ilustración 44

Campos adicionales de los eventos del honeypot.



En la tabla 2 se detallan las expresiones regulares y el detalle de los campos mencionados anteriormente.

Tabla 2

Expresiones regulares de los campos adicionales.

Campo	Descripción	Expresión regular
honeyport_logtype	OpenCanary utiliza números para identificar los diferentes tipos de logs que se generan. Los identificadores son de tipo numéricos y permiten filtrar estos eventos utilizando este identificador. Esto permite utilizar dicha propiedad para la generación de reglas, reportes y búsquedas, usando este campo como parámetro de búsqueda.	"logtype": ([^,]+)

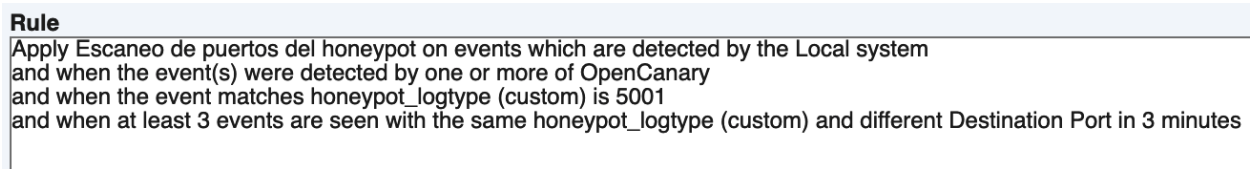
honeypot_protocol	Este campo permite identificar si la conexión se dio por medio del protocolo TCP o del protocolo UDP.	"PROTO": "([^"]+)

Las reglas también fueron analizadas, lo cual permitió identificar áreas de mejora. Los nuevos campos que se identificaron y mapearon permitieron modificar la lógica de las reglas y mejorar la capacidad y la “inteligencia” de detección. Las mejoras realizadas a las reglas se detallan a continuación:

4.4.1 Escaneo de puertos

Ilustración 45

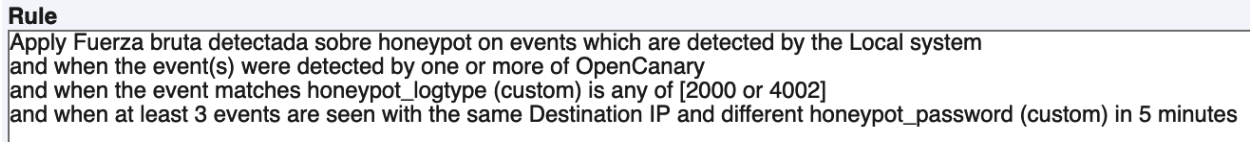
Lógica de la regla para la detección de escaneo de puertos.



4.4.2 Fuerza bruta

Ilustración 46

Lógica de la regla para la detección de ataques de fuerza bruta.



4.4.3 Accesos a la BD

Ilustración 47

Lógica de la regla para la detección de accesos no autorizados a la base de datos.

Rule

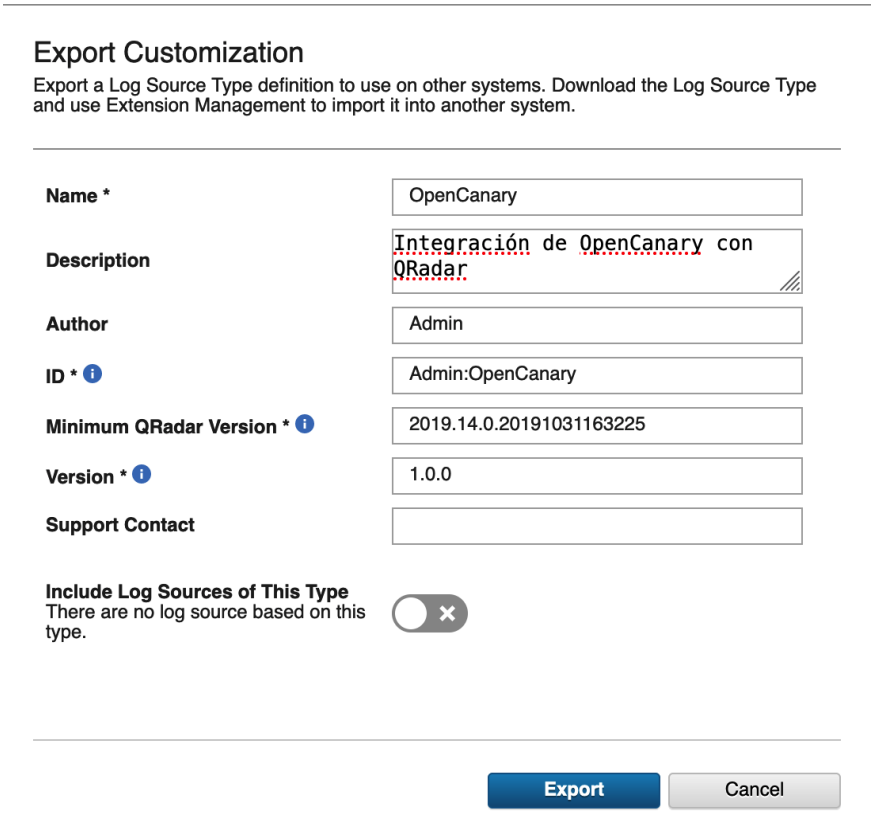
Apply Intento de acceso a la BD honeypot on events which are detected by the Local system
and when the event(s) were detected by one or more of OpenCanary
and when the destination port is one of the following 3306
and when the event matches honeypot_logtype (custom) is any of 8001
and when the event matches Username is not N/A

