Ingeniería de la Ciberseguridad
Curso 2023/2024

Práctica 1
Sesión práctica 5:

Modelado de amenazas

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

ÍNDICE

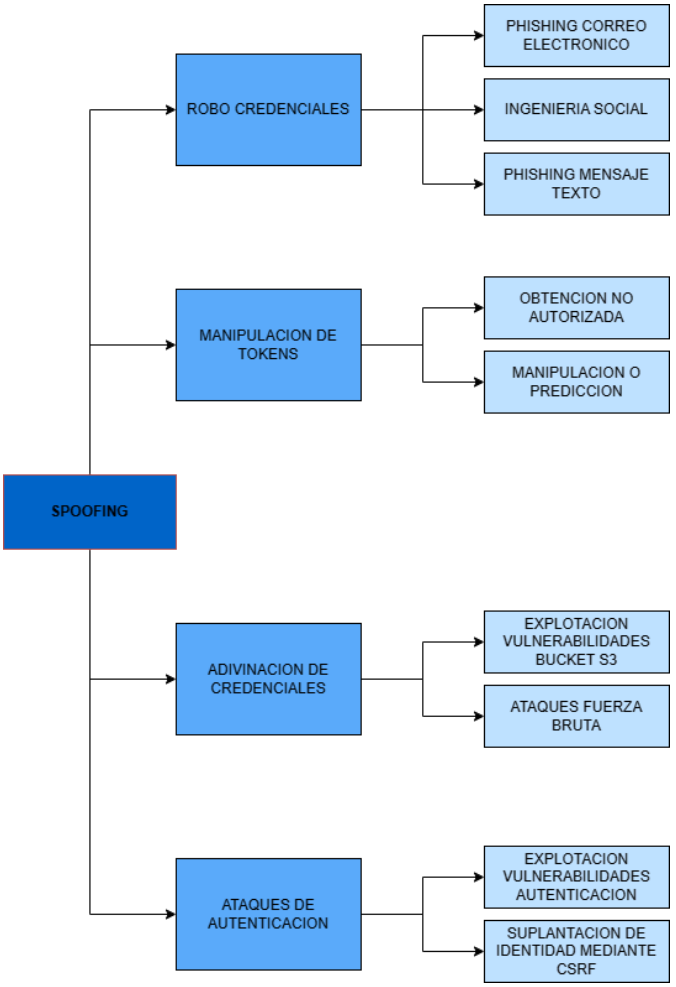
1. Metodología escogida

La estrategia seleccionada para estructurar el análisis de riesgos, que comenzó con Cornucopia de OWASP, es STRIDE. Este modelo de análisis de riesgos se suele emplear en el ámbito de la seguridad informática para identificar y clasificar las potenciales amenazas que podrían impactar un sistema o aplicación.

Cada letra del acrónimo STRIDE representa una categoría de amenazas específica: Suplantación de Identidad, Manipulación, Repudio, Revelación de Información, Denegación de Servicio y Elevación de Privilegios.

Para implementar esta metodología de manera efectiva, nos enfocaremos en las amenazas que hemos identificado como las más significativas dentro de cada una de las 6 categorías de STRIDE, utilizando como punto de partida el juego de Cornucopia de OWASP. Además, daremos prioridad a las amenazas que ocupen una posición más alta en el árbol de ataque dentro de cada categoría. Esta priorización se basará en diversos factores, como la criticidad de la amenaza, el tiempo requerido para mitigarla y un balance entre ambos, según nuestra evaluación.

2. Spoofing



El esquema mostrado en la figura previa ilustra 4 escenarios potenciales de ataque (nodos hijos) asociados al ataque de Suplantación de Identidad (nodo raíz). Cada nodo hijo presenta distintas técnicas empleadas para llevar a cabo el ataque.

De esta manera, hemos establecido el orden de criticidad de mayor a menor, con el objetivo de dar una mayor importancia a la mitigación de las vulnerabilidades que puedan provocar, es decir, los nodos situados en la parte superior presentan una mayor criticidad que los que están más abajo.

A continuación, vamos a explorar tres escenarios posibles que podrían surgir en relación al ataque de Suplantación de Identidad. Se han seleccionado los tres escenarios de ataque (nodos hijos) más preocupantes en el diagrama. Además, para cada escenario de ataque, elegiremos aleatoriamente una de sus posibles técnicas para dar una explicación más detallada.

