**ANEXO “A”**

**CAPITULO 4: Resultados y discusión**

**Desarrollo Sprint 3 - 2020**

1. **Objetivo del sprint**

En este Sprint se cubrirá el objetivo específico **OE1** “Visualizar comportamientos anómalos de los equipos y usuarios de una determinada red”.

Al implementar la historia de usuario **HU-PA03** “Quiero generar y visualizar ataques en la sistema de correlación de eventos”.

Se implementarán siguientes servidores y herramientas:

1. 01 Firewall Open Source **“pfSense”.**
2. 01 Servidor **LAMP** con **“Mutillidae”.**
3. 01Herramienta generadora de **Ataques**.

1. **Product Backlog**

A continuación, se presenta el Product Backlog completo para el Proyecto, este se encuentra priorizado con la técnica MoSCoW y la asignación de los puntos de historia con la estimación de serie Fibonacci.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID HU** | **Rol ¿Quien?** | **Característica Funcionalidad Objetivo ¿Quiero?** | **Razón Resultado ¿Para qué?** | **Prioridad** | **Pts Hist HU** | **# Sprint** |
|  | - |  |  |  |  |  |
| HU-PA01 | Como operador | Quiero visualizar alertas en caso de que ocurra una anomalía en la red. | Para tener una visualización rápida de las anomalías. | M | 8 | 1 |
|  | - |  |  |  |  |  |
| HU-PA02 | Como operador | Quiero recibir un correo electrónico en el cual se indique el incidente informático. | Para en caso de no estar en las dependencias, saber que incidente esta ocurriendo. | S | 13 | 2 |
|  | - |  |  |  |  |  |
| HU-PA03 | Como Mantenedor | Quiero generar y visualizar ataques en la sistema de correlación de eventos. | Para poder discriminar entre un incidente y un falso positivo. | M | 13 | 3 |
|  | - |  |  |  |  |  |
| HU-PA04 | Como operador | Quiero poder visualizar el estado de los dispositivos conectados a la red. | Para poder determinar que dispositivo se encuentra con problemas. | M | 13 | 4 |
|  | - |  |  |  |  |  |
| HU-PA05 | Como administrador | Quiero poder customizar patrones de detección en base a requerimientos. | Para poder detectar lo desconocido en la red. | M | 13 | 5 |
|  | - |  |  |  |  |  |
| HU-PA06 | Como administrador | Quiero poder implementar dicho sistema y que sea escalable, en el sentido de que se puedan agregar mas dispositivos. | Para poder tener una mejor visualización del estado de la red. | M | 13 | 1 |
|  | - |  |  |  |  |  |
| HU-PA07 | Como administrador | Quiero implementar un sistema que logre detectar patrones anómalos de comportamiento. | Para entregar una mejor visualización a los encargados de Seguridad TI. | M | 20 | 7 |
|  | - |  |  |  |  |  |
| HU-PA08 | Como administrador | Quiero crear reglas de detección de patrones anómalos de comportamiento. | Para poder detectar comportamientos anómalos en la red. | M | 13 | 6 |

**Tabla 4.1: Product Backlog**

1. **Sprint Backlog**

La siguiente tabla representa el Sprint Backlog planificado para el primer sprint, donde se asigna la estimación de horas de trabajo necesarias para completar cada tarea.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sprint #** | **3** | **Días Inicio Sprint** | **0** | **Inicio Puntos de Historia** | **40** |
| **Fecha de Inicio** | **20-04-2020** | **Días Termino Sprint** | **21** | **Término Puntos de Historia** | **0** |

|  |  |  |
| --- | --- | --- |
| **ID Tarea** | **Descripción** | **Estimación Inicial** |
| HU-PA03.T1 | Configurar de manera correcta los paneles, dispositivos y herramienta generadora de ataques. | 5 |
| HU-PA03.T2 | Agregar dispositivo que permita detectar anomalías en la red (pfSense - Snort). | 8 |
| HU-PA03.T3 | Efectuar pruebas, objeto visualizar alertas de seguridad. | 3 |
| HU-PA09.T1 | Coordinar Horario con profesor Guía Asistir a reunión y mostrar avances o realizar consultas Coordinar requerimientos de Product Owner Actualizar bitácora de reuniones | 2 |
| HU-PA10.T1 | Coordinar Horario con Cliente Asistir a reunión y mostrar avances o realizar consultas Coordinar requerimientos de Product Owner Actualizar bitácora de reuniones | 2 |
| HU-PA11.T1 | \_ Actualizar el Plan del Proyecto de Control de Cambios \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA12.T1 | \_ Actualizar el Plan del Proyecto de Control de la Configuración \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA13.T1 | \_ Actualizar el Plan del Proyecto Plan de Calidad \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA14.T1 | \_ Actualizar el Plan del Proyecto de Gestión de Riesgos \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA15.T1 | \_ Actualizar el Plan del Proyecto del Cronograma \_ Actualizar el Plan del Sprint \_ Integrar Plan del Sprint al Anexo de la Memoria | 2 |
| HU-PA16.T1 | Subir Códigos o archivos del entregable a Github o Drive, comentar los Commit o Branch y Documentar | 2 |
| HU-PA17.T1 | Realizar todas las pruebas necesarias para que el entregable quede sin errores y funcionando en producción, luego generar el Release en GitHub, asignar un TAG y documentar | 2 |
| HU-PA18.T1 | Entregar el documento al Cliente, para que tome conocimiento de todos los atributos o requisitos que se consideraron en el entregable, e indique si tiene observaciones | 2 |
| HU-PA19.T1 | Reunir todas las evidencias de avance del Sprint y redactar el Documento enfocandose en todos los puntos de la Pauta de corrección | 2 |
| HU-PA20.T1 | Reunir todas las evidencias de avance del Sprint y redactar el PowerPonit enfocandose en todos los puntos de la Pauta de corrección | 2 |

**Tabla 4.2: Sprint backlog**

1. **Duración del sprint**

Se establece que la duración para cada Sprint será de 3 semanas, el inicio de este será el día 20 de abril de 2020 y terminará el día 10 de mayo de 2020.