4.5 Creación de extensión de Open Canary para QRadar®

Luego de la creación de la fuente de información y la lógica de la regla QRadar®, este contenido puede ser exportado para su utilización en otros sistemas, sin tener que realizar los pasos anteriormente descritos. La plataforma cuenta con una herramienta que permite exportar el contenido creado para poder ser usado en otros sistemas. Desde la opción de editor de DSM (DSM Editor) se cuenta con una opción para editar este contenido. Una vez que se selecciona el contenido a exportar se puede usar la opción de exportar contenido (Export). Se debe llenar cierta información para realizar la exportación.

Ilustración 48

Proceso de exportación de la lógica creada para el mapeo de los logs de OpenCanary.



Una vez que se selecciona la opción de exportar, se va a generar un archivo de formato zip, el cual cuenta con toda la información necesaria para que QRadar® interprete correctamente los eventos de OpenCanary.

4.5.1 Instalación de la extensión en QRadar®

El proceso de importar el contenido en otro sistema QRadar® es bastante sencillo y se puede realizar desde la opción de administración de extensiones (Extensions Management) dentro del menú de administración.

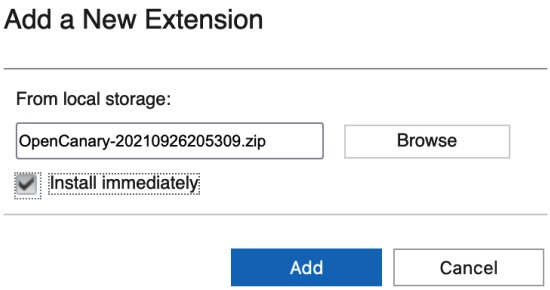
Ilustración 49

Menú para la administración de extensiones de QRadar®.

Desde esta opción y con el archivo del contenido previamente exportado, se puede realizar la importación de dicho contenido. Por medio de la opción de agregar (Add) se puede seleccionar el archivo con el contenido exportado, marcar la opción de instalar inmediatamente (Install immediately) y proceder a importar el contenido para su uso en otro sistema QRadar®.

Ilustración 50

Importación de la extensión en QRadar®



4.6 Publicación de la extensión

El contenido creado durante el desarrollo de este proyecto está a la disposición de la comunidad y es de distribución libre y gratuita, bajo la licencia de GNU Public License V3. Esto con el fin de proporcionar una solución que permita detectar intrusiones a una red de computadoras, a un bajo costo económico. La idea de este proyecto es proporcionar una solución que sea gratuita y que permita a la comunidad utilizar este contenido y expandirlo para que cubra otras posibles necesidades de seguridad. Si se desea realizar contribuciones, sugerencias o mejoras se pueden realizar al siguiente correo: warrenpcr@gmail.com.

La publicación de este proyecto y su contenido se realizó bajo la plataforma GitHub y se puede descargar utilizando el siguiente enlace: https://github.com/crmade/OpenCanary-QRadarCE

Capítulo 5: Análisis de resultados

En el siguiente capítulo se detallarán las actividades realizadas para probar la implementación y poder realizar un análisis de los resultados obtenidos.

