IMPLEMENTACION SISTEMAS IDS/SIEM

[Subtítulo del documento]

[FECHA]

[NOMBRE DE LA COMPAÑÍA]

[Dirección de la compañía]

INDICE

1.INTRODUCCIÓN

En el panorama actual de amenazas cibernéticas en constante evolución, las empresas de todos los tamaños se enfrentan a desafíos significativos para proteger sus activos digitales contra intrusiones maliciosas y violaciones de seguridad. Las organizaciones, independientemente de su tamaño, están expuestas a una variedad de amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de sus datos críticos.

En este contexto, la implementación de sistemas de detección de intrusiones (IDS), gestión de información y eventos de seguridad (SIEM), y la integración de un honeypot emerge como una estrategia vital para fortalecer la postura de seguridad de las medianas-pequeñas empresas. Estos sistemas trabajan de manera conjunta para proporcionar una defensa integral contra las amenazas cibernéticas al permitir una detección proactiva, recopilación de inteligencia, mejora de la respuesta a incidentes y evaluación continua de la postura de seguridad

2.FINALIDAD

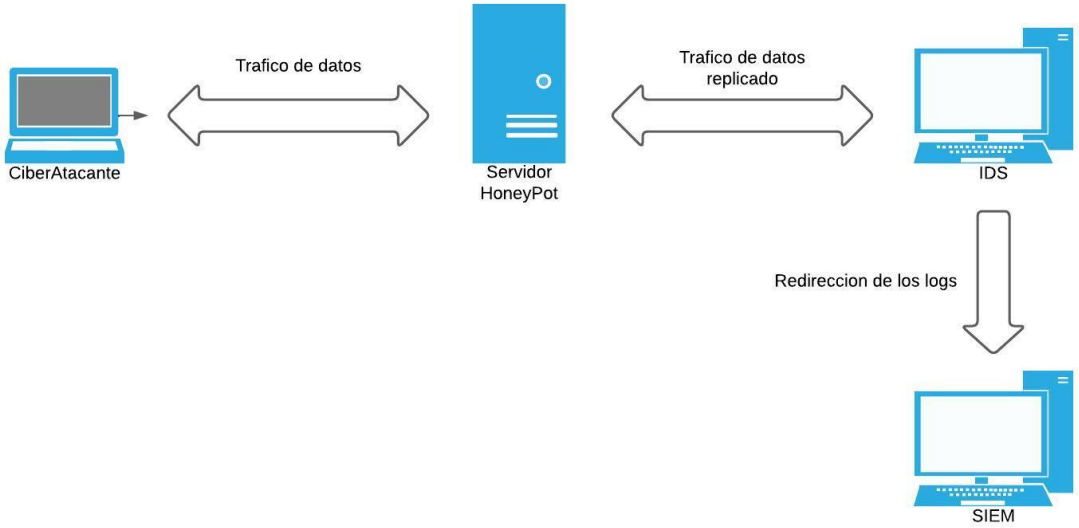
Este proyecto tiene como objetivo principal abordar las necesidades específicas de seguridad de una mediana-pequeña empresa, aprovechando la sinergia entre los sistemas IDS/SIEM y un honeypot para fortalecer sus defensas contra ataques cibernéticos. A través de la implementación cuidadosa de estas tecnologías, la empresa podrá mejorar su capacidad para detectar y responder a amenazas potenciales, proteger sus activos críticos y mantener la continuidad de sus operaciones comerciales.

3.OBJETIVOS

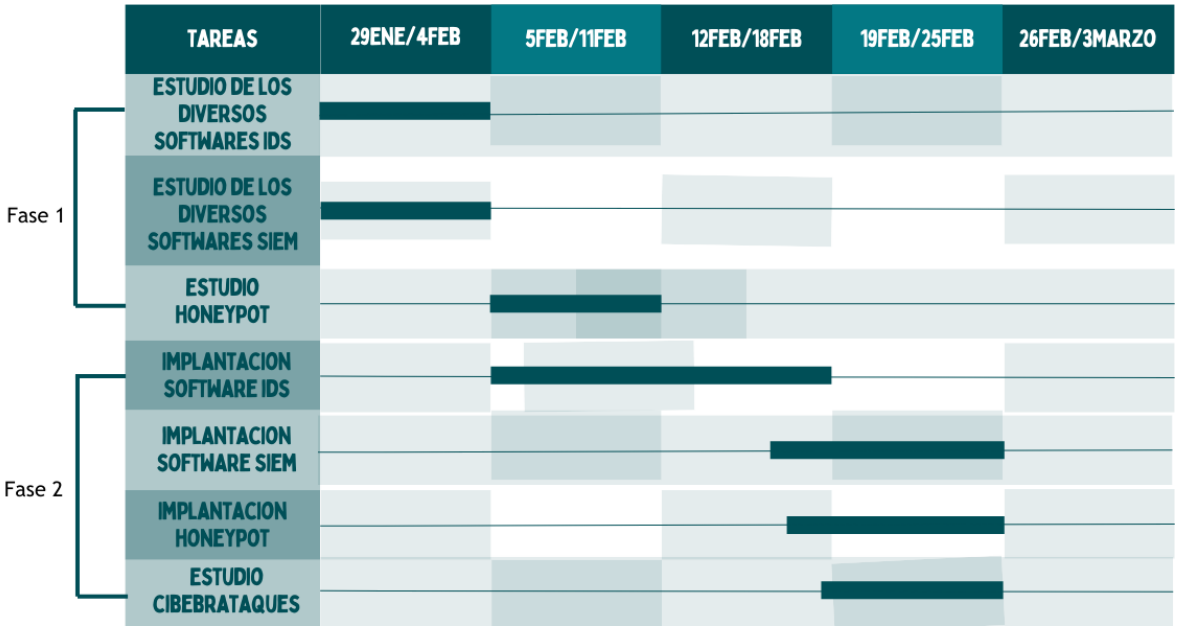
Los objetivos de este proyecto son, la configuración de honeypot de baja interacción, la instalación de sistemas IDS/SIEM, la configuración de como los logs serán enviados desde el servidor IDS al servidor SIEM, así como un acercamiento a los ciberataques más comunes.

4.MEDIOS NECESARIOS PARA LA REALIZACION DEL PROYECTO

Como podemos observar en el mapa topologico de la red en la imagen, representa la estructura del laboratorio que vamos a utilizar, como se puede observar, nuestro laboratorio se compone de 4 maquinas virtuales, una de ellas tendria un software IDS instalado, otra de ellas contendria el software SIEM , la otra alojaria nuestro honeypot y por ultimo la ultima maquina la cual se encargaria de los ciberataques.



5.PLANIFICACION



La planificación que he seguido la dividiremos en varias fases:

- Investigación de los softwares a utilizar (Fase 1)
  En esta fase me he enfocado en la investigación de los diferentes softwares IDS/SIEM, así como es estudio de los diferentes tipos de honeypot que existen.