1. **Criterios de aceptación**

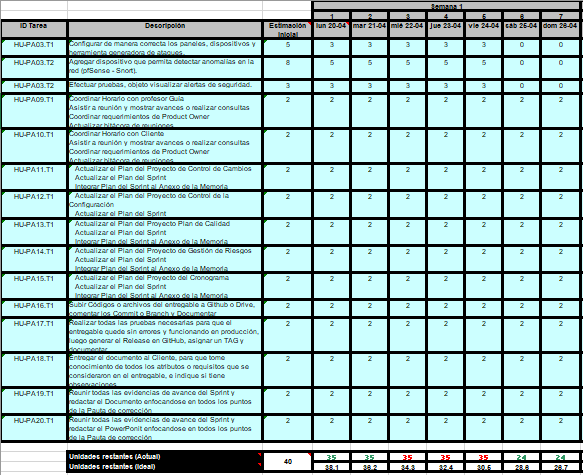
A continuación, se presentan los criterios de aceptación para la HU-PA03 que se desarrollara en el Sprint 3 (Hito-2) 2020.

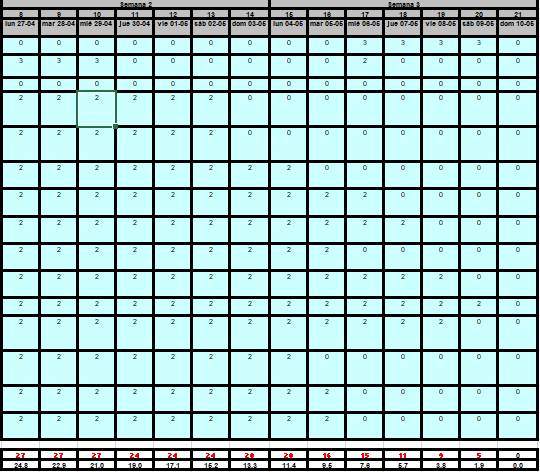
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CRITERIOS DE ACEPTACIÓN** | | | | | |
| **Número de**  **escenario** | **Criterio de aceptación (Título)** | **Contexto** | **Evento** | **Resultado / Comportamiento esperado** | **Estado** |
|  |  |  |  |  |  |
| E1 | HU-PA03.T2.E1 - Parseo generado correctamente desde FW pfSense. | Dentro del sistema debo poder visualizar el evento detectado por Snort. | Al seleccionar y hacer clic en Event, dentro de pfSense. | Visualizar evento gatillado en pantalla. | 100 % |
| E2 | HU-PA03.T2.E2 - Ataque generado desde plataforma Mutillidae | Al seleccionar ingresar a plataforma Mutillidae y seleccionar tipo de ataque. | Al seleccionar y hacer clic en Menu izquierdo Owasp 2017. | Visualizar el envio del ataque. | 100 % |
| E3 | HU-PA03.T2.E3 - Dashboard con detalle de anomalias en la red. | Al seleccionar en el menú superior "Search", filtrar por message o clasificación. | Al seleccionar y hacer clic en message y luego quick value. | Visualizar Dashboard tipo torta y tabla con detalle de incidente. | 100 % |

