Se requiere un sistema que tenga capacidad para realizar estudios de ataques web. Para esto debe permitir crear proyectos, cada proyecto tendrá un sistema controlado (honeypot) el cual será objeto de estudio, dependiendo del objetivo del estudio se podrá probar la efectividad de un algoritmo de detección entrenado con un determinado dataset o generar el mismo mediante emulación de ataques y captura de ataques reales. Es importante para esta parte que los ataques que sean realizados puedan ser plenamente identificados para su estudio.

El sistema debe generar reportes de los estudios realizados. Estos reportes deben ser presentados en tablas y gráficos mostrando comparaciones entre los resultados obtenidos por los diferentes datasets usados o los algoritmos probados. Estos reportes deben ser sobre: porcentajes de error como falsos positivos, falsos negativos y aciertos. e información adicional dependiendo de lo que se haya testeado.

El sistema debe permitir el manejo de usuarios y roles. Existen tres roles principales: Administrador de sistema, investigador e usuario común de sniff. El administrador del sistema podrá modificar cualquier parámetro del sistema, el investigador podrá realizar las pruebas en los ambientes creados y realizar las modificaciones a los proyectos de los cuales haga parte. El usuario común de sniff no podrá realizar modificaciones en estos ambientes y solo podra observar los reportes generados.

El sistema debe tener un sistema de alertas de ataques. Cuando la aplicación se encuentre bajo un ataque de “cualquier tipo” debe lanzarse una alerta al administrador del sistema con la información del ataque, tipo de ataque, recursos afectados, que está ocurriendo para que haga las labores necesarias para proteger al sistema del ataque. Adicionalmente se debe realizar una captura de todo el tráfico que ocurra durante el ataque para su posterior análisis y adición a los entornos de investigación.

Estudio ataques web:

* El sistema debe permitir crear un proyecto con: nombre, colaboradores, fecha de creación, autor, estado y tipo de estudio.
* El sistema debe permitir gestionar el versionamiento de cada proyecto.
* El sistema debe permitir adicionar colaboradores a un proyecto.
* El sistema debe permitir remover colaboradores a un proyecto.
* El sistema debe permitir modificar el estado del proyecto
* El sistema debe permitir modificar el tipo de algoritmo de clasificación
* El sistema debe permitir modificar el tipo de entrenamiento del algoritmo
* El sistema debe permitir modificar el dataset de entrenamiento
* El sistema debe permitir añadir vulnerabilidades al ambiente controlado
* El sistema debe permitir remover vulnerabilidades al ambiente controlado
* El sistema debe permitir volver a un estado inicial de un ambiente controlado
* El sistema debe permitir realizar ataques a un ambiente controlado
* El sistema debe permitir configurar los ataques al ambiente controlado tipo de vulnerabilidades y frecuencia de los ataques.

Reportes:

* El sistema debe generar reportes comparativos con los cambios realizados en los proyectos: indicadores estadísticos para la evaluación de estos (aciertos, falsos positivos, falsos negativos).
* El sistema debe generar reportes de los ataques que se hayan realizado a la aplicación.
* El sistema debe generar reportes de funcionamiento del sistema de detección

Sistema de Roles:

* El sistema debe permitir crear roles, modificar y eliminar roles.

Usuarios:

* El sistema debe permitir crear un usuario con: nombre, correo, contraseña, rol, estado.
* El sistema debe permitir modificar el nombre de un usuario.
* El sistema debe permitir modificar un rol a un usuario.
* El sistema debe permitir modificar la contraseña de un usuario.
* El sistema debe permitir cambiar el estado de un usuario.
* El sistema debe permitir limpiar una contraseña mediante un correo.

Servicio de análisis:

* Capacidad de analizar una captura de tráfico web para determinar si pertenece a un ataque y a qué tipo.

Administración del sistema

* El sistema debe poder modificar sus parámetros.

Requerimientos no funcionales:

* Escalable
* Interoperable
* Mantenible
* Modificable
* Parametrizable
* Seguro

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUU01** |
| **Nombre** | Generar Reporte Resultados |
| **Actor Principal** | Usuario Común |
| **Objetivo en Contexto** | Generar un reporte de resultados de un archivo pcap proporcionado por el usuario determinando si la captura pertenece o no a un cyberataque |
| **Precondiciones** | El sistema tiene activo un metodo de detección de cyberataques |
| **Disparador** | El usuario común hace uso de la funcionalidad |
| **Escenario** | 1. Usuario: activa la función 2. Usuario: Sube un archivo de tipo pcap 3. Sistema: Analiza el archivo 4. Sistema: Genera un reporte con los ataques encontrados si se encontraron 5. Usuario: Descarga el reporte generado |
| **Excepciones** | 1. El archivo subido no es de formato pcap 2. Mensaje de error indicando que el formato no es compatible |
| **Prioridad** | Deseable |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI01** |
| **Nombre** | Crear Proyecto |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Crear un proyecto de investigación para que tenga todas las características necesarias |
| **Precondiciones** | El investigador debe haber ingresado al sistema con exito |
| **Disparador** | El investigador inicia la función |
| **Escenario** | 1. El investigador inicia la función 2. El investigador diligencia el nombre y tipo de estudio 3. El sistema agrega un nuevo proyecto 4. Inicia el caso de uso CUI0 5. Inicial el caso de uso CUI0 |
| **Excepciones** | 1. El nombre del proyecto ya existe 2. Mensaje de excepción indicando que el nombre de proyecto ya existe |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI02** |
| **Nombre** | Login |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Permitir al investigador acceder a las funciones del sistema |
| **Precondiciones** | El investigador posee una cuenta válida |
| **Disparador** | El investigador intenta ingresar al sistema |
| **Escenario** | 1. El investigador ingresa al sistema 2. El investigador ingresa su usuario 3. El investigador ingresa su contraseña 4. El investigador ejecuta la función de ingreso 5. El sistema verifica los datos de acceso 6. El investigador ingresa al sistema |
| **Excepciones** | 1. El usuario o contraseña son invalidos 2. El investigador tiene una cuenta que se encuentra deshabilitada 3. El sistema muestra un mensaje de error indicando los fallos por los cuales no se pudo ingresar |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI03** |
| **Nombre** | Editar Proyecto |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Permitir al investigador crear nuevas versiones del mismo proyecto o modificar los colaboradores de este |
| **Precondiciones** | El investigador ingreso correctamente al sistema |
| **Disparador** | El investigador inicia la función |
| **Escenario** | 1. El investigador ejecuta la función 2. El investigador selecciona editar colaboradores 3. Inicial el caso de uso CUI0 4. El investigador selecciona crear nueva versión 5. Inicial el caso de uso CUI0 6. El investigador selecciona editar estado 7. El investigador selecciona el nuevo estado: en proceso, abandonado, terminado |
| **Excepciones** | 1. El proyecto se encuentra en estado finalizado 2. El sistema lanza un mensaje indicando que el proyecto no se puede editar |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI04** |
| **Nombre** | Generar Reporte Investigación |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | El investigador desea conocer los resultados de una versión del proyecto o su comparación con respecto a otra versión del mismo proyecto |
| **Precondiciones** | El investigador debe haber ingresado correctamente al sistema.  Debe existir un proyecto con una versión. |
| **Disparador** | El investigador ejecuta la función |
| **Escenario** | 1. El investigador ejecuta la función 2. El investigador selecciona el reporte de resultados de la versión actual 3. El investigador selecciona si desea comprar los resultados con otra versión 4. El sistema genera un reporte con los datos deseados 5. El investigador decide descargar o no los resultados |
| **Excepciones** |  |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI05** |
| **Nombre** | Editar Participantes |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | El investigador desea editar los participantes que se encuentran trabajando en un proyecto |
| **Precondiciones** |  |
| **Disparador** | Se ha iniciado el caso de uso CUI03 |
| **Escenario** | 1. El investigador selecciona remover colaboradores 2. El investigador selecciona los colaboradores a remover 3. El sistema remueve los colaboradores seleccionados 4. El investigador selecciona adicionar colaboradores 5. El investigador ingresa los nombres de usuario de los colaboradores a agregar 6. El sistema adiciona los nuevos colaboradores |
| **Excepciones** | 1. El nombre del usuario a agregar no existe 2. Mensaje de error indicando la inexistencia del usuario identificado con ese nombre de usuario. |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI06** |
| **Nombre** | Crear Versión |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Crear una nueva versión para un proyecto con características específicas para la investigación |
| **Precondiciones** | Existe un proyecto  El investigador es colaborador del proyecto |
| **Disparador** | Caso de uso CUI01  Caso de uso CUI03 |