    - Estudio de los diversos softwares IDS
      En el panorama actual de ciberseguridad, donde las amenazas cibernéticas evolucionan constantemente, el estudio de los diversos softwares de Detección de Intrusiones (IDS) se convierte en una piedra angular para la protección efectiva de las infraestructuras de tecnología de la información. Los sistemas IDS son herramientas esenciales que ayudan a las organizaciones a detectar y responder a posibles intrusiones o actividades maliciosas en sus redes y sistemas.

      Este estudio se centra en explorar los diferentes softwares IDS disponibles en el mercado, así como en comprender sus características, capacidades y aplicaciones. A través del análisis de estos sistemas, los profesionales de seguridad de la información pueden adquirir una comprensión más profunda de cómo funcionan, cómo se implementan y cómo se pueden integrar de manera efectiva en el entorno de seguridad de una organización.

La diversidad de los softwares IDS ofrece a los profesionales de seguridad una amplia gama de opciones para adaptarse a las necesidades y requisitos específicos de sus organizaciones. Desde soluciones de código abierto hasta plataformas comerciales, cada software IDS tiene sus propias fortalezas y debilidades, lo que requiere una evaluación cuidadosa para determinar cuál es la más adecuada para una situación particular.

- Estudio de los diversos softwares SIEM

  En el complejo y cambiante panorama de la ciberseguridad, la capacidad de recopilar, analizar y correlacionar datos de seguridad de diversas fuentes se vuelve fundamental para proteger las infraestructuras de tecnología de la información de las amenazas cibernéticas. Los sistemas de Gestión de Información y Eventos de Seguridad (SIEM) desempeñan un papel crucial al proporcionar a las organizaciones una visión integral de la seguridad de su entorno digital.

  Este estudio se enfoca en explorar los diferentes softwares SIEM disponibles en el mercado, así como en comprender sus características, funcionalidades y capacidades. Gracias al análisis detallado de estos sistemas, los profesionales de seguridad de la información pueden adquirir una comprensión más profunda de cómo pueden utilizarlos para mejorar la detección, respuesta y mitigación de amenazas cibernéticas.

- Estudio Honeypot

  En el campo de la ciberseguridad, la implementación de técnicas proactivas para identificar y mitigar las amenazas cibernéticas se ha vuelto esencial. Los honeypots son herramientas estratégicas que permiten a las organizaciones atraer, monitorear y analizar el comportamiento de los posibles atacantes, proporcionando valiosa inteligencia sobre las tácticas, técnicas y procedimientos utilizados en el panorama de las amenazas cibernéticas.

  Este estudio se basa en explorar los diferentes tipos y enfoques de honeypots disponibles, así como en comprender sus características,

aplicaciones y limitaciones. A través de un análisis detallado de estos sistemas, los profesionales de seguridad de la información pueden adquirir una comprensión más profunda de cómo pueden utilizar los honeypots para fortalecer la postura de seguridad de sus organizaciones y mejorar la capacidad de detección y respuesta a amenazas.

- Implementación de los softwares IDS/SIEM (Fase 2)

6.REALIZACION DEL PROYECTO

6.1 HONEYPOT

Un honeypot es una herramienta de seguridad informática que se utiliza para detectar, desviar o contrarrestar los ataques cibernéticos. Consiste en una trampa o señuelo diseñado para simular sistemas, servicios o datos reales y atraer a los atacantes para que interactúen con ellos. Los honeypot se utilizan con el propósito de estudiar el comportamiento de los atacantes, recopilar información sobre las técnicas utilizadas en los ataques, identificar amenazas potenciales y fortalecer las medidas de seguridad de una red o sistema informático.

En nuestro caso vamos a usar una máquina virtual con Ubuntu y lo único que haremos será abrir e instalar los protocolos que vamos a utilizar para los ciberataques.

- **Abrir Puertos**
  - Lo primero que haremos será abrir los puertos correspondientes a los protocolos que utilizamos, en nuestro caso **SSH, FTP, HTTP**

```
ufw enable

ufw allow (número puerto)
```

- **Instalar protocolos**
  - ```
    apt install ssh
    apt install vsftpd
    apt install apache2
    ```

6.2 SISTEMAS IDS

Los sistemas IDS se encargan de detectar patrones de actividad sospechosa en la red y en los sistemas informáticos de las empresas, esto podría incluir intentos de acceso no autorizado o tráfico malicioso, por tanto, el software IDS detecta la amenaza y genera una alerta.

Por ende, podríamos decir que un sistema IDS sirve para **monitorizar y detectar** en un sistema informático, un servidor web o una base de datos.

Existen diferentes tipos de IDS:

1. IDS de Red (NIDS/Network-based IDS)
   I. Estos pueden ser colocados estratégicamente en la red para monitorear el tráfico que pasa a través de ella.
   II. Examinan paquetes en busca de firmas conocidas de ataques, anomalías en el tráfico, o comportamiento sospechoso.
   III. Pueden ser basados en firma, detectando patrones específicos conocidos de ataque, o basado en anomalías, detectando desviaciones del tráfico normal.

2. IDS de Host (HIDS/Host-based IDS)
   I. Los IDS de host se ejecutan en los sistemas individuales y monitorean las actividades y eventos que ocurren en esos sistemas.
   II. Supervisan registros de eventos del sistema, archivos de registro, configuraciones del sistema, y otros aspectos del sistema operativo y las aplicaciones.
    ```

III. Son eficaces para detectar actividades anómalas que podrían indicar compromisos de seguridad en un host específico.
IV. Pueden detectar malware, intentos de acceso no autorizado, cambios no autorizados en archivos críticos del sistema, entre otros eventos.

3. IDS de Firma (Signature-based IDS)
    I. Los IDS de firma utilizan bases de datos de firmas conocidas de ataques para identificar actividades maliciosas.
    II. Comparan los patrones de tráfico o actividad observados con los patrones almacenados en la base de datos de firmas.
    III. Son efectivos para detectar amenazas conocidas, pero pueden pasar por alto ataques nuevos o variantes de ataques existentes que no estén en la base de datos de firmas.

4. IDS de Anomalías (Anomaly-based IDS)
    I. Los IDS de anomalías buscan comportamientos inusuales o anómalos en el tráfico de red o en la actividad del sistema.
    II. Construyen un perfil del tráfico o actividad normal y alertan sobre desviaciones significativas de ese perfil.
    III. Son útiles para detectar ataques desconocidos o variantes de ataques existentes que no coinciden con patrones de firma conocidos.
    IV. Pueden generar más falsos positivos que los IDS basados en firma, ya que cualquier desviación del comportamiento normal puede activar una alerta.

Ahora nos dirigiremos al porque se ha utilizado el software IDS de suricata sobre el de Snort, dos de los principales IDS del mercado.

Ambas herramientas son poderosas y ampliamente utilizadas en la comunidad de seguridad cibernética, cada una con sus propias ventajas y características distintivas.

Suricata, un IDS de código abierto, se destaca por su alto rendimiento y su capacidad de escalar en redes de alto tráfico. Su arquitectura multiproceso y multihilo permite una mayor eficiencia y capacidad de procesamiento en comparación con Snort. Además, Suricata ofrece soporte nativo para la decodificación de protocolos en tiempo real, lo que facilita la identificación de amenazas en capas más profundas del tráfico de red.

Por otro lado, Snort es una de las herramientas IDS más antiguas y establecidas en el mercado, con una amplia comunidad de usuarios y una extensa base de firmas de detección de amenazas. Su motor de detección de firmas altamente configurable y su interfaz de reglas flexibles lo hacen adecuado para escenarios donde se requiere un control detallado sobre las políticas de detección.

Por ende, nos hemos acabado decantando por Suricata, debido a su capacidad de procesamiento multihilo.

En nuestro caso en tema de hardware vamos a utilizar una máquina virtual con Ubuntu, donde alojaremos nuestro sistema IDS, el cual en nuestro caso hemos elegido **suricata,** debido a que, al tratarse de un software de código abierto, nos brinda más posibilidades.

Procederemos con la instalación del software suricata usando la guía oficial que hay en la bibliografía de este documento, en caso de no utilizar Ubuntu dirigirse al apartado de Installation que no se encuentra dentro de Quickstart guide.

Con estos dos comandos podemos ver información sobre la versión de suricata que tenemos instalada.