**Tabla 4.3: Criterios de aceptación**

1. **Seguimiento para Sprint 1**

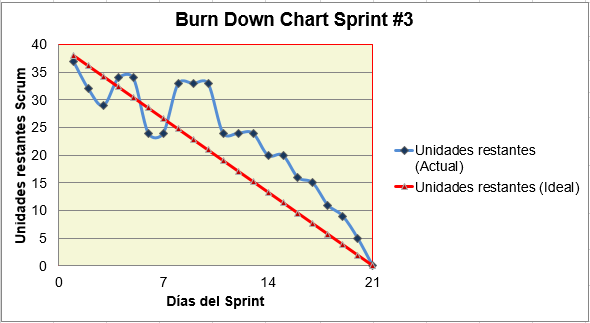
1. **Sprint Planning**





**Tabla 4.4: Seguimiento de sprint 1 backlog**

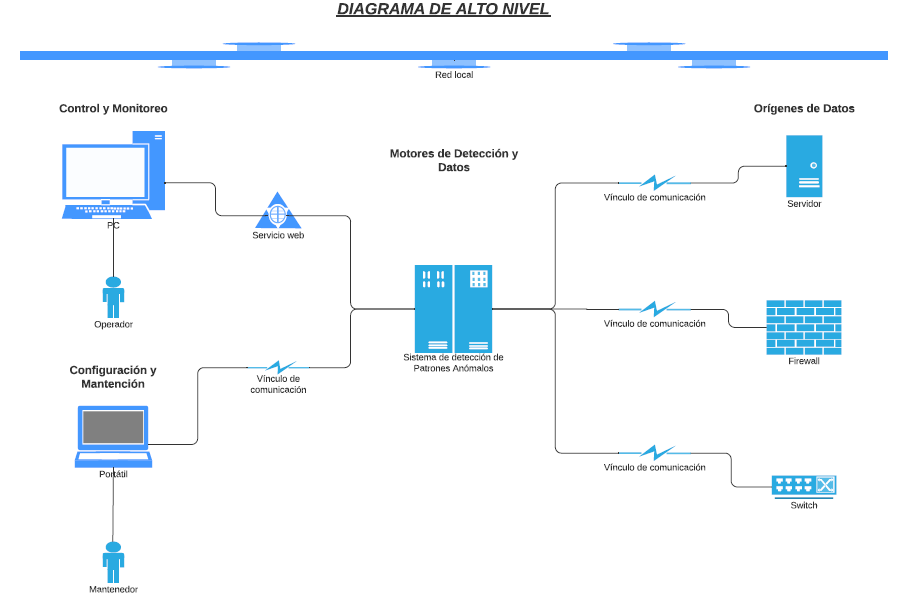
1. **Sprint 3 Burn Down Chart**



**Figura 4.5: Burn down chart**

1. **Arquitectura de la aplicación**

1. **Diagrama de Alto nivel**



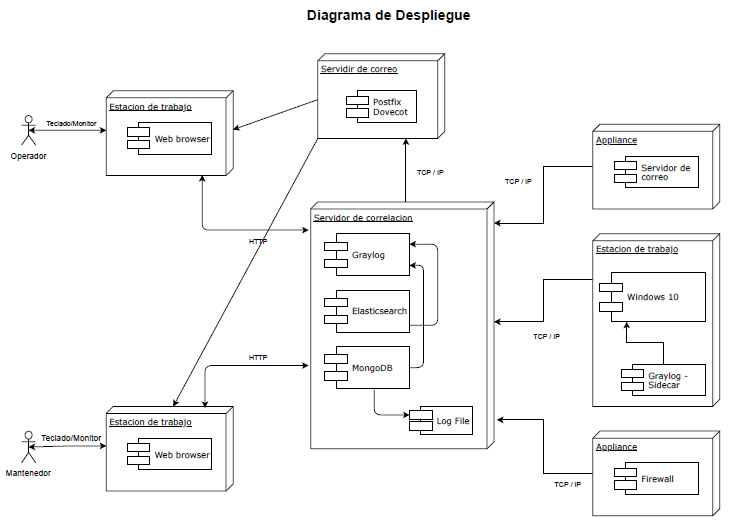
**Figura 4.6: Diagrama de Alto Nivel**

En la figura 4.6 se muestra el diagrama de Alto Nivel para la implementación del sistema, aquí podemos ver en forma macro 4 componentes o grupos de trabajo vistos desde bien arriba, los cuales son:

* **Control y monitoreo:**Este componente del diagrama esta destinado para el operador del sistema (Seguridad TI), será el encargado de monitorear, detectar y mitigar los posibles eventos informáticos que se originen.

* **Configuración y mantención:** Esta sección esta destinada al mantenedor, el cual tendrá la labor de dejar implementado y operando en forma optima todo el sistema.
* **Motores de detección y datos:** En este componente se encuentran los principales componentes del sistema, sus motores de correlación, bases de datos, motores de búsqueda, motores de parseo, etc. aquí es donde se realiza la ardua labor de parsear y customizar los diferentes ingresos de datos. Todo esto con el objetivo de entregar una mejor visualización al operador.
* **Data source:** Estos son los componentes encargados de alimentar a este gran sistema y a su vez también son los interesados en que sus comportamientos sean monitoreados. Debemos tener en cuenta que gran parte de estos logs nunca son observados, entonces con este sistema podremos ver efectivamente que es lo que sucediendo en segundo plano.

1. **Diagrama de despliegue**



**Figura 4.7: Diagrama de Despliegue**

En la figura 4.7 se muestra el diagrama de Despliegue para la implementación del sistema, en donde podemos observar lo siguiente:

* **Estación de trabajo Operador:**Aquí la comunicación e interacción con el sistema se realiza a través del protocolo http y por el puerto 9000, puerto que utiliza el correlacionador para poder interactuar con su interfaz de visualización.

* **Estación de trabajo Mantenedor:** Aquí la comunicación e interacción entre los distintos módulos que componen el sistema se realiza a través de:

- ssh (puerto 22)

- Vmware Workstation con máquinas Ubuntu 16.04.

- AnyDesk para servidor Ubuntu alojado en red UNAB.

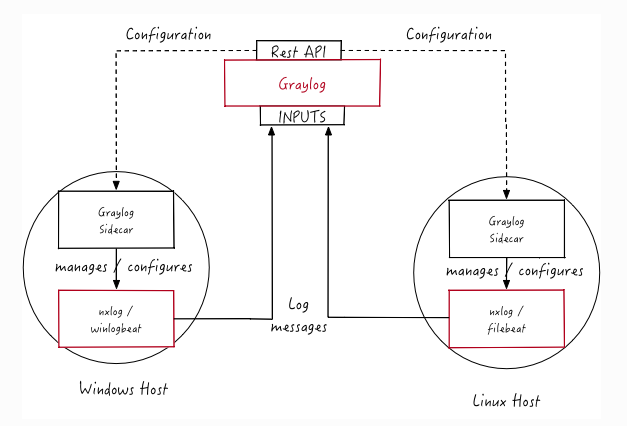
- Protocolo http, puerto 9000.

