

Actividad [#1]

[Detección y Prevención de Ataques de Acceso]

[“Seguridad Informática II ”]

Ingeniería en Desarrollo de Software

**Tutor: Elizabeth Guevara Roa**

**Alumno: Manuel Enrique Ramirez Lopez**

**Fecha: 13/09/2022**

***Indice***

***[Introduccion](#_Toc23778)* [1](#_Toc23778)**

***[Justificación](#_Toc16452)* [2](#_Toc16452)**

***[Contexto](#_Toc6288)* [3](#_Toc6288)**

***[Delimitacion del problema](#_Toc13891)* [4](#_Toc13891)**

[● Incidencias encontradas 4](#_Toc8083)

[● Reporte 5](#_Toc14810)

[● Análisis 5](#_Toc20499)

[● Identificación de mejoras 7](#_Toc26413)

***[Conclucion](#_Toc14777)* [8](#_Toc14777)**

***[Referencias](#_Toc19195)* [9](#_Toc19195)**

# *Introduccion*

En épocas actuales la gran revolución tecnológica esta en una faceta de grandes cambios donde grandes franquicias de diferentes rubros y tamaños estas mudando de un sistema arcaico del papel y pluma al ordenador y estaciones de trabajo donde se busca cada vez mas ser eficientes en los distintos procesos que conlleva cada una de las partes que conforma cada organización que va desde trabajo en piso de venta hasta el muy conocido hoy en día el “Home office” donde estos tipo de actividades comparten algo en común el uso de sistemas informáticos para su optimo desempeño.

A continuación seremos testigos de como es que se planifica de manera manual por decirlo de una manera familiar el como proteger los distintos tipos de accesos que existen entre cliente y servidor donde la informacion que se transmite es de suma importancia y debemos actuar antes de alguna catástrofe que pueda afectar de manera significativa la operación del la empresa.

# *Justificación*

En la Delimitacion del problema presentado nos podemos centrar en algunas ideas claves las cuales serán las bases firmes para poder desenvolver de manera optima dicho problema, donde pondremos como prioridad el problema “prevenir ataques de acceso” donde este se puede interpretar de distintas maneras eh incluyen a distintas partes de la empresa empezando por:

Riesgo humano: Donde por falta de conocimientos sobre como poder acceder de manera segura estos se conecten con sus datos de acceso como podrían ser correo electrónico y contraseña hasta llaves físicas de autentificacion o datos biométrico por acceder desde una red publica o intervenida por un tercero.

Riesgo de software: Al dejar al descubierto ciertas partes criticas como podrían ser bases de datos con informacion de todos los usuarios o informacion clave que pueda perjudicar de manera económica o de reputación a al empresa afectada.

Ojo estos podrían ser los problemas a simple vista de el primer punto, seguido a esto que va de la mano al punto de “Riesgo de software” observamos el segundo punto que trata de prevenir accesos a las redes donde principalmente los objetivos son los puentes de acceso que usan los usuarios esto se puede evitar con un debido analisis de riesgo a instalaciones de la empresa donde se plantea cada posible vulnerabilidad “física” dentro de las instalaciones como podrían ser que los empleados accedan desde una estacion de trabajo a alguna pagina ilícita que permita a terceros acceder a dicha red privada y hacerse con la informacion ¿Como podemos prevenir estos casos? Obteniendo el control total de la red monitoriando aspectos como: hardware, software, licencias y red y llevando bitacoras de todas las vulnerabilidades encontradas y su solucion adjuntando fecha de deteccion y correccion.

# *Contexto*

**Contextualización:** Se pretende utilizar algunas técnicas de protección ante ataques de explotación y obtención de acceso a sistemas de una entidad de crédito. En este sentido, deberás analizar los factores que enfatizan la importancia de la seguridad y que se describen a continuación:

**Escenario principal:** Acrecer es una organización privada dedicada a otorgar préstamos a terceros. Realiza el manejo de la información desde un servidor principal haciendo uso de una base de datos en Oracle. Además, maneja un sistema de control y registro de actividades relacionadas a financieras.