```
Suricata –build-info

Systemctl status suricata
```

Para empezar la configuración de suricata nos dirigiremos al archivo **suricata.yaml** el cual se encuentra se encuentra por defecto en la siguiente ruta **/etc/suricata/suricata.yaml**

Siguiendo la guía, deberemos configurar la variable $HOME_NET con la red o redes que queramos que el IDS monitoreé.

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"
```

Lo siguiente que habría que hacer seria indicar cual es la interfaz de red en la que nuestra red estaría fluyendo tal y como dice la guía oficial.

```
af-packet:
   - interface: ens33
     cluster-id: 99
     cluster-type: cluster_flow
     defrag: yes
     use-mmap: yes
     tpacket-v3: yes
```

Tambien podremos modificar la ruta donde se guardarán los logs que utilizaremos posteriormente.

```
default-log-dir: /var/log/suricata/
```

Suricata utiliza firmas para activar alertas, por lo que es necesario instalarlas y mantenerlas actualizadas con el siguiente comando. Las firmas son tambien llamadas reglas.

```
suricata-update
```

Luego, las reglas se instalan en **/var/lib/suricata/rules** que también es el valor predeterminado en la configuración y utiliza el único archivo **suricata.rules**.

Para asegurarnos de que todo funciona correctamente reiniciaremos el servicio y comprobaremos su correcto funcionamiento con el siguiente comando.

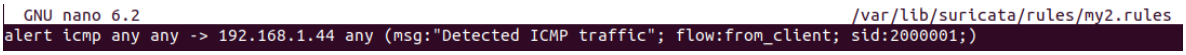
```
systemctl restart suricata

tail /var/log/suricata/suricata.log
```

Y buscaremos una línea que diga algo parecido a esto

```
6747 - Suricata-Main] 2024-02-15 12:19:07 Notice: threads: Threads created -> W: 2 FM: 1 FR: 1   Engine started.
```

Ahora llega el momento de crear nuestras propias reglas, para ello vamos a crearnos nosotros un fichero donde colocar nuestras reglas, que en nuestro caso lo llamaremos **my2.rules** y dentro escribiremos nuestra primera regla tal que así.



Vamos a explicar un poco la sintaxis para crear una regla:

```
alert icmp any any -> 192.168.1.44 any (msg:"Detected ICMP traffic"; flow:from_client; sid:2000001;)
```

- Action
  - Accion de la regla Alert (Lanzar una alerta al fichero de log)
- Header
  - Protocolo ICMP (Cuando un paquete utiliza el protocolo ICMP)
  - Dirección IP origen any (cualquiera)
  - Puerto de origen any (cualquiera)
  - Sentido -> (Paquete con este origen que se dirige a)
  - Dirección IP destino 192.168.1.44 (Dirección Honeypot)
  - Puerto de destino any (cualquiera)
- Rule options
  - Mensaje msg (Muestra mensaje: Detected ICMP traffic)
  - Dirección flujo de datos flow:from_client (Origen desde cliente)
  - Identificador de la regla sid:2000001

Por ejemplo, esta regla que hemos creado aquí, se encarga de detectar cuando realizamos un ping desde una ip externa, en este caso cualquiera, a la ip de nuestro honeypot.

6.3 SISTEMAS SIEM

Un SIEM (Security Information and Event Management) es un tipo de sistema de seguridad informática que proporciona una visión integral de la seguridad de la información en una organización al recopilar, correlacionar y analizar eventos de seguridad de múltiples fuentes en tiempo real. Estas fuentes pueden incluir

registros de dispositivos de red, registros de sistemas operativos, registros de aplicaciones, eventos de seguridad de endpoints, entre otros.

Es decir, la función principal de un SIEM es ayudar a las organizaciones a detectar, investigar y responder a amenazas cibernéticas e incidentes de seguridad de manera eficiente. Para lograr esto, un SIEM realiza las siguientes funciones:

1. Recopilación de datos: Recopila eventos y registros de seguridad de una amplia variedad de fuentes en toda la infraestructura de TI de la organización, incluidos dispositivos de red, servidores, sistemas de aplicaciones, endpoints y más.

2. Correlación de eventos: Correlaciona y analiza los eventos recopilados para identificar patrones y relaciones entre eventos aparentemente no relacionados que podrían indicar actividades maliciosas o incidentes de seguridad.

3. Detección de amenazas: Utiliza reglas predefinidas, firmas de amenazas y técnicas de análisis de anomalías para detectar actividades sospechosas o maliciosas en la red y los sistemas de la organización.

4. Notificación de alertas: Genera alertas y notificaciones en tiempo real para informar a los equipos de seguridad sobre eventos de seguridad importantes que requieren atención y acción inmediata.

5. Investigación de incidentes: Facilita la investigación y el análisis de incidentes de seguridad proporcionando herramientas para buscar y visualizar datos de seguridad, reconstruir la secuencia de eventos y determinar el alcance y el impacto de los incidentes.

6. Generación de informes y cumplimiento normativo: Genera informes detallados sobre la actividad de seguridad, las tendencias de amenazas, los incidentes detectados y el cumplimiento normativo para ayudar a las organizaciones a cumplir con los requisitos de auditoría y regulaciones de seguridad.

Seguiremos con él porque hemos elegido Splunk como software SIEM por encima de Graylog.