* **Servidor de correlación:** En este servidor Ubuntu 16.04 LTS, se encuentran alojados los siguientes módulos:
  + Graylog, correlacionador de eventos (Orquestador).
  + Elasticsearch, sistema de almacenamiento de trazas.
  + MongoDB, base de datos de configuración.
* **Orígenes de datos:** Los diferentes orígenes de datos enviar sus logs directamente a este correlacionador de eventos o también a través de intermediarios que en algunos casos son llamados agentes.

Implementación en laboratorio 316 UNAB:

Aquí se utilizaron 5 equipos Windows 10 y se implemento Graylog-Sidecar en cada uno de ellos.

**Graylog Sidecar** es un sistema de administración de configuración para diferentes recolectores de registros, también llamado Backends . Los nodos Graylog actúan como un concentrador centralizado que contiene las configuraciones de los recolectores de registros. En los dispositivos / hosts compatibles, Sidecar puede ejecutarse como un servicio (host de Windows) o daemon (host de Linux).



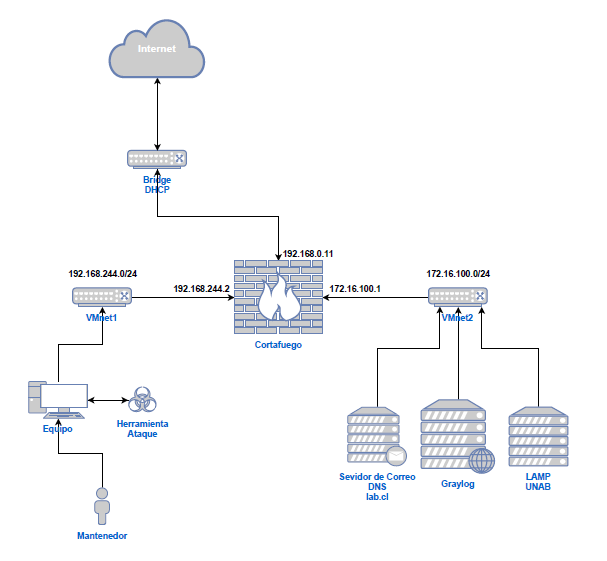
**Figura 4.8: Diagrama Graylog-Sidecar**

**fuente**

* **Servidor de correo:**

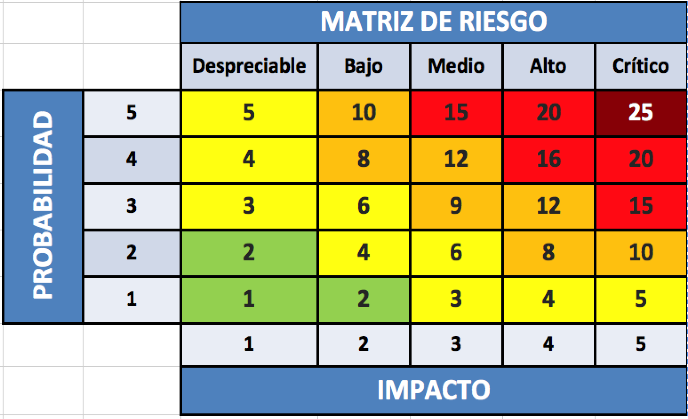
El cual esta compuesto por Postfix y Dovecot, Postfix es un mx (mail exchange) y Dovecot permite que se puedan conectar gestores de correo por imap o pop3, en este caso imap.

1. **Arquitectura Sprint 3**



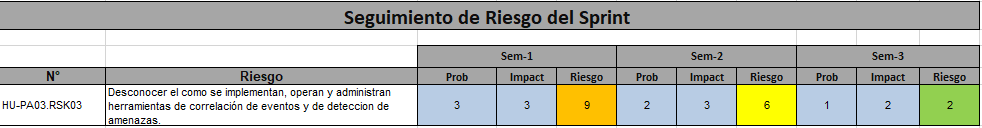
1. **Riesgo técnico del Sprint**

El análisis del riesgo técnico para este sprint se enumera como sigue, la estimación del riesgo se realizó teniendo en cuenta valores de impacto y probabilidad según tabla adjunta.



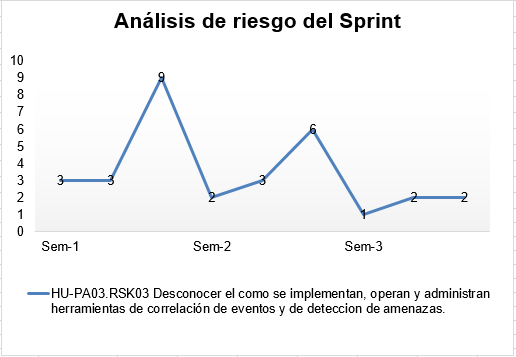
**Figura 4.11: Tabla de riesgo**

1. **Análisis de riesgo técnico Sprint 3**



**Tabla 4.12: análisis de riesgo técnico para Sprint 1**

1. **Análisis de riesgo del Sprint 3**



**Tabla 4.13: análisis de riesgo técnico para Sprint 3**

1. **Pruebas de aceptación / desarrollador**

Evidencias en los criterios de Aceptación que están asociados con las HU, en el Sprint Backlog.