- ## Escenario 1:

  Un grupo de ciberdelincuentes expertos en phishing ha ejecutado un ataque exitoso de robo de credenciales de acceso mediante correo electrónico en una empresa. Los hackers enviaron correos electrónicos falsificados a los empleados, haciéndose pasar por el servicio de soporte técnico de la empresa.

  Estos correos electrónicos contenían enlaces a una página web falsa, muy similar a la página oficial de la empresa. En la página falsa, se solicitaba a los empleados que ingresaran sus credenciales de acceso para verificar su identidad y resolver un supuesto problema técnico.

  Lamentablemente, algunos empleados de la empresa cayeron en la trampa y proporcionaron sus credenciales de acceso a los hackers. Con estas credenciales robadas, los hackers pudieron acceder a los sistemas de la empresa y obtener información confidencial, como datos de clientes y registros financieros.

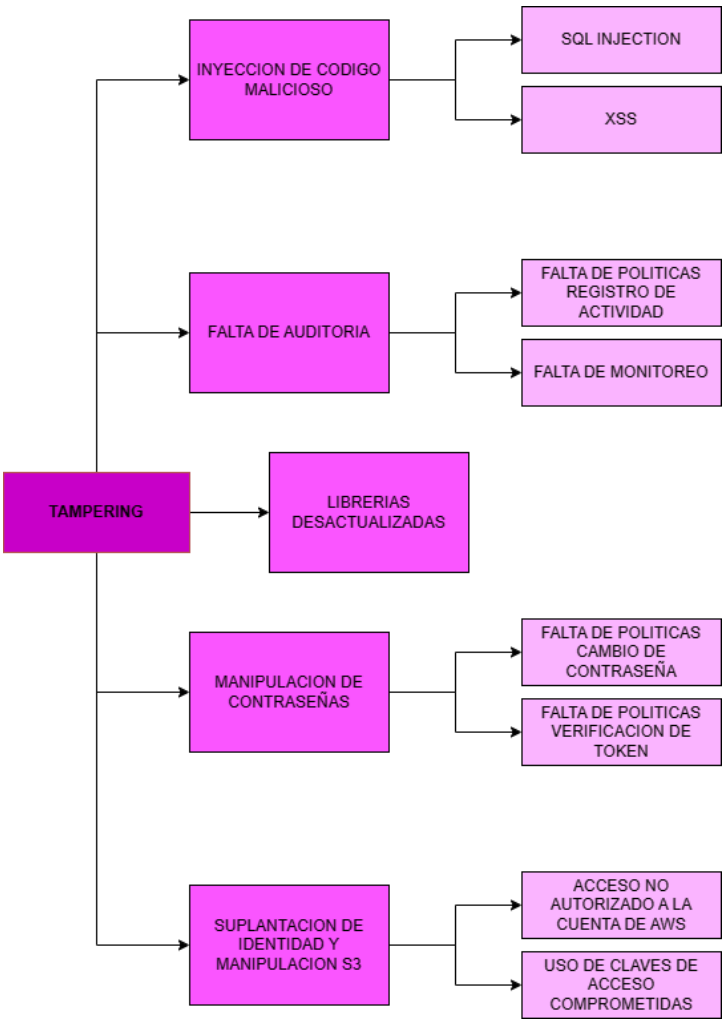
- ## Escenario 2:

  Un individuo malintencionado podría adquirir los tokens de sesión de los usuarios de manera no autorizada. Esto le otorgaría acceso a las cuentas de los usuarios y a toda la información financiera y personal que esté almacenada en la plataforma. Con este acceso, el atacante podría llevar a cabo transacciones financieras no autorizadas, acceder a datos personales o incluso suplantar la identidad del usuario para llevar a cabo acciones en su nombre.

- ## Escenario 3:

  Los atacantes podrían emplear herramientas automatizadas para probar diversas combinaciones de nombres de usuario y contraseñas predeterminadas con el fin de acceder a las cuentas de los clientes de ChaseMyCash. En el caso de que los clientes no hayan modificado sus credenciales por defecto, los atacantes podrían lograr acceso no autorizado a la plataforma, lo que les permitiría obtener información financiera y personal de los clientes.