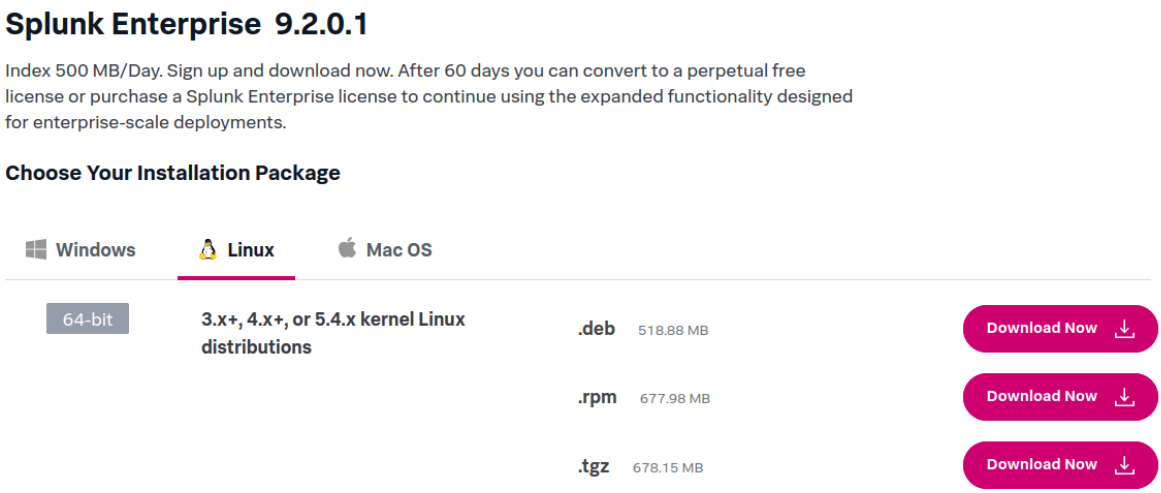
En la selección de una solución de gestión de registros y análisis de datos en el ámbito empresarial, es fundamental evaluar cuidadosamente las características y capacidades de las diferentes opciones disponibles. En este sentido, tanto Splunk como Graylog son plataformas ampliamente reconocidas que ofrecen funcionalidades avanzadas para la gestión y análisis de registros, sin embargo, hay algunas diferencias clave a considerar al elegir entre ambas.

Splunk, como líder en el mercado de análisis de datos operativos, destaca por su robusta arquitectura, escalabilidad y amplio conjunto de características. Ofrece una interfaz de usuario intuitiva y potente, que permite a los usuarios realizar búsquedas, análisis y visualización de datos de manera eficiente. Además, Splunk cuenta con una amplia gama de complementos y aplicaciones que amplían sus capacidades para diversos casos de uso, como seguridad, operaciones de TI, análisis de registros de aplicaciones, entre otros. Su modelo de licenciamiento basado en datos ingesta, aunque puede resultar costoso para implementaciones a gran escala, proporciona flexibilidad y permite a las organizaciones adaptarse a sus necesidades específicas.

Por otro lado, Graylog es una opción atractiva para aquellas organizaciones que buscan una solución de gestión de registros de código abierto. Ofrece funcionalidades sólidas de recopilación, almacenamiento y análisis de registros, junto con una comunidad activa de usuarios y desarrolladores que contribuyen al desarrollo y mejora continua del software. Graylog es conocido por su arquitectura flexible y su capacidad para escalar horizontalmente, lo que lo hace adecuado para implementaciones de diferentes tamaños. Además, su modelo de licenciamiento de código abierto proporciona una opción rentable para aquellas organizaciones que tienen presupuestos limitados y buscan una solución de gestión de registros económica y altamente personalizable.

En nuestro caso nos vamos a decantar por Splunk ya que posee una interfaz muy intuitiva, aunque sea un software más costoso de implementar en grandes escalas.

Para proceder con la instalación de Splunk, lo primero que tendremos que hacer será descargarnos su software, el cual lo podemos descargar desde la página oficial de Splunk, en nuestro caso vamos a descargar la versión Enterprise.



Una vez descargado lo descomprimimos de la siguiente forma:

```
tar -zxvf splunk-<VERSION>.tgz
```

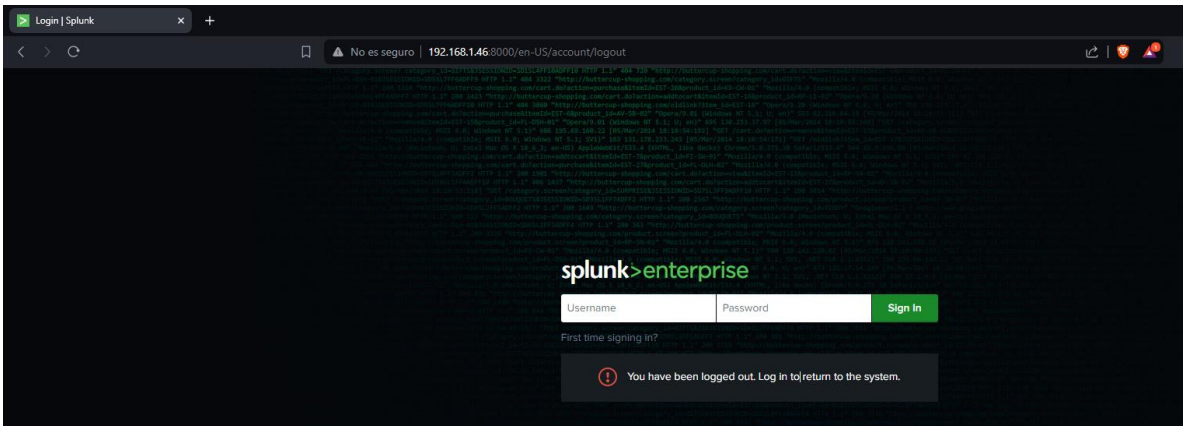
Reemplazar <VERSION> con la versión especifica de Splunk descargada.