1. **Escenario actual:**

Debido a la contingencia y al no ser posible asistir en forma presencial a los laboratorios de la Universidad, se implemento en forma paralela mismo laboratorio, en equipo de la Universidad, al cual se puede acceder en forma remota a través de software “AnyDesk”, de acuerdo a siguiente detalle:

1. 1 - VM Servidor Correo
2. 2 - VM Servidor Correlacionador
3. 1 - Cliente PC

Acceso en forma Remota, de acuerdo a siguiente detalle:

1. Software: Anydesk
2. ID: 120473124
3. Pass: Unab.2020

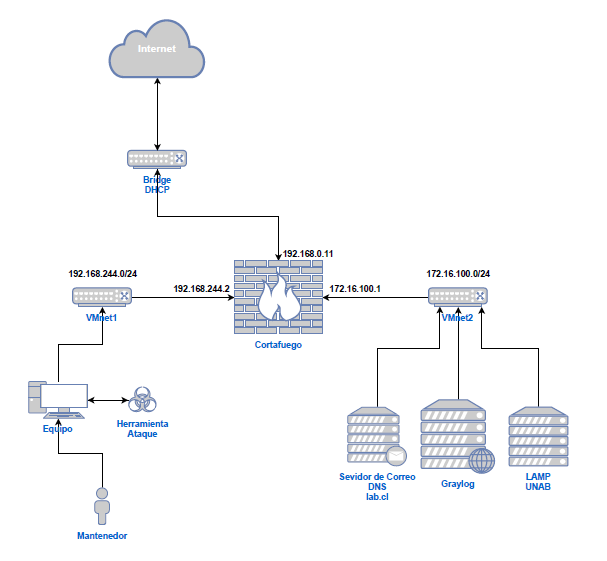
Con esto se logra ingresar al equipo donde se encuentra los equipos y dispositivos que componen este laboratorio.

Posterior a esto abrimos el navegador y accedemos al sistema se encuentra alojado en la siguiente url: <http://192.168.25.129:9000/>, las credenciales para ingresar son:

User : **admin**

Password : **Temeracbeta2020**

Independiente de esta implementación en equipamiento de la Universidad y por motivo de la contingencia actual (COVID-19), las pruebas de aceptación se realizaran en laboratorio implementado de acuerdo a siguiente diagrama:



|  |  |
| --- | --- |
| **Serie** | **SP1 – HU-PA02** |
| Nombre de la prueba | Ataque Web Stress visualizado en el panel de alertas |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al generar un ataque desde la herramienta “Web Stress” el sistema en base a sus reglas cargadas es capaz de detectar y enviar logs al correlacionador de eventos. |
| Historia de usuario | HU-PA03 |
| Pre-condición | * Haber generado un ataque desde “Web Stress”. * Ingresar parámetros para generar ataque, desde “Web Stress” |
| Pasos | * Seleccionar “Run” desde “Web Stress”. * Hacer clic sobre “Search” en Graylog y seleccionar alerta de ataque. * En caso sea requerido se puede realizar búsqueda por otras alertas que estén cumpliendo misma categoría. |
| Resultado esperado | Que la alerta muestre al menos:   * Timestamp * Source * Message |

|  |  |
| --- | --- |
| **Serie** | **SP3 – HU-PA02** |
| Nombre de la prueba | Alerta gatillada detectada por motores en Firewall “pfSense” |
| Tipo de prueba | Prueba unitaria |
| Resumen objetivo | Al generarse un ataque desde “Web Stress” (DDos- Attack) los motores de detección de ataque de pfSense deben detectar ataque y generar un log. |
| Historia de usuario | HU-PA03 |
| Pre-condición | * Haber ingresado en forma correcta al Firewall pfSense. * Ingresar con las credenciales correctas a Firewall. * Levantar herramienta “Web Stress” (DDos-Attack). |
| Pasos | * Seleccionar el menú principal de Firewall pfSense. * Ejecutar herramienta “Web Stress”: * Ingresar IP de la victima y cantidad de Thread. * Hacer clic en el botón “Run” * Visualizar widget de logs y verificar la cantidad de logs que se gatillan. |
| Resultado esperado | Que el widget de log genere una alta cantidad de detecciones del ataque que se esta realizando, debieran aparecer logs del tipo:   * Snort * Barnyard2 * nginx |

1. **Escenario anterior:**

El sistema se encuentra alojado en la siguiente url: <http://10.40.5.25:9000/>, a la cual se puede acceder desde los equipos de la red del laboratorio 306 (las islas de al fondo de la sala), las credenciales para ingresar son:

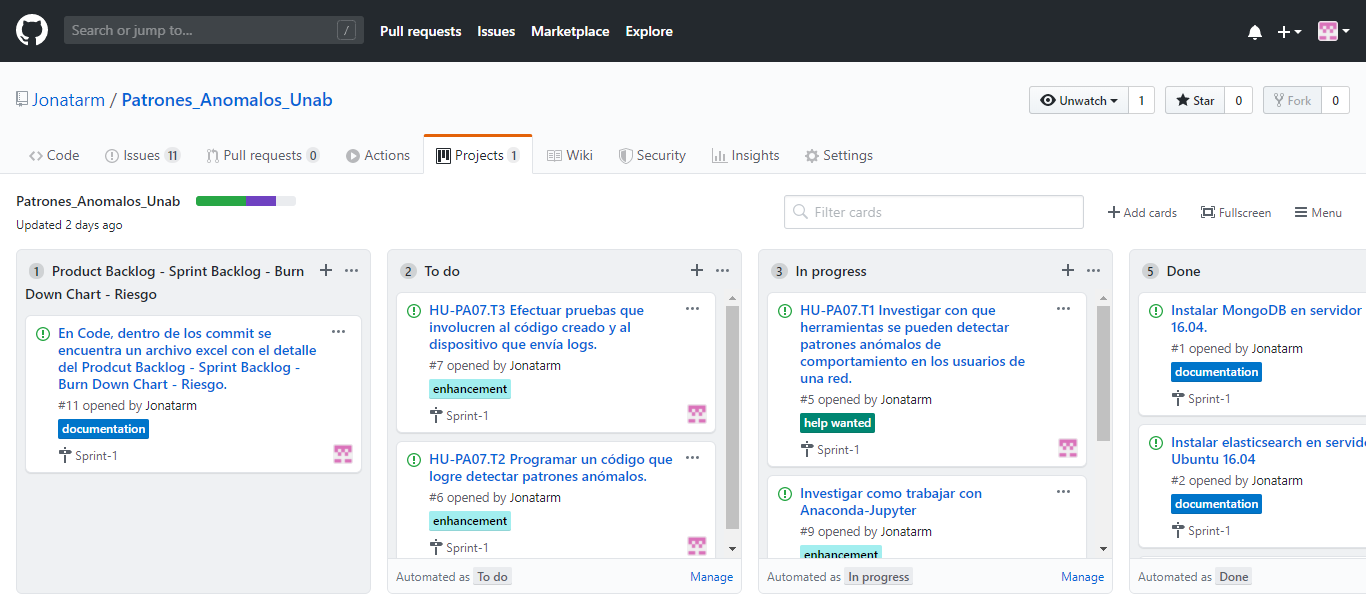
User : **admin**

Password: **Unab2020\***

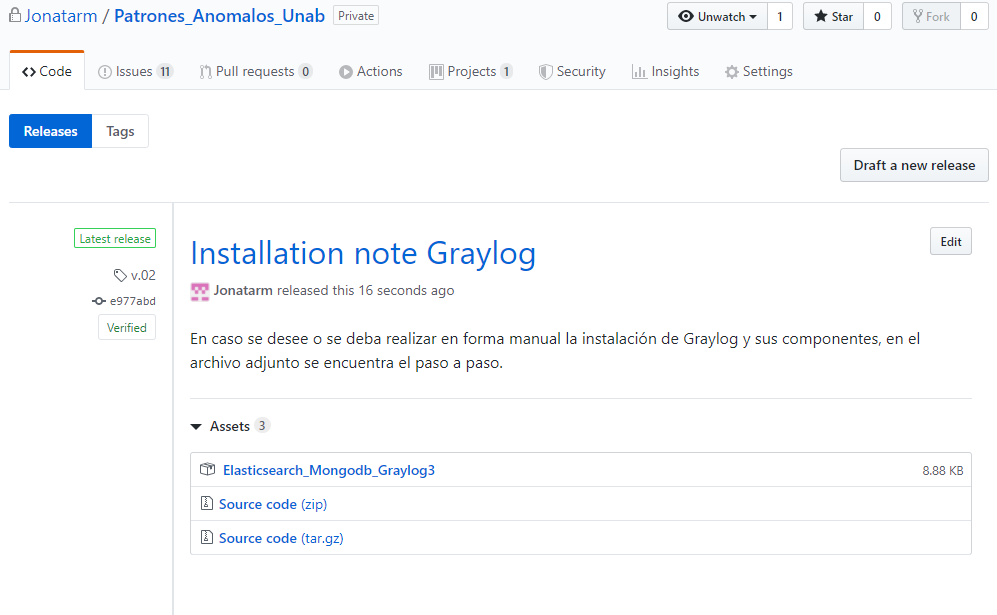
1. **Plan de control de versiones**

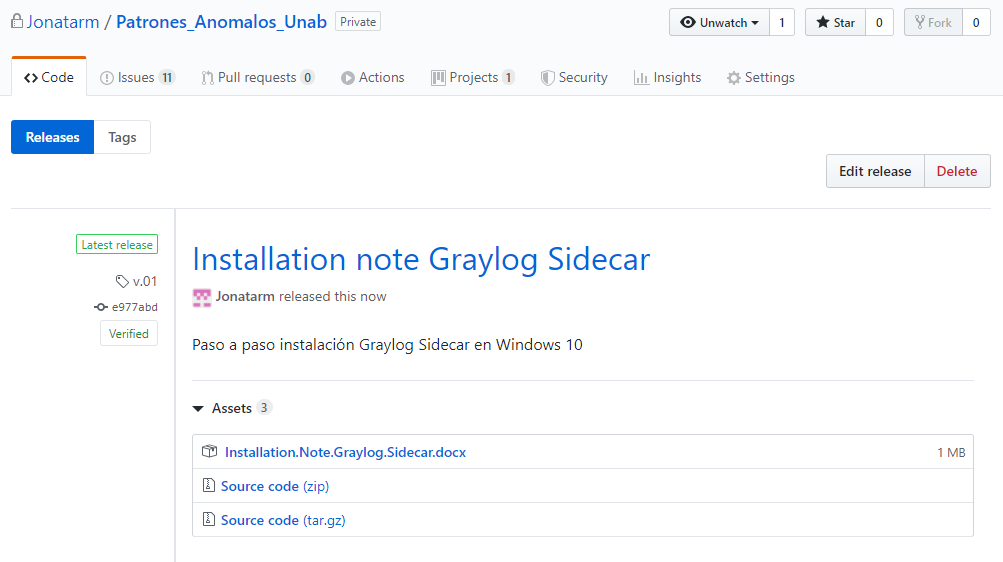
El control de versiones se mantiene según se menciona en el capítulo 3: Materiales y métodos. Este sprint se libera como la versión v.03 para la aplicación.