Dentro del análisis realizado de los posibles casos de uso a implementar, tres fueron los seleccionados a manera de prueba de concepto y ejemplificación de las ventajas de implementar e integrar herramientas honeypot y una herramienta que permita correlacionar y administrar los incidentes de seguridad, asociados o derivados de una posible intrusión a una red de computadoras. Los casos de uso implementados son los siguientes:

1. Detección de escaneo de puertos.
2. Detección de ataques de fuerza bruta.
3. Detección de intentos de autenticación sobre la base de datos.

5.1 Escaneo de puertos

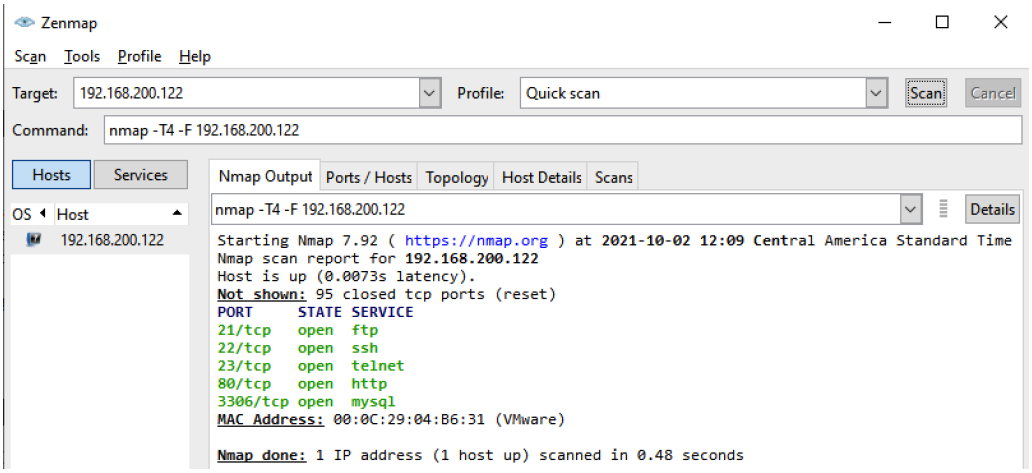
Para la realización del escaneo de puerto se va a utilizar la herramienta Zenmap, la cual cuenta con una interfaz gráfica. De igual manera se detallarán los comandos de nmap utilizados para realizar el escaneo de puertos.

El primer escaneo de puertos realizado sobre el honeypot logró identificar correctamente los puertos configurados durante la implementación de OpenCanary. El comando de nmap utilizado por la herramienta es el siguiente: nmap -T4 -F 192.168.200.122.

A continuación, se detallan los resultados obtenidos:

Ilustración 51

Resultado del escaneo de puertos con Zenmap.



Los puertos identificados por la herramienta son los esperados y los configurados durante la implementación de OpenCanary. Por otra parte, el SIEM pudo consumir e identificar correctamente los logs enviados por OpenCanary. En las siguientes imágenes se evidencia la correcta interpretación de los logs dentro de QRadar®

Ilustración 52

Evento en QRadar®.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	2	Oct 2, 2021, 12:06:30 PM	Unauthorized Access Attempt	192.168.200.131	0	192.168.200.122

Ilustración 53

Información del evento en QRadar®.

Event Information

Event Name	Actividad no autorizada sobre Honeypot						
Low Level Category	Unauthorized Access Attempt						
Event Description	Actividad no autorizada sobre Honeypot detectada.						
Magnitude	(10)	**Relevance**	10	**Severity**	10	**Credibility**	10
Username	N/A						
Start Time	Oct 2, 2021, 12:08:46 PM	**Storage Time**	Oct 2, 2021, 12:08:46 PM	**Log Source Time**	Oct 2, 2021, 12:08:46 PM		
honeypot_logtype (custom)	5001						
honeypot_password (custom)	N/A						
honeypot_protocol (custom)	TCP						
honeypot_useragent (custom)	N/A						
Domain	Default Domain						

5.1.1 Detección de escaneo de puertos

La lógica de la regla también fue puesta a prueba al momento de la detección de los escaneos de puertos realizados, con el fin de simular las actividades que realizaría un atacante, una vez que obtenga acceso a la organización.