Para continuar con la instalación, nos dirigiremos al directorio **splunk/bin** y ejecutaremos el siguiente comando:

```
./splunk start --accept-license
```

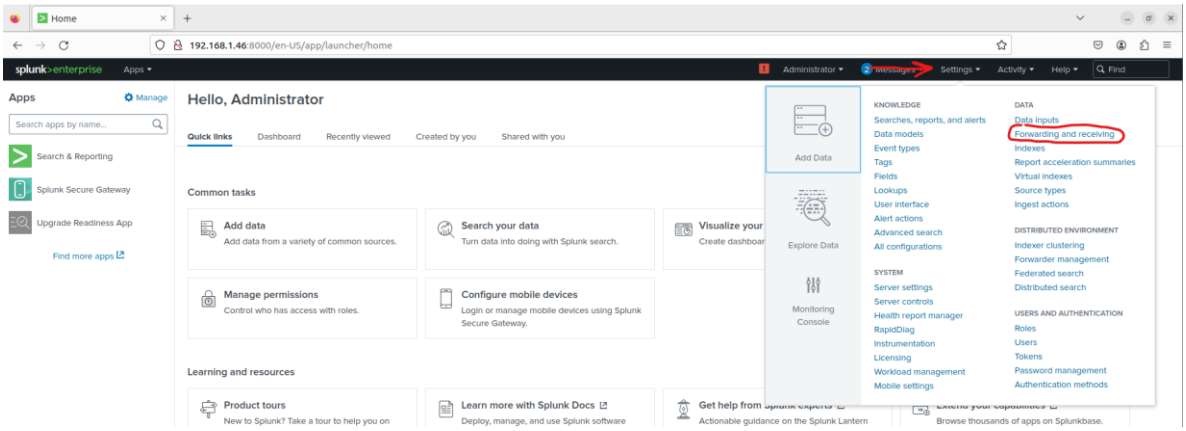
El algún punto de la instalación se nos pedirá proporcionar un nombre de administrador, asi como una contraseña, para luego poder acceder a la interfaz gráfica.

Ahora para poder acceder a la interfaz de splunk, deberemos dirigirnos al navegador y poner en el buscador la ip de la maquina donde splunk este alojado, asi como el puerto en el que corre, en mi caso sería:

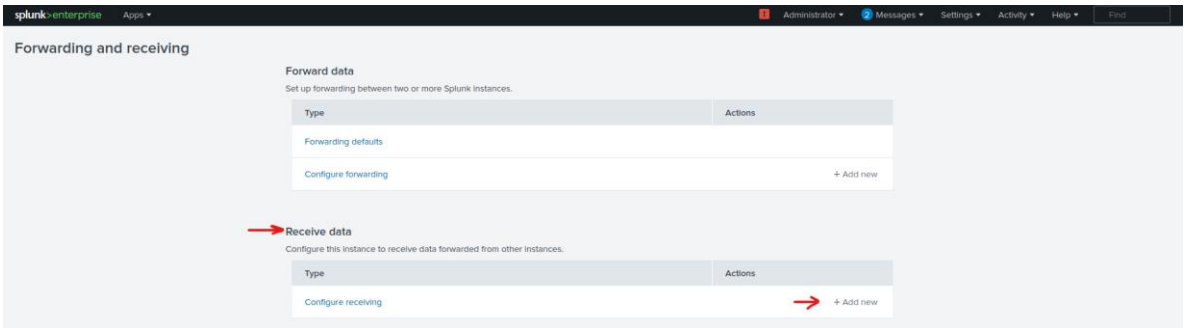


Lo primero que deberemos hacer es abrir el puerto por el que nos van a llegar los logs desde splunk.

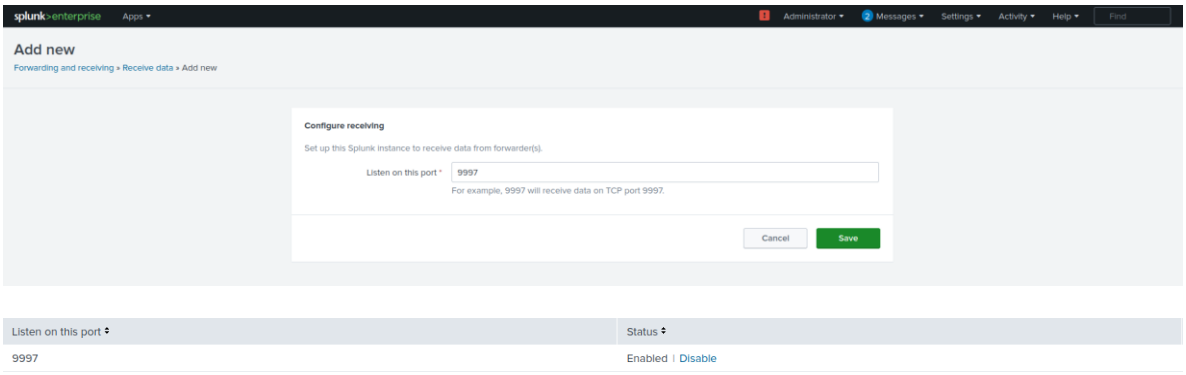
Dentro de settings, nos dirigiremos al apartado de Forwarding and receiving.



Una vez dentro de este apartado nos dirigiremos a Receive data, y añadiremos una nueva.



En nuestro caso vamos a utilizar el puerto 9997, que es el puerto por donde nos van a llegar los logs desde suricata.



Para redirigir los logs desde Suricata hasta Splunk, usaremos la herramienta Universal Splunk Forwarder, que permite la recopilación y el reenvío eficiente de datos de logs y eventos desde múltiples fuentes hacia un servidor central de Splunk para su indexación y análisis. Este componente ligero y versátil facilita la implementación de una arquitectura de recopilación de datos distribuida y escalable, esencial para el monitoreo y la gestión de la información de seguridad en entornos empresariales.

Universal Splunk Forwarder ofrece una amplia gama de capacidades y características, incluyendo:

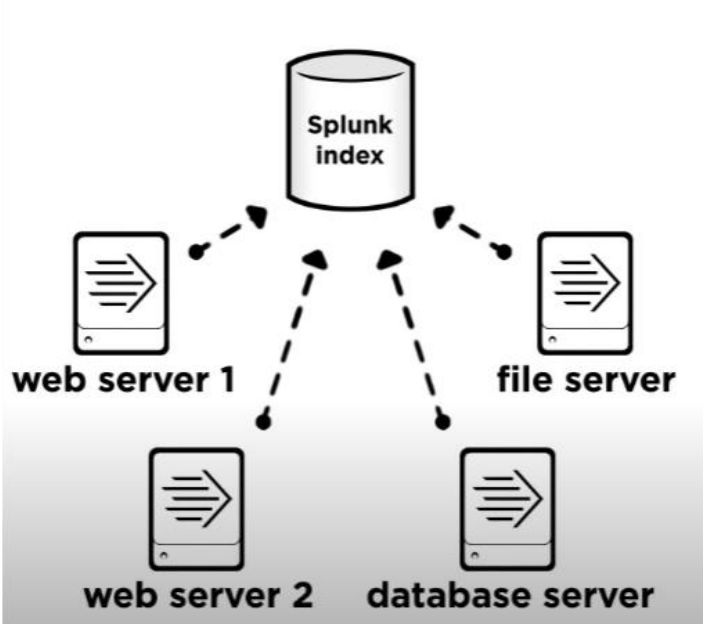
1. Recopilación de Datos Eficiente: Permite la recopilación de logs y eventos desde diversas fuentes, como sistemas operativos, aplicaciones, dispositivos de red y sensores de seguridad, utilizando una variedad de protocolos de comunicación, incluyendo TCP, UDP y archivos de registro locales.