GitHub : <https://github.com/Jonatarm/Patrones_Anomalos_Unab/projects/1>

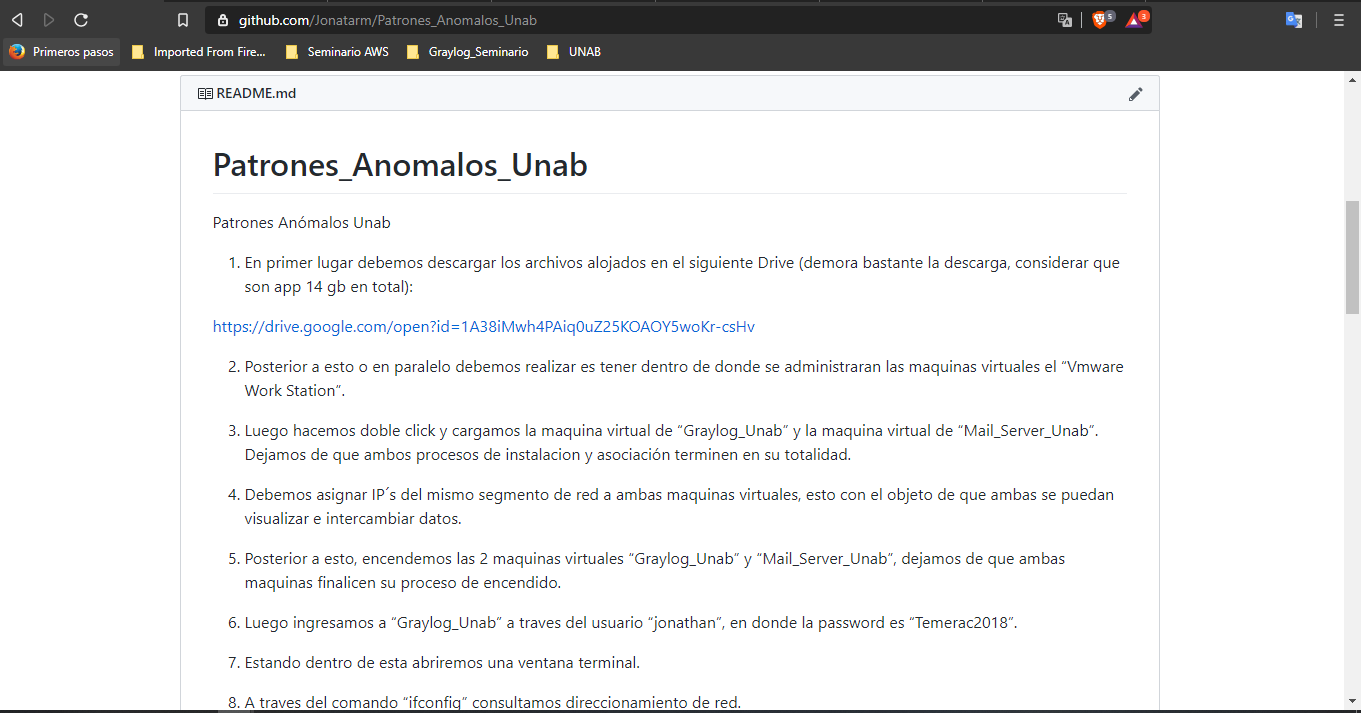


**Figura 4.14 Liberación aplicación web GitHub**

**Figura 4.15 Installation note Graylog**

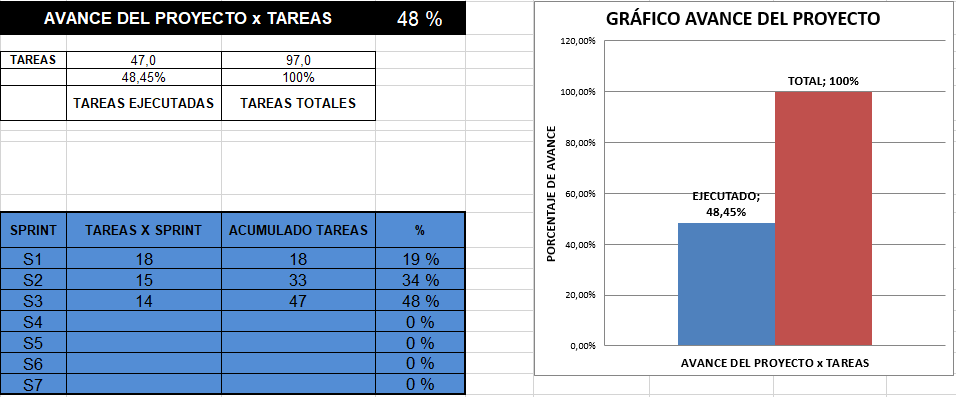


**Figura 4.16 Installation note Graylog Sidecar**

****

**Figura 4.17 readme.md**

1. **Métricas Producto / Proyecto**

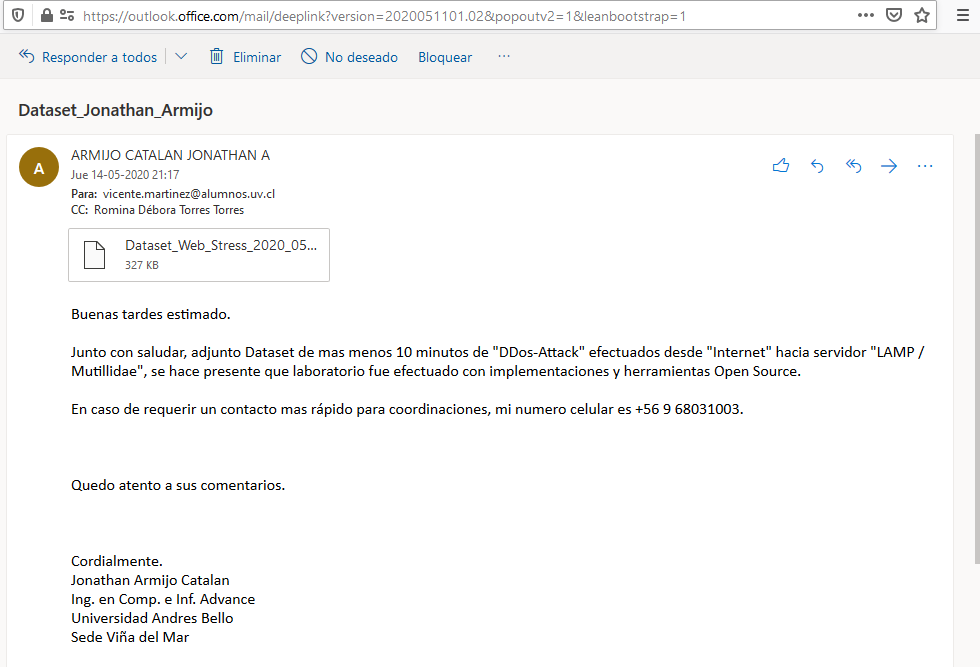
****

1. **Post Morten**

Las pruebas con el cliente y aceptación del producto fueron realizadas de forma remota a raiz de la contingencia que nos afecta actualmente.

En esta sesión en la que participo el Product Owner y el Cliente se demostro como esta funcionando actualmente el sistema y como operan sus distintos modulos.

A su vez se determino extraer los logs del tipo de ataque efectuado del tipo “Web Stress” y enviarlos a la cuenta de correo del alumno Vicente Martinez para la evaluación de estos y la comparacion con el Dataset de Mustafa.



1. **Capítulo 5: Conclusiones**

A continuación, se detalla la lección aprendida en este Sprint 3:

La pandemia “COVID-19” que nos afecta a nivel mundial, ha provocado que todas las coordinaciones, reuniones, acuerdos, etc. se realicen en forma mas lenta y no con la regularidad esperada.

Sin perjuicio de lo anterior, se estima que se ha logrado sacar adelante este Sprint en su totalidad.

1. **Problemas abiertos:**

Durante el desarrollo del proyecto se han encontrado problemas, los que se detallan a continuación.