| **Escenario** | 1. El investigador diligencia la nueva versión con nombre y justificación. 2. El investigador selecciona configurar entorno 3. inicio caso de uso CUI0 4. El investigador selecciona configurar Dataset 5. inicia caso de uso CUI0 6. El investigador selecciona configurar cyberataques 7. inicia el caso de uso CUI0 8. El investigador selecciona configurar metodo de aprendizaje. 9. inicia el caso de uso CUI0 |
| **Excepciones** |  |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI08** |
| **Nombre** | Configurar Entorno Controlado |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Realizar las configuraciones necesarias al entorno como posibles vulnerabilidades, sistema operativo y servidores |
| **Precondiciones** | Debe existir una versión |
| **Disparador** | CUI06 |
| **Escenario** | 1. El investigador selecciona el sistema operativo del entorno 2. El investigador selecciona los servidores disponibles que deban ser instalados en el entorno 3. El investigador selecciona qué vulnerabilidades debe ofrecer el entorno controlado |
| **Excepciones** |  |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI09** |
| **Nombre** | Configurar Dataset |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Configurar el dataset con el cual va a funcionar el detector de ataques |
| **Precondiciones** | Existe un entorno controlado |
| **Disparador** | CUI06 |
| **Escenario** | 1. El investigador selecciona un dataset existente o proporciona uno nuevo 2. El sistema carga el dataset |
| **Excepciones** | 1. El dataset subido no cuenta con el formato especificado 2. Mensaje de error que muestre que el dataset es erróneo |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI10** |
| **Nombre** | Configurar Cyberataques |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Configurar los ciberataques que serán realizados al entorno controlado. |
| **Precondiciones** | Existe un entorno controlado |
| **Disparador** | CIU06 |
| **Escenario** | 1. El investigador selecciona los ataques que serán realizados 2. El investigador configura los parámetros de los ataques seleccionados 3. El investigador selecciona la frecuencia de los ataques. |
| **Excepciones** |  |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI11** |
| **Nombre** | Configurar Método de Aprendizaje |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Configurar el método de aprendizaje con el que funcionara el detector de ataques. |
| **Precondiciones** | Existe un dataset y un entorno controlado |
| **Disparador** | CUI06 |
| **Escenario** | 1. El investigador selecciona el algoritmo de detección 2. El investigador selecciona el método de aprendizaje 3. El investigador selecciona la técnica de aprendizaje |
| **Excepciones** | 1. El dataset no tiene las características necesarias |
| **Prioridad** | Importante |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI12** |
| **Nombre** | Crear Usuario |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Crear un nuevo usuario para acceso al sistema |
| **Precondiciones** |  |
| **Disparador** | El administrador ejecuta la función |
| **Escenario** | 1. El Investigadorr ingresa los datos del usuario: nombre, correo, rol y estado. 2. El sistema crea el usuario |
| **Excepciones** | 1. El correo del usuario ya se encuentra registrado 2. La contraseña no cumple con los estandares |
| **Prioridad** | Deseable |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUI13** |
| **Nombre** | Editar Usuario |
| **Actor Principal** | Investigador |
| **Objetivo en Contexto** | Editar los datos del usuario |
| **Precondiciones** | El investigador se ha ingresado exitosamente |
| **Disparador** | El investigador ejecuta la función |
| **Escenario** | 1. El investigador seleciona los datos a editar 2. El investigador diligensia los datos a editar 3. El sistema pide verificación de la contraseña 4. El investigador digita la contraseña 5. El sistema guarda los cambios |
| **Excepciones** | 1. Los datos diligenciados no cumplen con el estándar 2. La contraseña es incorrecta |
| **Prioridad** | Deseable |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUA01** |
| **Nombre** | Crear Rol |
| **Actor Principal** | Administrador |
| **Objetivo en Contexto** | Crear un nuevo rol en el sistema |
| **Precondiciones** |  |
| **Disparador** | El administrador ejecuta la función |
| **Escenario** | 1. El administrador ejecuta la función 2. El administrador diligencia la información del rol: nombre y descripción 3. El sistema crea el nuevo rol |
| **Excepciones** | 1. El nombre del rol ya existe |
| **Prioridad** | Deseable |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUA02** |
| **Nombre** | Editar Rol |
| **Actor Principal** | Adminsitrador |
| **Objetivo en Contexto** | Editar un rol creado |
| **Precondiciones** |  |
| **Disparador** | El administrador ejecuta la función |
| **Escenario** | 1. El administrador ejecuta la función 2. El administrador diligencia los datos a editar 3. El sistema edita el rol |
| **Excepciones** | 1. Los datos diligenciados no cumplen con los estándar |
| **Prioridad** | Deseable |

|  |  |
| --- | --- |
| **Campo** | **Descripción** |
| **Identificador** | **CUA03** |
| **Nombre** | Modificar Parámetros |
| **Actor Principal** | Administrador |
| **Objetivo en Contexto** | Modificar los parámetros del sistema |
| **Precondiciones** |  |
| **Disparador** | El administrador ejecuta la función |
| **Escenario** | 1. El administrador ejecuta la función 2. El administrador selecciona los parámetros a modificar 3. El administrador modifica los parámetros. 4. El sistema guarda los cambios |
| **Excepciones** | 1. Los datos diligenciados no cumplen con el estándar |
| **Prioridad** | Deseable |