2. Seguridad y Fiabilidad: Incorpora funcionalidades de seguridad avanzadas, como cifrado de datos, autenticación y control de acceso, para garantizar la integridad y la confidencialidad de los datos recopilados durante su transmisión y almacenamiento.

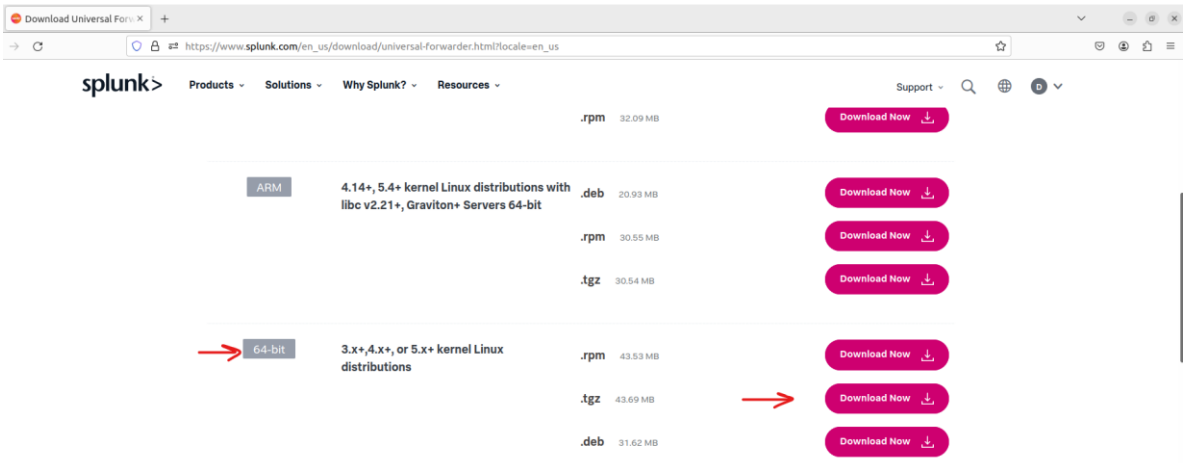
3. Optimización del Ancho de Banda: Implementa técnicas de compresión y optimización del tráfico para minimizar el consumo de ancho de banda durante la transmisión de datos a través de redes de bajo ancho de banda o conexiones de red de alta latencia.

4. Configuración y Gestión Simplificadas: Ofrece una interfaz intuitiva y herramientas de configuración centralizada para facilitar la implementación, configuración y administración de múltiples instancias de Universal Splunk Forwarder en entornos distribuidos y heterogéneos.

En resumen, el Universal Splunk Forwarder desempeña un papel fundamental en la infraestructura de Splunk, proporcionando la capacidad de recopilar datos de logs y eventos desde diversas fuentes y enviarlos de manera eficiente a un servidor central de Splunk para su análisis y visualización.



La herramienta puede ser descargada desde la página oficial de Splunk, en nuestro caso descargaremos la versión 64-bit



Una vez descargado, lo descomprimiremos e instalaremos con los mismos comandos que usamos para instalar Splunk

```
./splunk start --accept-license
```

Luego después de haber instalado Universal Splunk Forwarder lo que tendremos que hacer es añadir la IP donde esta alojado Splunk, para que nuestro IDS redireccione los logs hacia este.

```
suricata@suricata-machine:~/Downloads/splunkforwarder/bin$ ./splunk add forward-server 192.168.1.46:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R suricata:suricata /home/suricata/Downloads/splunkforwarder"
Splunk username: splunk
Password:
Added forwarding to: 192.168.1.46:9997.
```

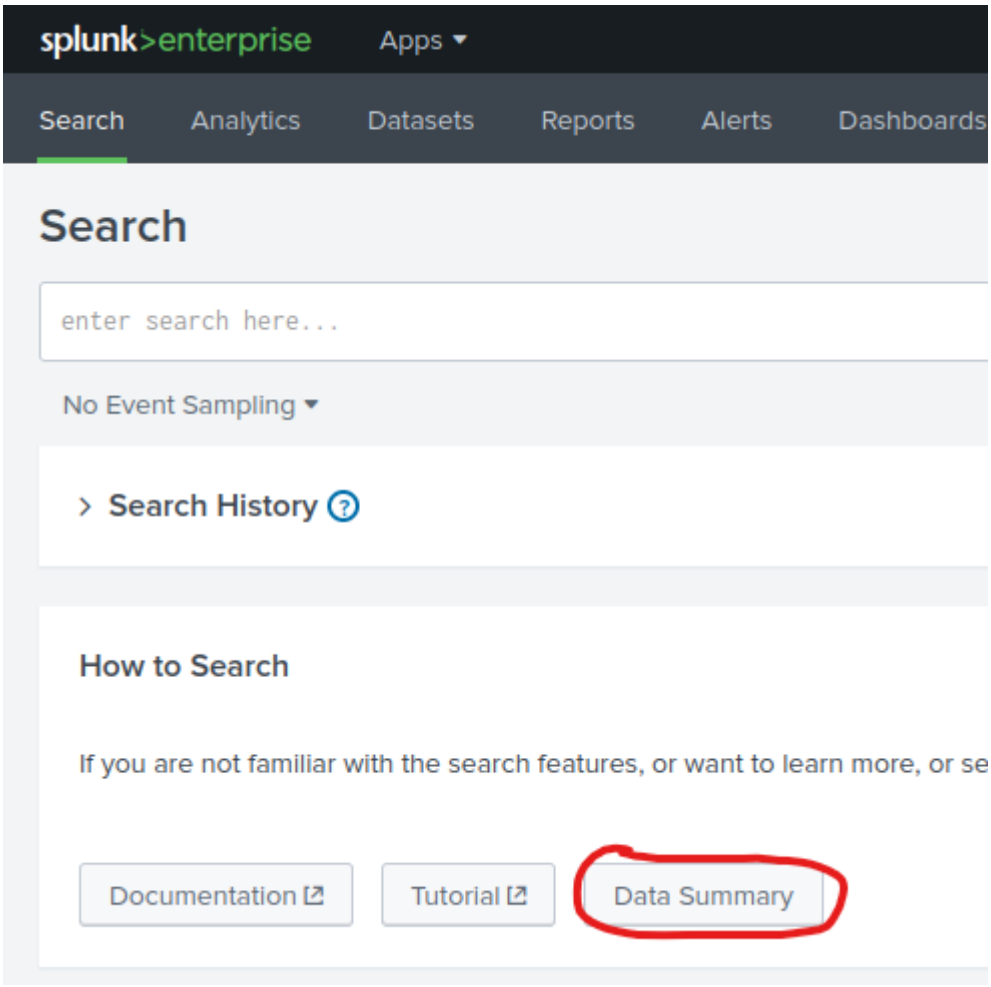
Luego de haber añadido nuestro indexador deberemos decirle a nuestro Universal Splunk Forwarder que datos queremos de enviar, esto lo haremos gracias a la función **add monitor**

```
suricata@suricata-machine:~/Downloads/splunkforwarder/bin$ ./splunk add monitor -auth splunk:12345678 /var/log/suricata/fast.log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R suricata:suricata /home/suricata/Downloads/splunkforwarder"
Added monitor of '/var/log/suricata/fast.log'.
```