3. Tampering



Utilizaremos la misma metodología que en el ataque anterior para evaluar la gravedad de los posibles escenarios en este tipo de ataque. A continuación, describiremos tres escenarios de ataque de mayor preocupación:

- ## Escenario 1:

  Un hacker detecta una falla en el monitoreo de los registros de seguridad de ChaseMyCash y decide aprovecharla para llevar a cabo un ataque. El hacker comienza intentando acceder a la aplicación mediante técnicas de fuerza bruta y, después de varios intentos, logra obtener las credenciales de acceso de un usuario registrado.

  Una vez dentro del sistema de manera ilegítima, el hacker lleva a cabo diversas acciones maliciosas, como la extracción de información personal y financiera de los usuarios o la realización de transacciones fraudulentas. Debido a la falta de auditoría y monitoreo de los registros de seguridad, estas actividades pasan desapercibidas para el equipo de seguridad de ChaseMyCash durante un tiempo prolongado.

- ## Escenario 2:

  Un atacante descubre una vulnerabilidad en el sistema de seguridad de ChaseMyCash que le permite realizar una inyección de código SQL. Esto podría permitirle acceder a la base de datos de la aplicación y robar información confidencial de los usuarios, así como modificar datos, generando graves problemas para los usuarios.

- ## Escenario 3:

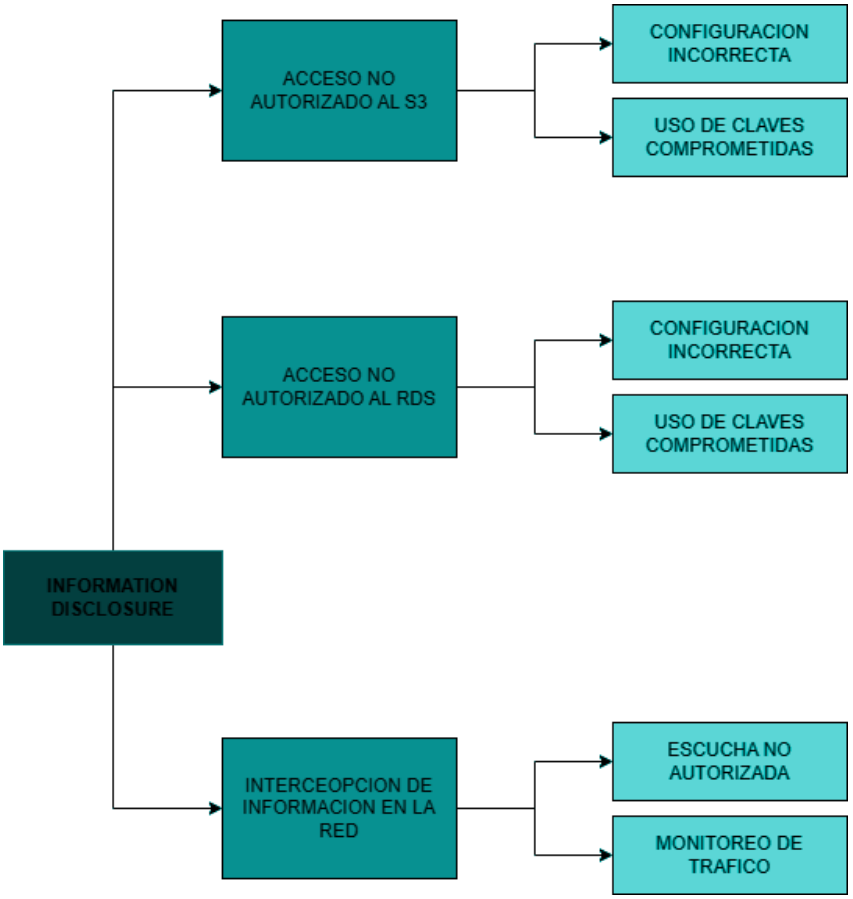
  Un grupo de ciberdelincuentes ha encontrado una vulnerabilidad en la seguridad de ChaseMyCash que les permitió obtener acceso a las contraseñas y tokens de los usuarios. La ausencia de políticas de cambio de contraseñas y la debilidad de las mismas permitieron a los hackers mantener el acceso durante días sin ser detectados.