Ilustración 54

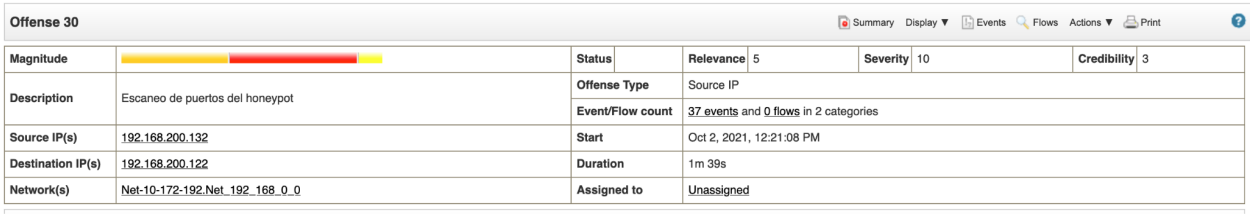
Eventos de escaneo de puertos en QRadar®

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:22:48 PM	Access Denied	192.168.200.132	0	192.168.200.122
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	5	Oct 2, 2021, 12:22:37 PM	Unauthorized Access Attempt	192.168.200.132	0	192.168.200.122
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:22:21 PM	Access Denied	192.168.200.132	0	192.168.200.122
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	10	Oct 2, 2021, 12:22:10 PM	Unauthorized Access Attempt	192.168.200.132	0	192.168.200.122
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:21:59 PM	Access Denied	192.168.200.132	0	192.168.200.122
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	10	Oct 2, 2021, 12:21:49 PM	Unauthorized Access Attempt	192.168.200.132	0	192.168.200.122

Como se puede evidenciar en la imagen anterior, QRadar® logró identificar y generar una alerta (ofensa) derivada de dichos logs. Dentro de la ofensa, se pueden identificar los eventos que contribuyeron a la generación de dicha alerta e información más detallada de la alarma.

Ilustración 55

Detalle de la alerta generada en QRadar®.



Offense 30

Summary | Display ▼ | Events | Flows | Actions ▼ | Print

Magnitude		**Status**		**Relevance**	5	**Severity** 10	**Credibility** 3
Description	Escaneo de puertos del honeypot	**Offense Type**	Source IP				
		Event/Flow count	37 events and 0 flows in 2 categories				
Source IP(s)	192.168.200.132	**Start**	Oct 2, 2021, 12:21:08 PM				
Destination IP(s)	192.168.200.122	**Duration**	1m 39s				
Network(s)	Net-10-172-192.Net_192_168_0_0	**Assigned to**	Unassigned				

QRadar® permite identificar fácilmente la cantidad de eventos que han contribuido a esta alerta. Para este caso específico, el SIEM ha correlacionado 37 eventos que desencadenaron la generación de esta alerta. Los mismos se detallan a continuación.

Ilustración 56

Eventos que contribuyeron a la generación de la alerta en QRadar®.

Event Name	Log Source	Event Count	Time ▼	Low Level Category
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:22:48 PM	Access Denied
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	5	Oct 2, 2021, 12:22:37 PM	Unauthorized Access Attempt
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:22:21 PM	Access Denied
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	10	Oct 2, 2021, 12:22:10 PM	Unauthorized Access Attempt
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:21:59 PM	Access Denied
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	10	Oct 2, 2021, 12:21:49 PM	Unauthorized Access Attempt
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:21:19 PM	Access Denied
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:21:08 PM	Access Denied
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:21:08 PM	Access Denied
Escaneo de puertos del honeypot	Custom Rule Engine-8 :: qradar-ce	1	Oct 2, 2021, 12:21:08 PM	Access Denied
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	2	Oct 2, 2021, 12:21:08 PM	Unauthorized Access Attempt
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	1	Oct 2, 2021, 12:21:08 PM	Unauthorized Access Attempt
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	1	Oct 2, 2021, 12:21:08 PM	Unauthorized Access Attempt
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	1	Oct 2, 2021, 12:21:08 PM	Unauthorized Access Attempt

5.2 Ataques de fuerza bruta

Como parte de las tácticas y técnicas utilizadas por los atacantes para obtener acceso a un equipo de la red, estos actores maliciosos utilizan ataques de fuerza bruta para tratar de adivinar las contraseñas y/o usuario de un servicio, esto con el objetivo de obtener acceso a un sistema o plataforma.