En caso de que queramos comprobar cuantos indexadores están conectados a nuestro Universal Splunk Forwarder lo haremos de la forma que muestra la captura a continuación:

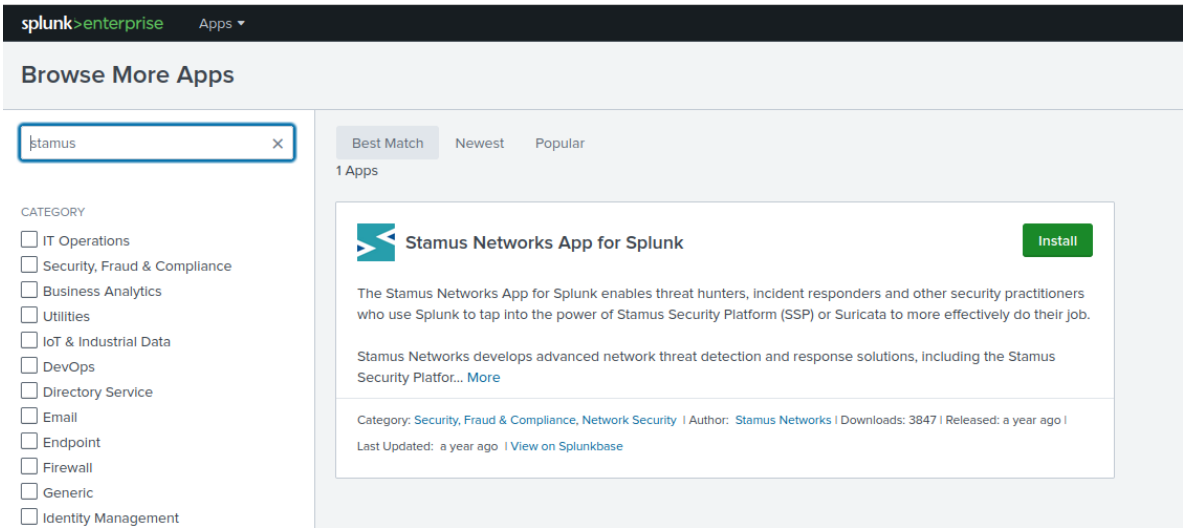
```
root@suricata-machine:/home/suricata/Downloads/splunkforwarder/bin# ./splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R suricata:suricata /home/suricata/Downloads/splunkforwarder"
Active forwards:
        192.168.1.46:9997
Configured but inactive forwards:
        None
```

Dentro de Splunk podremos comprobar todos los forwarder que están conectados a nuestro indexador, para hacerlo nos debermos dirigir al apartado de Search & Reporting y una vez dentro de este apartado, seleccionamos Data Summary.



Una vez comprobado que a Splunk le están llegando los logs, vamos a descargar una aplicación especifica para el IDS suricata, que nos permite crear un Dashboard con una vista mas simplificada de toda la información que se encuentra en los logs.

Para ello nos dirigiremos al apartado **Find more Apps** y en el buscador pondremos **Stamus**

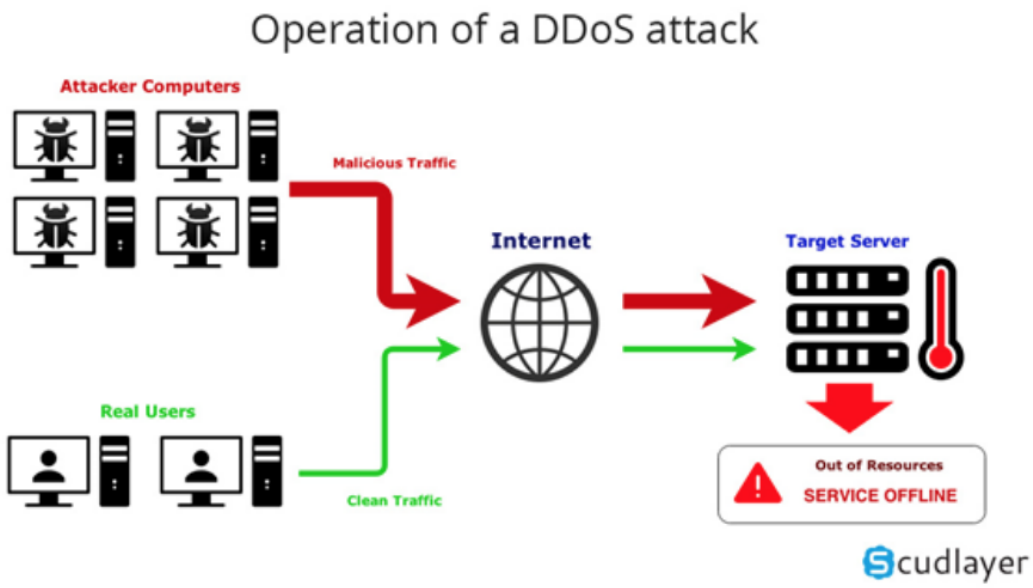


7.PRINCIPALES CIBERATAQUES

Ataques de denegación de servicio (DDoS):

Los ataques de denegación de servicio son una forma de ciberataque que tiene como objetivo abrumar un sistema, red o servicio en línea con una cantidad abrumadora de tráfico falso o solicitudes de conexión. Estos ataques buscan interrumpir el funcionamiento normal del objetivo, haciendo que se vuelva inaccesible para usuarios legítimos.

La forma en que funciona un ataque DDoS es relativamente simple pero efectiva. Los perpetradores utilizan una red de dispositivos comprometidos, conocidos como botnets, para enviar una gran cantidad de tráfico al objetivo simultáneamente. Estos dispositivos pueden incluir computadoras, servidores, dispositivos IoT u otros dispositivos conectados a internet que han sido infectados con malware y están bajo el control del atacante.



Existen diferentes tipos de ataques DDoS:

- Ataques de inundación de tráfico: Este es el tipo más común de ataque DDoS, en el que los atacantes envían grandes volúmenes de tráfico al objetivo, abrumando sus recursos de red y provocando una interrupción en el servicio. Estos ataques pueden utilizar diferentes protocolos de red, como UDP (User Datagram Protocol), TCP (Transmission Control Protocol) o ICMP (Internet Control Message Protocol), para inundar el objetivo con paquetes de datos falsos.
- Ataques de agotamiento de recursos: En este tipo de ataque, los atacantes se enfocan en agotar los recursos del sistema objetivo, como la capacidad de procesamiento, la memoria o el ancho de banda. Esto puede lograrse mediante el envío de solicitudes de conexión legítimas pero abrumadoras, como solicitudes HTTP GET, hasta que el sistema ya no pueda responder a las solicitudes legítimas de los usuarios.

