Institut Puig Castellar

Projecte / Crèdit de síntesi

Documento funcional

ALUMNE/GRUP: Jhoan Esteban y Daniel Trias

---

1. Introducción y contexto

La ciberseguridad es un pilar fundamental en el ámbito de los sistemas informáticos actuales. Los equipos, redes y aplicaciones están constantemente expuestos a amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. En este contexto, resulta imprescindible comprender no sólo cómo se defienden los sistemas, sino también cómo funcionan los ataques que los ponen en riesgo.

Con el objetivo de profundizar en el estudio de la ciberseguridad desde una perspectiva tanto ofensiva como defensiva, además de un enfoque puramente teórico, se plantea un modelo basado en la experimentación y la simulación de situaciones reales en entornos controlados.

La solución propuesta consiste en un proyecto práctico de investigación y simulación de ataques y defensas en entornos controlados, con el objetivo de comprender cómo funcionan las amenazas reales y cómo se pueden mitigar.

2. Análisis de requisitos

2.1. Requisitos funcionales (RF)

Codigo	Descripción del requisito funcional
RF1	Comprender el funcionamiento de los ataques más comunes en sistemas informáticos.
RF2	Analizar las vulnerabilidades que pueden ser explotadas en diferentes escenarios.
RF3	Aplicar medidas de defensa adecuadas para prevenir o mitigar los ataques estudiados.
RF4	Fomentar el aprendizaje práctico mediante roles diferenciados (atacante y defensor).
RF5	Evaluar los resultados obtenidos tras cada simulación para mejorar la comprensión de los conceptos.

2.2. Requisitos no funcionales (RNF)

Codigo	Descripción del requisito no funcional
RNF1	Las pruebas se realizan únicamente en entornos de laboratorio.
RNF2	El proyecto tendrá un enfoque educativo y no malicioso.
RNF3	La documentación será clara y comprensible.

2.3. Restricciones

Condicions o limitacions del projecte.

- Uso de máquinas virtuales y sistemas de prueba.
- Recursos disponibles (temps, equip, materials):
- Dependències o limitacions tècniques:

3. Análisis de usuarios y roles

Roles	Descripción	Permisos principales
Atacante	Simula ataques según la temática estudiada	Ejecutar ataques en laboratorio
Defensor	Aplica medidas de seguridad	Configurar defensas
Analista	Monitorizar y concluir los resultados	Revisión del ataque a tiempo real

4. Casos de uso / Escenarios de uso

Codigo	Nombre del caso de uso	Actor principal	Descripción	Resultado esperado
CU1	Investigación del ataque	Atacante / Defensor	Estudio teórico del ataque, su funcionamiento y contexto	Conocimientos adquiridos
CU2	Simulación del ataque	Atacante	Ejecución del ataque en entorno controlado (solo en ataques técnicos)	Ataque exitoso o bloqueado
CU3	Aplicación de defensa	Defensor	Implementación de medidas de protección y mitigación	Sistema protegido o ataque detectado

5. Estructura de la información

El proyecto no gestiona una base de datos como tal, aunque creemos alguna para algún ataque, pero sí una estructura de información organizada por temáticas.

- Temática de ataque.
- Rol asignado (atacante o defensor).
- Entorno utilizado.
- Resultado de la simulación.
- Conclusiones obtenidas.

6. Diseño de la interfície

El proyecto no dispone de una interfaz gráfica propia. La interacción se realiza mediante herramientas de línea de comandos, sistemas operativos y entornos virtualizados.

La documentación escrita y grabaciones de los ataques actuarán como interfaz principal para la comprensión del proyecto.

7. Planificación técnica

El proyecto se desarrollará de forma semanal, dedicando cada semana a una tipología de ataque distinta.

Para los ataques de carácter técnico (red, malware, contraseñas, aplicaciones web, configuración e insider), se realizará una simulación práctica completa en un entorno de laboratorio.

En el caso de ataques basados en ingeniería social, como el phishing, no se llevará a cabo una simulación directa, ya que el conocimiento previo del ataque invalidará su efectividad. En su lugar, se realizará una investigación teórica que incluirá perfiles de posibles víctimas, ejemplos reales y medidas de prevención.

Las simulaciones prácticas de los ataques y defensas serán grabadas en vídeo con el objetivo de disponer de evidencias de su realización y facilitar su explicación durante la presentación del proyecto.

1. Ataques de Ingeniería Social

- Phishing
- Spear phishing
- Smishing / Vishing
- Pretexting
- Baiting

2. Malware

- Virus
- Troyanos
- Gusanos
- Ransomware
- Spyware
- Adware
- Rootkits

3. Ataques de Red

- DDoS / DoS (Denegación de servicio)
- Sniffing (escucha de tráfico)
- Spoofing (suplantación)
- Man-in-the-Middle (MitM)
- Session hijacking

4. Ataques a Aplicaciones Web

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Path traversal
- File inclusion

5. Ataques a Contraseñas

- Fuerza bruta
- Diccionario
- Credential stuffing
- Keylogging

6. Ataques a Configuración o Infraestructura

- Explotación de vulnerabilidades (exploits)
- Privileged escalation (escalada de privilegios)
- Ataques a APIs
- Ataques a contenedores / virtualización

7. Ataques de Insider (internos)

- Robo de datos
- Sabotaje
- Uso indebido de privilegios

8. Análisis de riesgos

8.1. Identificación de riesgos

8.1 Identificación de riesgos

- Falta de tiempo para completar todas las temáticas.
- Dificultad técnica en la implementación de algunos ataques o defensas.
- Errores de configuración en el entorno de laboratorio.
- Pérdida de información o configuraciones.

8.2. Valoración y respuesta

Riesgo	Probabilidad	Impacto	Plan de prevención
Falta de tiempo	Alta	Alta	Buena planificación y organización
Problemes tècnics	Mitjana	Mitjana	Dificultad en los programas o comprensión del ataque/defensa
Error en el laboratorio	Baixa	Alta	Tener backups de los laboratorios.

9. Validación y criterios de éxito

El proyecto se considerará exitoso si:

- Se completaron todas las temáticas previstas.
- Cada ataque y defensa puede ser explicado y justificado.
- Las simulaciones técnicas se realizan correctamente en entornos controlados.
- Se dispone de evidencias audiovisuales que demuestran la realización de las simulaciones.
- Se documentan los resultados obtenidos de forma clara.

La validación se realizará mediante la revisión de la documentación, el análisis de los vídeos grabados y la demostración durante la presentación del proyecto.

10. Conclusión

Este documento funcional común define la base y el enfoque general del proyecto de ciberseguridad. La separación en distintos documentos funcionales permite un análisis más claro y estructurado de los objetivos y responsabilidades de cada rol.

Gracias a este enfoque, el proyecto no solo refuerza los conocimientos teóricos, sino que fomenta el aprendizaje práctico y crítico, acercando a los alumnos a situaciones reales del ámbito de la ciberseguridad.

A partir de este documento, se desarrollan los documentos funcionales específicos del atacante y del defensor, donde se detallan sus objetivos, requisitos y criterios de éxito particulares.