4. Repudiation

- ## Escenario 1:

  Si un intruso accede a la base de datos de los clientes y se hace pasar por el personal de ChaseMyCash, podría contactar a dichos clientes y venderles licencias falsas. La falta de monitoreo de la actividad de la aplicación y de los usuarios permitiría que cualquier acción maliciosa pasará desapercibida, lo que permitiría al atacante eludir la responsabilidad de sus acciones y dificultaría la identificación del verdadero culpable.

5. Information Disclosure



- ### Escenario 1:

  Un atacante malintencionado descubre que ChaseMyCash utiliza un Bucket S3 para almacenar los datos de sus usuarios, y que la configuración de políticas de acceso a ese bucket no es correcta. El hacker aprovecha esta oportunidad para llevar a cabo un ataque de acceso no autorizado al bucket. Una vez dentro, descarga y roba información personal y financiera de usuarios de ChaseMyCash, pues se encuentra sin cifrar.

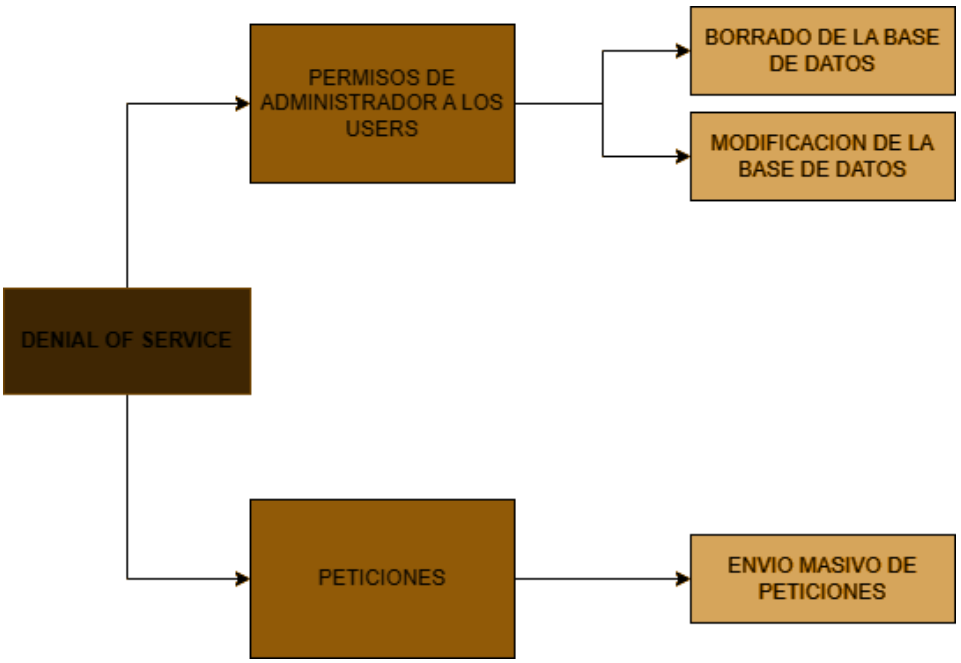
- ### Escenario 2:

  Un atacante descubre una configuración incorrecta de permisos en la base de datos RDS de ChaseMyCash. Aprovechando esta falla, accede sin autorización a la base de datos y obtiene información confidencial de los clientes de la empresa.

- ## Escenario 3:

  Si un desarrollador de ChaseMyCash sube accidentalmente un archivo de configuración a un repositorio público que contiene claves de acceso a la base de datos, un atacante podría obtener acceso a la base de datos y obtener información confidencial de los usuarios.