- Ataques de amplificación: En estos ataques, los atacantes explotan vulnerabilidades en los protocolos de red para amplificar el tráfico malicioso y aumentar su impacto en el objetivo. Por ejemplo, en un ataque de amplificación DNS (Domain Name System), los atacantes envían solicitudes DNS falsas con la dirección IP de la víctima falsificada a servidores DNS mal configurados, que responden con respuestas amplificadas que inundan al objetivo con tráfico no deseado.

- Ataques de protocolo de capa de aplicación: Estos ataques se dirigen a vulnerabilidades en aplicaciones específicas, como servidores web, servicios de correo electrónico o aplicaciones de mensajería instantánea. Los atacantes pueden enviar solicitudes maliciosas diseñadas para agotar los recursos del servidor objetivo o explotar vulnerabilidades de software para hacer que el servicio sea inaccesible.

- Ataques de SYN flood: En este tipo de ataque, los atacantes envían un gran número de solicitudes de conexión SYN (Synchronize) a un servidor, pero no completan el proceso de conexión, lo que lleva a que el servidor agote sus recursos al mantener conexiones abiertas no utilizadas.

Por tanto, los ataques DDoS pueden ser devastadores para las organizaciones afectadas. Pueden experimentar una interrupción total en sus servicios en línea, lo que resulta en pérdidas financieras, daño a la reputación y la pérdida de la confianza de los clientes. Además, estos ataques pueden ser utilizados como una táctica de distracción mientras los atacantes llevan a cabo intrusiones más profundas en el sistema objetivo.

En resumen, los ataques de denegación de servicio representan una seria amenaza para la disponibilidad y la integridad de los servicios en línea. Con el aumento de la dependencia de la tecnología digital, es crucial que las organizaciones estén preparadas para defenderse contra estos ataques y mantener la continuidad de sus operaciones en un entorno cada vez más interconectado y vulnerable.

Ataques de fuerza bruta:

Los ataques de fuerza bruta representan una de las formas más básicas y persistentes de intentar acceder a sistemas informáticos protegidos. Esta técnica, utilizada por ciberdelincuentes con diversos propósitos maliciosos, implica el uso de programas automatizados para probar una amplia gama de combinaciones posibles de nombres de usuario y contraseñas con el objetivo de encontrar las credenciales correctas que les permitan ingresar a un sistema o cuenta en línea.

El proceso detrás de un ataque de fuerza bruta es relativamente simple pero efectivo. Los atacantes utilizan software especializado que genera

automáticamente múltiples combinaciones de contraseñas, desde secuencias alfabéticas hasta combinaciones numéricas y caracteres especiales. Estas herramientas prueban continuamente estas combinaciones contra la interfaz de inicio de sesión de un sistema o aplicación web, intentando autenticarse repetidamente hasta que encuentren una combinación válida.

Los objetivos de los ataques de fuerza bruta pueden ser diversos. Desde acceder a cuentas de correo electrónico y redes sociales para robar información personal o financiera, hasta comprometer sistemas empresariales para acceder a datos sensibles o realizar acciones maliciosas. Además, este tipo de ataques puede ser utilizado para comprometer la seguridad de dispositivos IoT, sistemas de punto de venta, servidores y cualquier otra plataforma que requiera autenticación.

A pesar de su simplicidad, los ataques de fuerza bruta pueden ser devastadores si no se toman medidas adecuadas de seguridad. Para protegerse contra estos ataques, es fundamental seguir buenas prácticas de seguridad, como utilizar contraseñas robustas y únicas para cada cuenta, implementar la autenticación multifactor (MFA) siempre que sea posible, y monitorear activamente los intentos de inicio de sesión sospechosos. Además, los administradores de sistemas y desarrolladores de aplicaciones deben implementar medidas de seguridad adicionales, como el bloqueo automático de cuentas después de un número determinado de intentos fallidos de inicio de sesión, para mitigar el riesgo de ataques de fuerza bruta. En última instancia, la conciencia y la preparación son clave para defenderse contra esta forma común pero persistente de ciberataque.

Ataques de inyección SQL:

La inyección SQL es una de las vulnerabilidades más comunes y peligrosas que pueden afectar a las aplicaciones web en la actualidad. Este tipo de ataque aprovecha las debilidades en la forma en que las aplicaciones interactúan con las bases de datos, permitiendo que los atacantes ejecuten comandos SQL no autorizados.

En un ataque de inyección SQL, los ciberatacantes aprovechan los campos de entrada de usuario en formularios web u otros puntos de acceso a una aplicación. Utilizan estos campos para insertar código SQL malicioso en las consultas que se envían a la base de datos subyacente. Una vez que el código malicioso se ejecuta en la base de datos, los atacantes pueden realizar una variedad de acciones

perjudiciales, como robar datos confidenciales, modificar o eliminar datos, o incluso tomar el control total del sistema.

Los ataques de inyección SQL pueden tener consecuencias devastadoras para las organizaciones y los usuarios. Los datos sensibles, como información personal, credenciales de inicio de sesión, detalles de tarjetas de crédito o información empresarial confidencial, pueden ser comprometidos. Esto puede conducir a robos de identidad, fraudes financieros, pérdida de reputación y otros daños graves.

Para prevenir los ataques de inyección SQL, es crucial que los desarrolladores adopten buenas prácticas de programación segura. Esto incluye el uso de parámetros de consulta parametrizados o el uso de API de acceso a la base de datos que automatizan la creación de consultas SQL seguras. Además, las aplicaciones deben ser probadas regularmente en busca de vulnerabilidades y se deben implementar medidas de seguridad adicionales, como firewalls de aplicaciones web y sistemas de detección de intrusiones.

Los usuarios también pueden protegerse contra los ataques de inyección SQL teniendo cuidado al interactuar con aplicaciones web. Evitar hacer clic en enlaces sospechosos o descargar archivos de fuentes no confiables puede ayudar a prevenir que los atacantes aprovechen vulnerabilidades en las aplicaciones.

En resumen, los ataques de inyección SQL representan una seria amenaza para la seguridad en línea. Con conciencia, educación y prácticas de desarrollo seguras, podemos trabajar juntos para mitigar este riesgo y proteger nuestros sistemas y datos contra los ciberdelincuentes.

8.CONCLUSIONES

9.BIBLIOGRAFIA

Sitio Web oficial de Suricata (IDS): https://suricata.io/

Documentación oficial sobre Suricata: https://docs.suricata.io/en/latest/index.html

Sitio Web oficial de Splunk (SIEM): https://www.splunk.com/

Universal Splunk Forwarder: https://www.splunk.com/en_us/blog/learn/splunk-universal-forwarder.html

Configurar universal splunk forwarder: https://www.youtube.com/watch?v=rs6q28xUd-o