Institut Puig Castellar

Projecte / Crèdit de síntesi

Document funciona_Atacante

ALUMNE/GRUP: Jhoan Esteban y Daniel Trias

Institut Puig Castellar **1**
Projecte / Crèdit de síntesi 1
Document funcional 1
1. Introducció i context 2
2. Anàlisi de requisits 2
2.1. Requisits funcionals (RF) 2
2.2. Requisits no funcionals (RNF) 2
2.3. Restriccions 3
3. Anàlisi d'usuaris i rols 3
4. Casos d'ús / Escenaris d'ús 3
5. Model de dades o estructura de la informació 4
6. Disseny de la interfície 4
7. Planificació tècnica 4
8. Anàlisi de riscos 5
8.1. Identificació de riscos 5
8.2. Valoració i resposta 5
9. Validació i criteris d'èxit 5
10. Conclusió 6

1. Introducción y contexto

El atacante. Se nos suele definir como un usuario o grupos de usuarios con un interés por alterar la seguridad de un sistema, Robar o destruir datos, Pero no tiene porque todo ser malo, Los atacantes también pueden ser analizadores y buscadores de vulnerabilidades en nuestro propio sistema con el fin de saber defender lo nuestro. Queremos ser ese tipo de hacker, Nuestro objetivo en el proyecto es analizar el sistema, buscar fallos y poder atacar, Qué mejor manera de defender una base sabiendo como actúa el enemigo.

2. Análisis de requisitos

2.1. Requisitos funcionales (RF)

Codigo	Descripción del requisito funcionales
RF1	Investigar el funcionamiento del ataque asignado cada semana.
RF2	Preparar el entorno necesario para ejecutar el ataque.
RF3	Ejecutar ataques técnicos en un entorno controlado.
RF4	Intentar evadir o superar las medidas de defensa existentes.
RF5	Documentar el proceso y los resultados del ataque.
RF6	Grabar en vídeo la ejecución del ataque cuando sea posible.

2.2. Requisitos no funcionales (RNF)

Codigo	Descripción del requisito no funcional
RNF1	Los ataques se realizan únicamente con fines educativos.
RNF2	No se atacarán sistemas reales ni externos
RNF3	Los ataques deberán ser reproducibles

2.3. Restricciones

- Uso exclusivo de máquinas virtuales.
- Ataques limitados al entorno del laboratorio.

3. Anàlisi d’usuaris i rols

Roles	Descripción	Permisos principales
Atacante	Simula ataques según la temática estudiada	Ejecutar ataques en laboratorio

4. Casos d’ús / Escenaris d’ús

Como comentamos anteriormente en el contexto, Realizaremos 7 casos de ataques, Como se observa en la tabla

Codi	Nom del cas d’ús	Actor principal	Descripció	Resultat esperat
CU1	Investigación y preparación del ataque	Atacante	Investigar y preparar el método de ataque.	Conocimiento y Preparación
CU2	Comienzo del ataque	Atacante	Comenzar la Simulación del Ataque	Ataque con éxito. Ataque Bloqueado.
CU3	Análisis de resultados	Atacante	Analizar los resultados obtenidos para su correspondiente Documentación	Documentación del proceso.

5. Estructura de la información

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

- Tipo de ataque realizado
- Herramientas utilizadas
- Sistema objetivo
- Resultado obtenido
- Evidencias (videos y capturas)
- Conclusiones del ataque

6. Diseño de la interfície

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

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

7. Planificación técnica

El atacante dedicará cada semana a la preparación y ejecución del ataque asignado.

En ataques técnicos se realizará una simulación práctica completa. En ataques de ingeniería social se hará un estudio teórico, análisis de perfiles vulnerables y ejemplos reales, sin simulación directa.

Las ejecuciones técnicas serán grabadas en video como prueba del trabajo realizado.

8. Análisis de riesgos

8.1 Identificación de riesgos

- Ataques demasiado complejos.
- Errores de configuración en el entorno.
- Pérdidas de evidencia

8.2. Valoración y respuesta

Riesgos	Probabilidad	Impacto	Plan de prevención
Ataque demasiado complejo	Media	Alto	Ajusta los ataques acorde al nivel
Errores de configuración	Media	Alto	Pruebas previas
Pérdidas de evidencia	Baja	Alta	Realizar backups

9. Validació i criteris d'èxit

El ataque se considera Exitoso cuando cuando la mayoría de los puntos siguientes se cumplan:

1. El ataque cumple con su objetivo final.
2. El ataque nos enseña fallas en el sistema y nos permite mejorar la defensa del defensor.
3. La respuesta del servidor o cliente defensor bloquea o rechaza el ataque con éxito, lo que valida la seguridad del mismo.
4. La simulación del ataque permite realizar una documentación de calidad para el aprendizaje.

10. Conclusió

Como conclusión final con esta parte del documento definimos lo que será el rol del atacante y todo lo que se espera conseguir con este, Aprenderemos temas interesantes y complejos que pueden llevarnos a situaciones difíciles. así creando una metodología de estudio donde se investiga y se pone a prueba.

Mejoramos y masterizamos el uso de máquinas virtuales, comandos y navegación profunda. tendremos la función de encontrar huecos en nuestro sistema, consiguiendo así la mejor seguridad para el mismo.

Con la idea del proyecto clara y la teoría realizada, Los siguientes pasos serán comenzar a crear el entorno de pruebas, los procesos de investigación y documentación del mismo. A partir de ahora comienza la parte de desarrollo del proyecto.