Se ha detectado en este Sprint que es de vital importancia para la correcta visualización y parsing de los datos, el dominar la creación y comprensión de expresiones regulares, Patrones Grok y JSON.

Respecto principalmente al tiempo que se debe dedicar a la investigación de como trabajan, configuran, operan y customizan los sistemas Open Source en el área de seguridad.

En esto ha sido de vital importancia la profesora guía, ya que gracias a su labor he podido sortear estos inconvenientes.

1. **Trabajo Futuro**

Como trabajo pendiente quedan la realización de las historias de usuario HU-PA04, HU-PA05, HU-PA07, HU-PA08; las cuales están consideradas para los siguientes Sprint.

También como trabajo a corto plazo y con el objeto de entregar una mejor visualización y enriquecimiento de datos (logs) enviados al correlacionador, se debe considerar el crear otros tipos de ataques, con el objetivo de tener una mayor espectro de detecciones.

También se debe considerar el crear parsing detallado de los logs que actualmente se están procesando en el correlacionador de eventos.

1. **Revisión del Sprint 2**

Al finalizar el sprint 3 se realizó una reunión con el Product Owner, para presentar la liberación de los avances para este sprint.

El objetivo programado para este sprint fue de completar la **HU-PA03,** la cual se alineo con el objetivo específico **OE1** “Visualizar comportamientos anómalos de los equipos y usuarios de una determinada red”, establecidos al inicio de este documento, el cual trato de implementar y configurar 01 Firewall Open Source “pfSense”, 01 servidor LAMP con “Mutillidae” y 01 herramienta para la generación de ataques en un sistema controlado.