**Documento de Casos de Prueba:**

**Nombre del Proyecto:** Cerberus **Versión:** 1.0 **Fecha:** **24/7/23**

**Tipo de Prueba:** Prueba Funcional

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Caso de Prueba | Identificador | Descripción | Función a Probar | Condiciones Iniciales | Flujo | Resultado Esperado | Resultado Obtenido | Estado | Tester |
| Detección de Intrusiones | CP001 | Verificar que el software detecte intrusiones en la red | Detección de intrusiones | El software Cerberus debe estar instalado y configurado | 1. Abrir Cerberus 2. Configurar parámetros de detección 3. Simular intento de intrusión | Generar alerta de intrusión | Se generó una alerta de intrusión correctamente | Satisfactoria | Bryan andion |
| Actualización de Firmas | CP002 | Verificar que Cerberus actualice la base de datos de firmas de seguridad | Actualización de firmas | Cerberus conectado a Internet | 1. Abrir Cerberus 2. Acceder a la configuración de actualización 3. Iniciar actualización | Base de firmas actualizada correctamente | La base de firmas se actualizó exitosamente | Satisfactoria | Bryan andion |
| Generación de Reportes | CP003 | Verificar la generación de reportes de seguridad | Generación de reportes | Datos de seguridad almacenados | 1. Abrir Cerberus 2. Acceder a la sección de generación de reportes 3. Seleccionar tipo de reporte y configurar parámetros 4. Generar reporte | Reporte generado correctamente | El reporte se generó sin problemas | Satisfactoria | Bryan andion |

**Documento de Procedimiento de Prueba:**

**Nombre del Proyecto:** Cerberus **Versión:** 1.0 **Fecha:** **24/7/23**

**Tipo de Prueba:** Prueba Funcional

**Procedimiento de Prueba:**

1. Preparación:
   * Configurar el ambiente de prueba con el software Cerberus instalado y funcionando correctamente.
   * Definir los criterios de aceptación para cada caso de prueba.
2. Ejecución:
   * Realizar cada caso de prueba según los escenarios definidos.
   * Registrar los resultados obtenidos en cada caso de prueba.
   * Identificar y documentar cualquier problema o error encontrado durante las pruebas.
3. Evaluación:
   * Comparar los resultados obtenidos con los criterios de aceptación establecidos.
   * Validar si cada caso de prueba pasó o falló según los resultados obtenidos.
4. Reporte:
   * Generar un informe final que incluya los resultados de cada caso de prueba.
   * Incluir detalles de los incidentes encontrados y acciones correctivas propuestas.

**Documento de Registro de Incidentes de Prueba:**

**Nombre del Proyecto:** Cerberus **Versión:** 1.0 **Fecha 24/7/23**

**Tipo de Prueba:** Prueba Funcional

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Caso de Prueba | Identificador | Descripción del Incidente | Fecha de Registro | Estado | Responsable |
| Detección de Intrusiones | CP001 | No se generó alerta de intrusión | [Fecha de registro] | Fallida | Bryan andion |
| Actualización de Firmas | CP002 | Error en la actualización, base de firmas no actualizada | [Fecha de registro] | Fallida | Bryan andion |
| Generación de Reportes | CP003 | Formato incorrecto en el reporte generado | [Fecha de registro] | Fallida | Bryan andion |