5.2.1 Detección de intentos de ataques de fuerza bruta

Para simular este tipo de ataques sobre el protocolo HTTP se utilizó la herramienta Hydra, la cual permite realizar autenticaciones de manera automatizada, lo que permite simular un ataque de fuerza bruta. El comando utilizado para la herramienta Hydra es el siguiente:

sudo hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.200.122 http-post-form "/index.html:username=admin&password=^PASS^:The account or password is invalid. Please try again."

QRadar® pudo detectar los eventos originados de los intentos de acceder a la página web:

Ilustración 57

Eventos de intentos de acceder recursos en el honeypot.

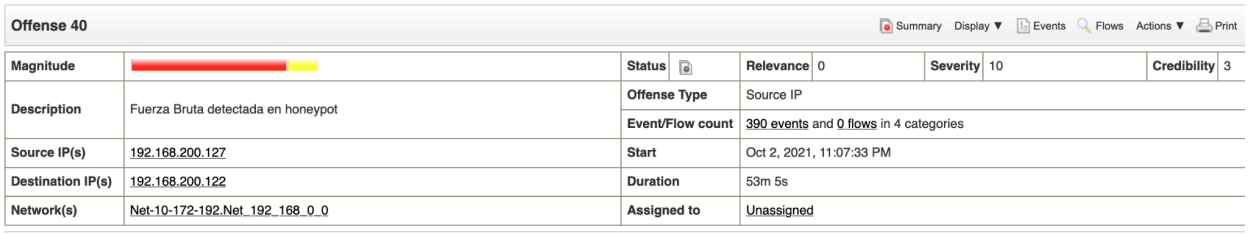
Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	2	Oct 2, 2021, 1:48:30 PM	Unauthorized Access Attempt	192.168.200.127	0	192.168.200.122	0	N/A
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	29	Oct 2, 2021, 1:48:30 PM	Unauthorized Access Attempt	192.168.200.127	47960	192.168.200.122	80	admin
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	31	Oct 2, 2021, 1:48:30 PM	Unauthorized Access Attempt	192.168.200.127	41776	192.168.200.122	80	N/A
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	22	Oct 2, 2021, 1:48:20 PM	Unauthorized Access Attempt	192.168.200.127	0	192.168.200.122	0	N/A
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	212	Oct 2, 2021, 1:48:20 PM	Unauthorized Access Attempt	192.168.200.127	38419	192.168.200.122	80	N/A
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	218	Oct 2, 2021, 1:48:20 PM	Unauthorized Access Attempt	192.168.200.127	43281	192.168.200.122	80	admin
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	22	Oct 2, 2021, 1:48:10 PM	Unauthorized Access Attempt	192.168.200.127	0	192.168.200.122	0	N/A
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	235	Oct 2, 2021, 1:48:10 PM	Unauthorized Access Attempt	192.168.200.127	46602	192.168.200.122	80	admin

Al igual que el caso de uso anterior, el SIEM generó una alerta que permite a los analistas de seguridad realizar la investigación asociada con este tipo de actividades.

Las siguientes imágenes detallan la alerta originada y los eventos que contribuyeron a la generación de dicha ofensa.

Ilustración 58

Detalle de la alerta generada en QRadar®.



Offense 40

Summary | Display ▼ | Events | Flows | Actions ▼ | Print

Magnitude		**Status**		**Relevance** 0	**Severity** 10	**Credibility** 3	
Description	Fuerza Bruta detectada en honeypot	**Offense Type**	Source IP				
		Event/Flow count	390 events and 0 flows in 4 categories				
Source IP(s)	192.168.200.127	**Start**	Oct 2, 2021, 11:07:33 PM				
Destination IP(s)	192.168.200.122	**Duration**	53m 5s				
Network(s)	Net-10-172-192.Net_192_168_0_0	**Assigned to**	Unassigned				

5.3 Intento de autenticación contra la base de datos

Otro de los servicios del honeypot es del servidor de base de datos MySQL, el cual está disponible en el puerto 3306 del servidor señuelo. Muchos atacantes intentan autenticarse contra este servicio para extraer información, posiblemente sensible, de la organización. Para simular este tipo de ataques utilizó la herramienta llamada MySQL Benchmark, la cual permite realizar conexiones de administración para base de datos.

