Juan Camilo Lara - 201424726

María Del Rosario León - 201423755

Andrea Carolina Montoya - 201713889

Caso #2

A.

1. Debido a que la aplicación Novasoft financiero en línea tiene como propósito ocuparse de las operaciones financieras de la empresa es necesario que se protejan los datos de los servicios que ofrecen, como lo son las cuentas por pagar y/o cobrar, los servicios de facturación y los servicios de compras.

* Identificación de clientes: Si un tercero logra obtener esta información podría suplantar al cliente tanto dentro de la aplicación como en el exterior.
* Correo del cliente: Si un actor no autorizado logra tener acceso a los correos podría suplantar a la empresa frente a sus clientes y causar la pérdida de estos.
* Teléfono del cliente: Si un actor no autorizado logra tener acceso a los números de teléfono podría suplantar a la empresa frente a sus clientes y causar la pérdida de estos o a través de spoofing suplantar al cliente.
* Información bancaria: Esta información le permite a un tercero afectar directamente a la compañía de forma económica al interferir con las transacciones o poner en riesgo al cliente de forma similar.
* Tarjetas de crédito: Con esta información un tercero podría hacer compras en nombre de los clientes o vender la información de la tarjeta.

2.

Las 4 vulnerabilidades que encontramos fueron los siguientes:

* **Spoofing:** Un dispositivo no autorizado puede entrar al sistema, ya que nos se verifica la autenticidad del dispositivo que desea realizar la transacción.
* **Information disclousure**: Como la información se manda sin protección, esta puede ser interceptada y filtrada por usuarios no autorizados.
* **Man in the middle:** Debido a que la información que se envía no esta protegida, un usuario no autorizado puede interceptarla, manipularla y enviar información errónea afectando la integridad de la información.
* **Denial of service:** Se puede perder la capacidad de acceder al sistema por un exceso de peticiones realizadas para las cuales el servidor no esta preparado. Esto impediría que los clientes puedan realizar transacciones.

Las soluciones que proponemos son las siguientes:

* **Certificado digital:** El certificado digital, permite que los dispositivos se identifiquen delante del otro evitando así el spoofing. Además, con el certificado se manda una llave publica con una validez igual a la del certificado, permitiendo que tanto cliente como servidor obtengan llaves y puedan comenzar una llave simétrica.
* **Encriptación:** Hacer uso de cifrado asimétrico para que si la información es interceptada esta no pueda ser entendida por aquellos que no deben, ya que la única forma de descifrarlo es tener la llave hermana.
* **Firewall:** A través de un firewall se puede filtrar las peticiones que se quieren aceptar y las que no. De esta manera, se puede configurar el firewall para que rechace ciertos tipos de peticiones para que los atacantes no puedan colapsar el sistema.
* **Hashing:** Mandar el hash de la petición realizada, permite saber si la información fue alterada o no. Esto se logra gracias a que si el mensaje fue alterado el hash recibido no coincidirá con el que resulta del mensaje recibido.