6. Denial of Service



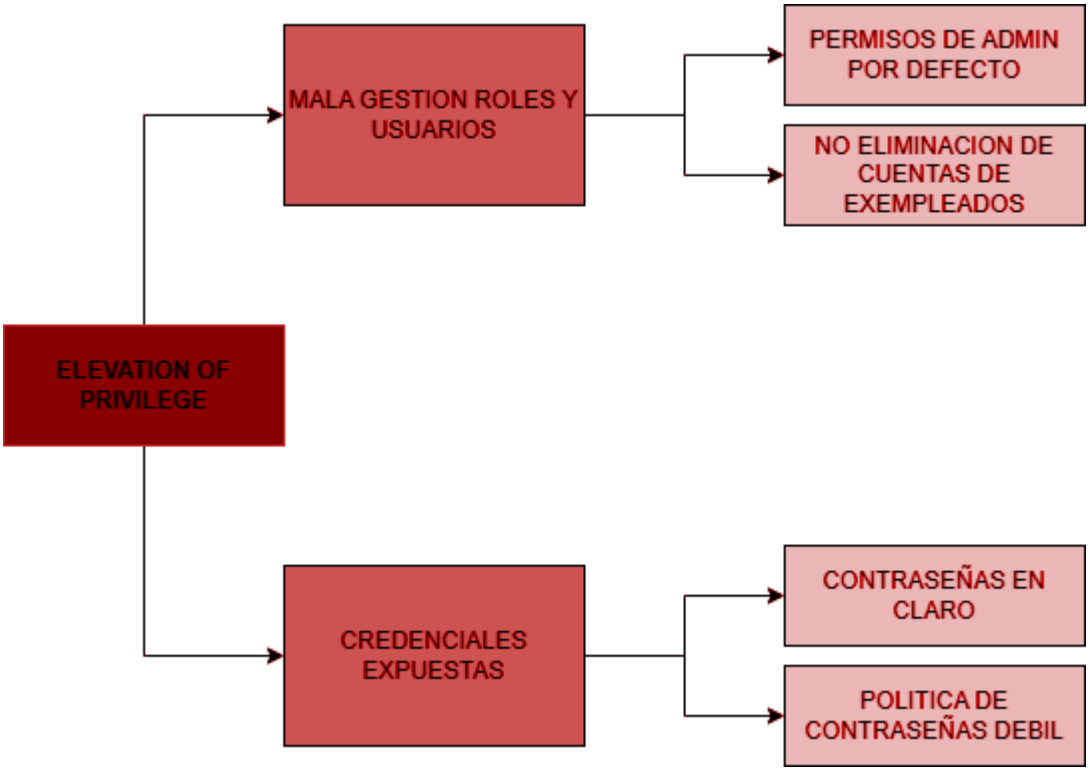
- ## Escenario 1:

  Un empleado de ChaseMyCash con privilegios de administrador tendría acceso completo a la base de datos. Si este empleado no sigue los protocolos de seguridad adecuados o utiliza su acceso de manera maliciosa, podría borrar o modificar la base de datos. Esto podría ocurrir si el empleado está descontento, busca venganza o es objeto de coacción. Dado que la aplicación depende activamente de la base de datos para ofrecer el servicio, cualquier modificación o eliminación podría provocar una denegación de servicio.

- ## Escenario 2:

  La empresa lanza una campaña publicitaria viral que atrae a una avalancha de usuarios a la aplicación ChaseMyCash, saturando el balanceador de carga y superando la capacidad del clúster del frontend. Como resultado, el frontend se vuelve lento e inaccesible, provocando una denegación de servicio. Además, el backend, ubicado en el mismo dominio, también podría sufrir una denegación de servicio, afectando la experiencia del usuario y potencialmente causando la pérdida de clientes.

7. Elevation of Privilege



- ## Escenario 1:

  Un empleado de ChaseMyCash utiliza su portátil con Windows 11 y tiene permisos de administrador por defecto. Decide descargar e instalar un software de terceros que parece ser útil para su trabajo diario. Sin embargo, el software, que en realidad es malicioso, aprovecha los permisos de administrador del usuario para obtener acceso completo al sistema y realizar una elevación de privilegios.

  Con los permisos elevados, el software malicioso puede desactivar el software de seguridad del usuario, instalar software adicional, realizar cambios en la configuración del sistema, acceder a datos confidenciales, entre otros. Además, dado que todos los empleados tienen permisos de administrador en sus equipos, el software malicioso puede propagarse fácilmente a otros sistemas en la red.

- ## Escenario 2:

  Un atacante podría interceptar las credenciales de inicio de sesión de un usuario de ChaseMyCash al enviarlas en texto plano por correo electrónico. Si el atacante obtiene acceso a la cuenta de correo electrónico del usuario, podría obtener sus credenciales y realizar una elevación de privilegios dentro de la aplicación. Una vez dentro, el atacante tendría acceso a los datos financieros y personales del usuario, así como a la información de otros usuarios si cuenta con los permisos necesarios. Además, si el usuario utiliza la misma contraseña en otros servicios, el atacante podría intentar acceder a ellos también.