**Escenario secundario:** La financiera requiere el manejo de su seguridad ante posibles ataques, motivo por el cual se te solicita formar parte del proyecto como analista e implementador de mecanismos de seguridad informática. Por consiguiente, el gerente solicita lo siguiente:

● Prevenir los ataques de acceso.

● Prevenir accesos a las redes.

● Validar las licencias de sus recursos por cuestiones de los aspectos legales y regulatorios.

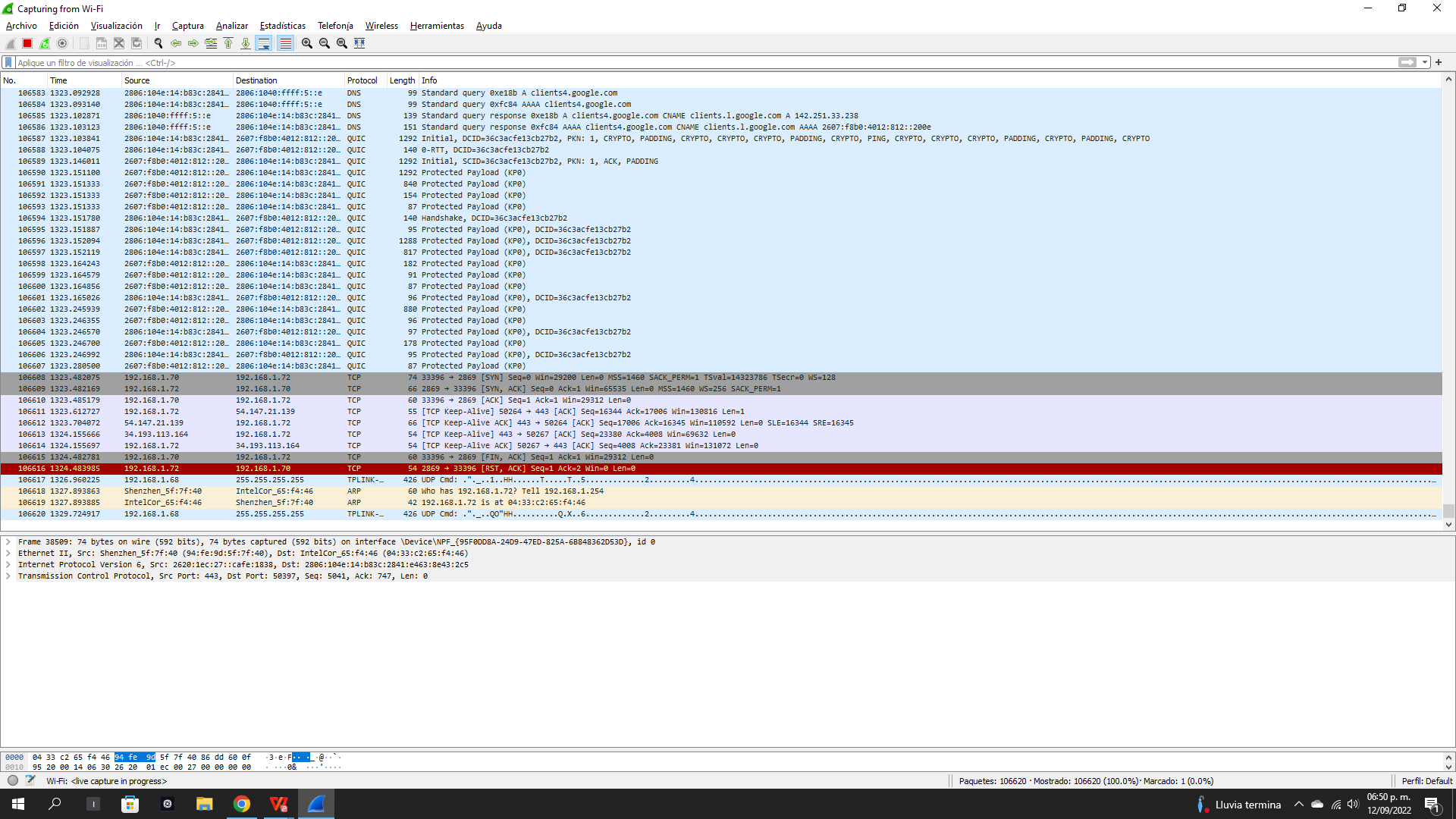
● Control total y auditoría cada semana del sistema, hardware, software, licencias y red.

