Juan Felipe Mejia Parra - 201517650

Juan Esteban Cañizares Ortiz - 201817053

Análisis Caso 2

1. Debido a que el sistema maneja información sensible y personal de sus usuarios estos deben ser protegidos de forma exhaustiva por los desarrolladores del portal web y los administradores del sistema.

   Algunos de los datos importantes que se deben proteger en el sistema incluyen:

   - **Información de acceso al portal:** Si un actor no autorizado llega a tener acceso a la información de acceso (Usuario-contraseña) de cualquier usuario implica una vulnerabilidad completa a la información propia de ese usuario en modo lectura y la persona no autorizada podría incluso permitirse modificar la información de dicho usuario. Esto implicaría que la entidad estaría proveyendo información privada a un tercero.
   - **Datos de recaudación:** En modo lectura, una vulneración a este tipo de datos permitiría a un tercero tener acceso a toda la información bancaria propia de la caja de pensiones y sus afiliados como, números de cuenta, contraseñas, saldos disponibles y generación de facturas. En modo escritura sería posible redireccionar los recaudos a una cuenta personal en vez de la propia de la caja de pensiones. Una vulneración en este tipo de datos claramente desemboca en perdidas monetarias para los usuarios y la entidad.
   - **Historial laboral:** En modo escritura un usuario estaría en capacidad de modificar su historia laboral con el fin de sumarse años de experiencia y poder recibir su pensión antes o por mayor cantidad de años.
   - **Nomina de pensionados:** En modo lectura se podría acceder a la información personal de todos los afiliados de la entidad. En modo escritura existiría la posibilidad de añadir o retirar personas del fondo de pensiones sin pasar por los tramites legales requeridos.
2. Algunas de las vulnerabilidades propias del sistema, basado en problemas como el espionaje, adulteración, suplantación y repudio de la información serían:

- El sistema de la pagina web no especifica la implementación de un protocolo https para la correcta encriptación de sus datos. Esto facilita a posibles hackers el poder desencriptar la información transmitida de la web al servidor y viceversa.
- El hecho de que exista una subred interna que conecta todos los computadores internos, a pesar de que estén desconectados de las otras redes y servidores de la entidad, implica que una vez se vulnere un único computador interno también se podrá tener fácil acceso al resto de sistemas de la compañía.
- Los datos no se almacenan de forma encriptada, ni se utiliza una llave ya sea simétrica o asimétrica, lo cual facilita el acceso de los datos contenidos en el servidor.
- Los backups de procesamiento y almacenamiento no están guardados en una red segura y tampoco se encuentran de forma encriptada, estos backups son fácilmente accesibles por alguien externo y contienen de igual manera la información propia del fondo de pensiones y de todos sus afiliados.

3. Para solucionar estos problemas de encriptación desarrollamos una clase ClienteProtocolo que se encarga de ejecutar de ejecutar el protocolo planteado en el modelo del taller. Una vez establecidos y enviados los mensajes de inicio, conexión y respuesta, se procede a ejecutar alguno de los algoritmos de encriptación planteados.

   En este caso es importante resaltar, que el programa escoge uno de estos algoritmos de forma aleatoria de un Array previamente creado e inicia su sesión. Posteriormente, el programa se encarga de autenticar tanto el servidor como el cliente y finalmente se hace la transferencia de la información con la respectiva respuesta de rechazo o aceptación por parte del servidor.