5.3.1 Detección de intentos de autenticación contra la base de datos

Utilizando MySQL Benchmark y realizando varios intentos de conexión se generaron eventos del OpenCanary, identificados por QRadar®:

Ilustración 59

Intentos de acceso no autorizado a la base de datos.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	1	Oct 2, 2021, 2:19:37 PM	Unauthorized Access Attempt	192.168.200.132	50094	192.168.200.122	3306
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	1	Oct 2, 2021, 2:19:37 PM	Unauthorized Access Attempt	192.168.200.132	0	192.168.200.122	0
Actividad no autorizada sobre Honeypot	OpenCanaryCustom @ 192.168.200.122	1	Oct 2, 2021, 2:19:35 PM	Unauthorized Access Attempt	192.168.200.132	50093	192.168.200.122	3306

Estos eventos de seguridad contribuyeron a la generación de una alerta de seguridad relacionada con este tipo de acciones:

Ilustración 60

Alerta generada por los eventos de accesos no autorizados a la base de datos.

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users
33	Intento de conexión a la BD honeypot	Source IP	192.168.200.132		192.168.200.132	192.168.200.122	root

5.4 Análisis de resultados

Luego de las pruebas realizadas sobre el honeypot y la validación de la detección de estos eventos por parte del sistema SIEM, se puede determinar que QRadar® es capaz de detectar y alertar este tipo de ataques con una confianza del 100%. El escaneo de puertos, utilizando comandos de nmap, fueron detectados y alertados con éxito:

Ilustración 61

Alerta Escaneo de puertos.

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs
	30	Escaneo de puertos del honeypot	Source IP	192.168.200.132		192.168.200.132	192.168.200.122

La detección de ataques de fuerza bruta, realizadas sobre puerto 80 y puerto 22, fue satisfactoria por parte del SIEM. Esta alerta permite a los analistas de seguridad identificar y responder de acuerdo al tipo de actividad alertada. Para este caso de uso específico, QRadar® pudo detectar y alertar oportunamente los ataques de fuerza bruta realizados por la herramienta Hydra (puerto 80) y los intentos realizados de manera manual (puerto 22) también:

Ilustración 62

Alerta ataque de fuerza bruta.

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users
38	Fuerza Bruta detectada en honeypot	Source IP	192.168.200.127		192.168.200.127	192.168.200.122	root

El caso de uso de intentos de acceso a la base de datos también fue exitoso. Las pruebas realizadas para autenticarse sobre este servicio generaron eventos a nivel de OpenCanary que el SIEM pudo identificar adecuadamente y levantar la alerta correspondiente.

Ilustración 63

Alerta acceso no autorizado a la base de datos

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users
33	Intento de conexión a la BD honeypot	Source IP	192.168.200.132		192.168.200.132	192.168.200.122	root

En la tabla 3, se detallan los puertos configurados y si fueron o no detectados por el escáner de puertos.

Tabla 3

Resultados obtenidos por el escáner de puertos contrastado con los puertos configurados.

Puertos configurados	Detectado por el escáner de puertos
21	Sí
22	Sí
80	Sí
3306	Sí
23	Sí

En la tabla 4 se detallan los casos de uso y si fueron o no detectados por el SIEM:

Tabla 4

Casos de usos generados y su detección por parte de QRadar®

Caso de uso	Generó una Alerta
Ataques de fuerza bruta	Sí
Escaneo de puerto	Sí
Intentos de acceso a la base de datos	Sí

La siguiente tabla detalla una comparación de los casos de uso desarrollados, los puertos utilizados para interactuar con el honeypot y si QRadar® logró generar una alerta de seguridad o no.

Tabla 5

Casos de uso, puertos y detección por parte del SIEM

Caso de uso	Puerto	Generó una Alerta
Ataque de Fuerza Bruta	21	Sí
	22	Sí
	23	Sí
	80	Sí
	3306	Sí
Escaneo de puertos	21	Sí
	22	Sí
	23	Sí
	80	Sí
	3306	Sí
Acceso a base de datos	21	N/A
	22	N/A
	23	N/A

	80	N/A
	3306	Sí

Capítulo 6: Trabajo futuro

El proyecto desarrollado en este documento constituye una prueba de concepto funcional y está pensado para que pueda ser expandido en el futuro. Desde nuevos casos de uso hasta nuevas implementaciones son tan solo algunas de las ideas para trabajos futuros.

De igual modo, las ideas planteadas y desarrolladas en este trabajo podrían ser migradas a otras plataformas SIEM similares a QRadar®. Si bien es cierto, toda la lógica creada aplica únicamente para la integración de OpenCanary con QRadar®, las ideas son extrapolables a soluciones similares.