● Monitoreo completo de la red.

● Es importante que se guarde la bitácora, eliminarla e iniciar una nueva para detectar los cambios desde el día 1.

# *Delimitacion del problema*

## ● Incidencias encontradas



Haciendo el debido test durante un tiempo prolongado se ah detectado de forma inusual a la empresa “amazon” donde interviene en el flujo de paquetes de salida donde recopila informacion sobre “intereses” o palabras clave para predecir gracias a su motor de búsqueda y dar una respuesta lo mas acertada para su plataforma.

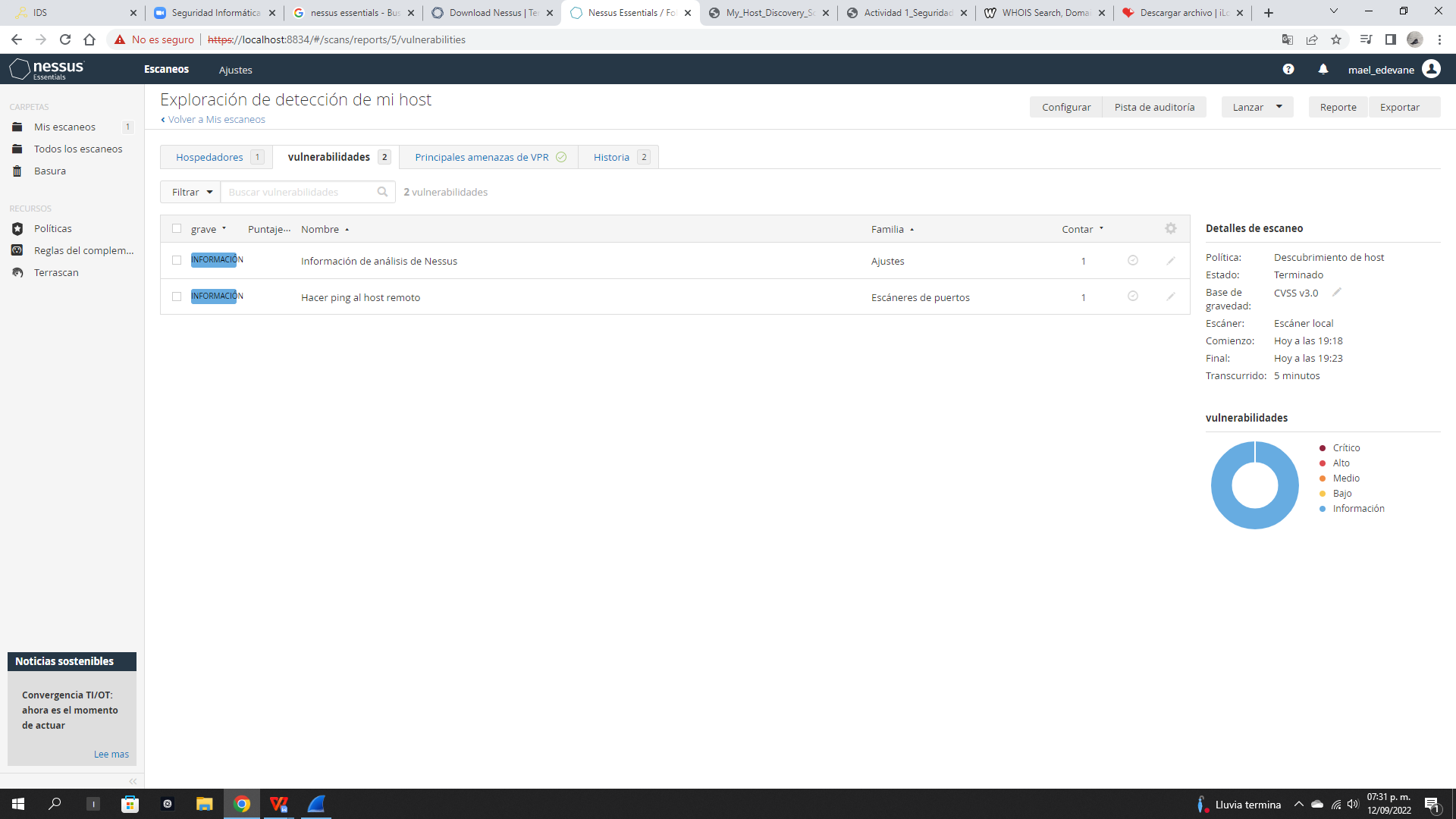
## ● Reporte

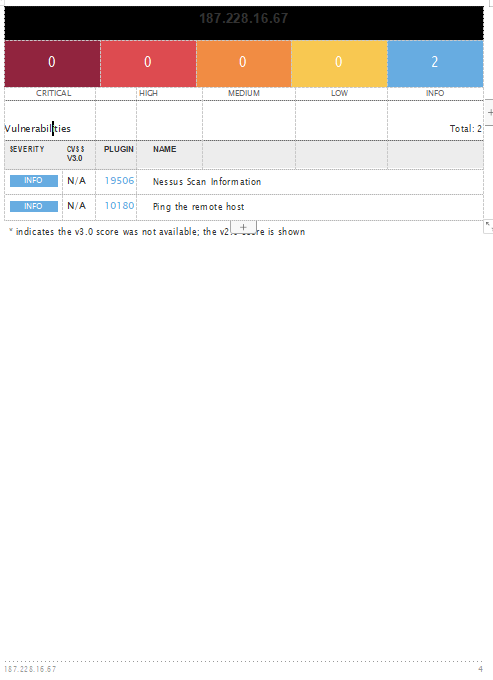
Se ha realizado el debido analisis por medio de 2 programas los cuales son WireShark y Nessu Essentiall donde con cada uno se obtienen resultados diferentes donde uno es para analisis detallado “WireShark” y el segundo realiza un analisis general donde da relevancia a aspectos como vulnerabilidades criticas y arroja recomendaciones para combatirlos.

