Institut Puig Castellar

Proyecto / Credito de sintesi

Document funcional_Defensor

ALUMNE/GRUP: Jhoan Esteban y Daniel Trias

---

1. Introducción y contexto

El rol del defensor representa la parte encargada de proteger los sistemas frente a posibles ataques. En el ámbito de la ciberseguridad, este rol es fundamental, ya que se centra en la prevención, detección y mitigación de amenazas.

El defensor actuará en un entorno de laboratorio controlado, aplicando medidas de seguridad basadas en la temática semanal estudiada. Su función principal será evitar que el ataque realizado por el atacante cumpla su objetivo o, en su defecto, detectar y minimizar su impacto.

2. Análisis de requisitos

2.1. Requisitos funcionales (RF)

Codigo	Descripción del requisito funcional
RF1	Analizar el tipo de ataque que se va a realizar cada semana.
RF2	Configurar medidas de seguridad adecuadas al ataque estudiado.
RF3	Detectar intentos de ataque durante la simulación.
RF4	Mitigar o bloquear el ataque cuando sea posible.
RF5	Registrar y documentar las acciones realizadas.

2.2. Requisitos no funcionales (RNF)

Codigo	Descripció del requisit no funcional
RNF1	Las defensas se aplicarán únicamente en entornos de laboratorio.
RNF2	El enfoque será preventivo y educativo.
RNF3	Las configuraciones deberán ser estables y reproducibles
RNF4	La documentación será clara y comprensible.

2.3. Restricciones

- No se aplicarán medidas de seguridad en sistemas reales.
- Uso limitado a los recursos disponibles del laboratorio.
- Tiempo de preparación condicionado al calendario semanal.

3. Análisis de usuarios y roles

Objectiu: identificar qui farà servir el sistema i què podrà fer.

Descriu els diferents tipus d'usuari, les seves necessitats i els seus permisos.

Rol	Descripció	Permisos principals
Defensor	Gestiona usuaris i recursos.	Alta, baixa i modificació de dades.

4. Casos de uso / Escenarios de uso

Codigo	Nombre del caso de uso	Actor principal	Descripció	Resultat esperat
CU1	Preparación de defensas	Defensor	Configuración previa de medidas de seguridad	Sistema protegido
CU2	Detección de ataque	Defensor	Identificación de actividad sospechosa	Ataque detectado
CU3	Respuesta al ataque	Defensor	Aplicación de acciones correctivas	Impacto reducido

5. Estructura de la información

La información generada por el rol defensor se organizará de la siguiente manera:

- Tipo de ataque estudiado.
- Medidas de seguridad aplicadas.
- Resultado de la defensa.
- Evidencias obtenidas (logs, capturas o vídeos).
- Conclusiones.

6. Diseño de la interfície

El rol defensor no dispone de una interfaz gráfica propia. La interacción se realiza mediante sistemas operativos, herramientas de seguridad y paneles de configuración.

La documentación y los registros generados actúan como principal medio de consulta.

7. Planificació tècnica

Sistemas operativos: Linux y Windows.

- Entornos: Máquinas virtuales.
- Herramientas: utilidades de seguridad, monitorización y grabación de pantalla.
- Metodología: preparación, detección, respuesta y evaluación.

Las acciones del defensor durante la simulación serán grabadas en vídeo como evidencia de las medidas aplicadas.

8. Anàlisi de riesgos

8.1 Identificación de riesgos

- Configuración incorrecta de medidas de seguridad.
- Falta de detección del ataque.
- Exceso de restricciones que afecten al sistema.

8.2. Valoración y respuesta

Riesgo	Probabilidad	Impacto	Plan de prevención o contingencia
Error de configuración	Media	Alta	Pruebas previas
No detectar el ataque	Media	Alto	Monitorización
Sistema inestable	Baja	Media	Ajustes graduales

9. Validación y criterios de éxito

La defensa se considerará exitosa si:

- El ataque es bloqueado o detectado.
- Se reduce el impacto del ataque.
- Se justifican correctamente las medidas aplicadas.
- Existen evidencias documentadas y audiovisuales.

10. Conclusión

Este documento funcional define el rol del defensor dentro del proyecto de ciberseguridad. A través de este enfoque, se pretende reforzar la importancia de la prevención y la respuesta ante incidentes.