A modo de sugerencia para implementaciones futuras, se podría implementar un honeypot de conexiones remotas de administración de plataformas Windows (RDP) y la implementación del protocolo SMB dentro de OpenCanary, el cual es explotado por varios tipos de aplicativos maliciosos para expandirse en la red y permitiría una detección de este tipo de actividades a lo interno de la organización.

La idea principal del proyecto es demostrar las capacidades de detección que plataformas de tipo honeypot brindarían a todo tipo de organizaciones, indiferentemente de su tamaño. Por este motivo, el proyecto se liberó con la licencia GNU Public License V3, la cual permite su libre utilización, modificación y distribución, garantizando que se mantenga gratuito para todos los usuarios.

Capítulo 7: Conclusiones

En el más reciente estudio de la compañía IBM, se puede notar como en los últimos 5 años ha venido en incremento la cantidad de días que les toma a las organizaciones poder detectar y contener un incidente de seguridad. Para el 2017 el promedio era de 257 días, el siguiente año aumentó a 266. Luego en 2019 un promedio de 279; en 2020 de 280 y para el 2021 se tiene un promedio de 287 días (IBM, 2021).

Esto no es más que un indicativo de la necesidad de diseñar soluciones que permitan a las compañías la detección temprana y oportuna de incidentes de seguridad. Dentro del estudio de IBM, se estima una reducción de más de un millón de dólares en costos disminuyendo la cantidad de días que le toma a las organizaciones detectar y contener un incidente de seguridad, si se realiza en menos de 200 días. Se estima que el costo de una brecha de seguridad identificada y contenida en menos de 200 días puede ascender a los 3.6 millones de dólares. En los incidentes con un promedio de días mayor a 200, el costo puede aumentar hasta los 4.8 millones de dólares (IBM, 2021).

La solución propuesta, desarrollada e implementada en este proyecto facilita la identificación de posibles intrusiones a una red computacional utilizando sistemas señuelos y monitoreando las actividades por medio de un sistema SIEM. La integración de herramientas libres y gratuitas, junto con la utilización de hardware de tamaño compacto y bajo costo, como lo son los dispositivos Raspberry Pi, permiten reducir los costos económicos asociados a la implementación de la solución propuesta en este trabajo.

Como lo menciona Chris Sander en su libro: *Intrusion detection honeypots: detection through deception*, la batalla no se pierde cuando un atacante logra entrar a la red, la batalla se pierde cuando la información privada de una organización o persona es robada (Sanders, C. 2020).

La detección de un intruso dentro de una red de computadoras es fundamental para la reducción del impacto de una brecha, tanto económica como reputacional, sobre las organizaciones. La implementación de sistemas de señuelo (honeypots) y la monitorización de estos dispositivos por medio de plataformas SIEM, demostró con un grado muy alto de efectividad el valor que este tipo se soluciones podría aportar para mejorar la postura de ciberseguridad de las organizaciones, sin importar su tamaño, nicho de negocio, ni presupuesto.

Bibliografía

Bell, J. B. (2017). *Cheating And Deception.* ROUTLEDGE.

Borges, E. (2021). *SecurityTrails: Best Honeypots for Detecting Network Threats*. SecurityTrails Index Page. https://securitytrails.com/blog/top-honeypots

Gartner_Inc. (2020, February 18). *Magic Quadrant for Security Information and Event Management*. Gartner. https://www.gartner.com/en/documents/3981040.

Gartner_Inc. (s.f.). *Definition of Security Information and Event Management (SIEM).* Gartner Information Technology Glossary. Gartner. https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

IBM. (2020). *Cost of a Data Breach Study. IBM.* https://www.ibm.com/security/data-breach.

IBM. (2021). *Cost of a data breach report 2021*. https://www.ibm.com/security/data-breach.

OpenCanary. (2018). *OpenCanary*. OpenCanary.org. https://opencanary.readthedocs.io/en/latest/.

Raspberry Pi Foundation. (2021). Raspberry Pi Foundation - *About Us*. https://www.raspberrypi.org/about/

Sanders, C. (2020). *Intrusion detection honeypots: detection through deception*. Chris Sanders.

Spitzner, L. (2003). *Honeypots: tracking hackers*. Addison-Wesley.

Stallings, W. (2012). *Sistemas Operativos: Aspectos Internos y principios de diseño*. Pearson Educación.