## ● Análisis

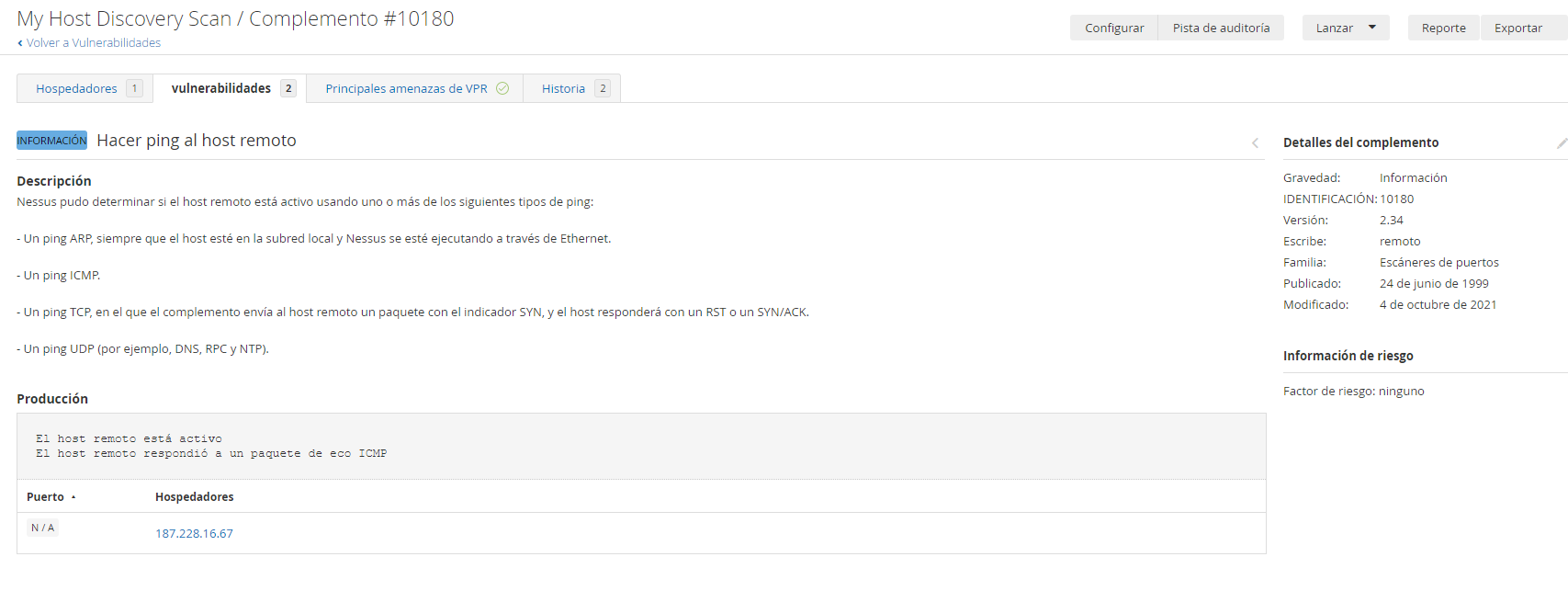
-Observando detenidamente se logra observar que diferentes empresas dedicadas a la venta de productos se dedican a “recopilar” informacion como palabras clave para mostrarte en forma de publicidad los articulos que mas se asemejen a tus gustos.

-PDF generado por Nessu Essential





## ● Identificación de mejoras

Algunas recomendaciones que nos manda son que nos debemos conectar por medio de cable ethernet para mayor seguridad ya que actualmente en la computadora que se ejecuto el analisis esta conectada a Internet por medio de Wifi.

# *Conclucion*

Para el termino de esta actividad se lograron recabar distintos tipos de experiencias que van desde el descubrimiento de programas para el analisis de red en curso hasta reportes completos que dictaminan la causa o fugas de informacion existen en tu red, aunque esta vez se realizo de manera local en una computadora domestica nos arrojaron distintas advertencias que son de bajo riesgo, es de suma importancia realizar este tipo de “pruebas” ya en un entorno mas complejo como podrían ser centros corporativos, plantas de producción u oficinas lo que mas vale y con lo que se trabaja día a día es la informacion tanto personal de nuestros clientes como corporativa que son clave para un futuro prometedor en la empresa. En pocas palabras es muy importante tomar en cuenta la planificación de como queremos conectar nuestras estaciones de trabajo para así evitar vulnerabilidades dentro de nuestras instalaciones y hacerlas seguras.

# *Referencias*

*WHOIS Search, Domain Name, Website, and IP Tools - Who.is*. (s. f.). Recuperado 12 de septiembre de 2022, de https://who.is/

ilovepdf.com. (s. f.). *Convierte tus PDF a WORD editable*. iLovePDF - Herramientas online para PDF. Recuperado 12 de septiembre de 2022, de https://www.ilovepdf.com/es/pdf\_a\_word

*Obtenga un código de activación | Nessus®*. (s. f.). Tenable®. Recuperado 12 de septiembre de 2022, de https://es-la.tenable.com/products/nessus/activation-code