PROPUESTA DE ASEGURAMIENTO Y ANÁLISIS DE VULNERABILIDADES CON TÉCNICAS DE ETHICAL HACKING EN AMBIENTE CONTROLADO PARA LA EMPRESA NOSTRADAMUS S.A.S

YENNI MILENA ACOSTA MONTOYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2021

PROPUESTA DE ASEGURAMIENTO Y ANÁLISIS DE VULNERABILIDADES CON TÉCNICAS DE ETHICAL HACKING EN AMBIENTE CONTROLADO PARA LA EMPRESA NOSTRADAMUS S.A.S

YENNI MILENA ACOSTA MONTOYA

Proyecto de Grado – presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Ing. Fernando Zambrano Hernández
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2021

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Fecha sustentación

DEDICATORIA

Dedico este esfuerzo, a mi esposo quien ha compartido conmigo el trabajo en esta especialización y ha disfrutado cada paso, quien es mi mayor motivación y me impulsa a continuar y no claudicar a pesar de las circunstancias, el cansancio o falta de tiempo, a mis padres quienes sembraron en mí el gusto y la pasión por el aprendizaje, quienes conocieron los inicios en este camino por el saber.

AGRADECIMIENTOS

Agradezco a Dios por sabiduría para continuar con estos estudios, a mis padres que han estado para ayudarme en los momentos que inicié mi carrera. A mi esposo le agradezco por la paciencia por la colaboración necesitaba por estar ahí en los momentos que más lo necesito para motivarme y continuar a seguir la meta para terminar esta especialización en seguridad informática como porque sabemos que va a ser de gran ayuda para nosotros la familia.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

RESUMEN

En el desarrollo se conocerán fundamentos teóricos sobre temas relacionados a la seguridad informática y seguridad de la información ya que es un componente esencial en la actualidad para el funcionamiento de compañías que utilizan las tecnologías de la información, tras la generación de diversas amenazas y vulnerabilidades. En este proyecto de grado se plantea el análisis de vulnerabilidades en la infraestructura NOSTRADAMUS S.A.S empresa perteneciente al sector tecnológico cuyo objetivo es brindar servicios en los sectores educativos, corporativos y gubernamentales, con proyectos de educación y capacitación, esta organización brinda Capacitación y soporte por 24/7, en los últimos días la empresa fue vulnerada por delincuentes informáticos y por consiguiente le fue robara su información por medio de ataques remotos, esta brecha de seguridad lo que ocasiono fue la pérdida de imagen corporativa, perdida de datos y por consiguiente pérdida de clientes. El objetivo de este proyecto es realizar un análisis de vulnerabilidades dentro de la infraestructura de la organización y gestionar desde un enfoque estratégico y directivo las Políticas la Seguridad para el tratamiento de la Información de la Empresa, con el fin de mitigar estos riesgos y evitar que vuelva a ocurrir estas afectaciones.

Palabras clave: Ethical Hacking, Seguridad informática, seguridad de la información, Pentest, Vulnerabilidad

ABSTRACT

In the development, theoretical foundations on issues related to computer security and information security will be known since it is an essential component today for the operation of companies that use information technologies, after the generation of various threats and vulnerabilities. In this degree project the analysis of vulnerabilities in the infrastructure is proposed NOSTRADAMUS SAS, a company belonging to the technology sector whose objective is to provide services in the educational, corporate and government sectors, with education and training projects, this organization provides training and support for 24 / 7, in recent days the company was violated by computer criminals and therefore its information was stolen through remote attacks, this security breach which caused the loss of corporate image, loss of data and consequently loss of customers. The objective of this project is to carry out a vulnerability analysis within the organization's infrastructure and manage the Security Policies for the treatment of Company Information from a strategic and directive approach, in order to mitigate these risks and prevent them from these affectations reoccur.

Key Words: Ethical Hacking, Security Information, seguridad de la información, Pentest, vulnerability

INTRODUCCIÓN

Este proyecto plantea realizar el análisis de la empresa Nostradamus SAS, utilizando una metodología y pruebas de penetración cuyo objetivo es el descubrir y evaluar las vulnerabilidades que se presenten, y poder determinar las estrategias de defensa para la organización y establecer las respectivas recomendaciones de solución ante las vulnerabilidades encontradas; para la realización de este proceso se efectuarán pruebas de intrusión, y análisis de vulnerabilidades, estas prácticas son realizadas en las compañías para conocer su nivel de seguridad.

En el desarrollo se conocerán fundamentos teóricos sobre temas relacionados a la seguridad informática y seguridad de la información ya que es un componente esencial en la actualidad para el funcionamiento de compañías que utilizan las tecnologías de la información, tras la generación de diversas amenazas y vulnerabilidades.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

La información es de los activos más importantes y relevantes en una compañía, regularmente esta se gestiona en sistemas informáticos los cuales facilitan el aprovechamiento, ya que en esta infraestructura es donde se transporta, almacena y procesa por ende debe ser segura y confiable.

Muchas empresas no son conscientes y están expuestas a ataques informáticos que pueden afectar los datos sensibles e información relevante de la organización[1]. Dependiendo del tipo de negocio se corre un mayor o menor riesgo en ser víctima de ataques informáticos.

Según un informe realizado por la firma de seguridad Digiware, reveló que en 2017 en Colombia se registraron 198 millones de ataques cibernéticos, tras estos ataques hubo pérdidas por más de $6.179 millones de dólares. Digiware determinó que 5 de cada 6 ataques exitosos en el país se deben a suplantación de usuarios, vulnerabilidades en aplicaciones, mala configuración en infraestructura, falta de parcheo, malware avanzado, sistemas ineficientes.[2]

Y con todas estas cifras aún hay empresas que piensan que los ataques informáticos le ocurren a las demás entidades y no a ellos: con este tipo de pensamientos se frena la innovación y la limitan lo que dificulta las tareas de inversión en materia de seguridad, ya que consideran que puede ser algo costoso, sin embargo el no tener conocimientos

[1] Latam Kaspersky [En línea] Bogotá 2020 [Fecha de Consulta: septiembre 2020] Disponible en https://latam.k (Kapersky, fd) aspersky.com/about/press-releases/2018_la-falta-de-conocimiento-en-seguridad-informatica-pone-en-riesgo-a-las-empresas

[2] Dinero [En línea]. Bogotá 2017 [Fecha de Consulta: junio 2019]Disponible en https://www.dinero.com/Item/ArticleAsync/250321?nextId=250338&nextId=250317

en el área acarrea mayores costos, ya que al ser atacados los ciber-delincuentes buscan recompensas lucrativas ante esto las empresas optan por correr el riesgo y quedar vulnerables ante las amenazas[3].

1.2. FORMULACIÓN DEL PROBLEMA

El problema planteado en la empresa NOSTRADAMUS S.A.S fue ocasionado en sus sistemas operativos Windows 7 el cual fue atacado por delincuentes informáticos que afectaron los navegadores web al hacer uso de técnicas de ingeniería social y usando la herramienta de metasploit, los ciberdelincuentes pudieron ejecutar una elevación de privilegios lo cual les permitió el robo de la información, desencadenando una serie de eventos desafortunados en la imagen corporativa de la empresa incurriendo así en la perdida de los datos, a raíz de esto los clientes molestos se retiraron de la compañía y de seguir así la empresa podría llegar a instancias de cerrar sus puertas, por esto se plantea el siguiente interrogante.

1.3. PREGUNTA DE INVESTIGACIÓN

¿Cómo por medio de metodologías de Ethical Hacking se puede asegurar la continuidad de los negocios de la empresa NOSTRADAMUS S.A.S.?

[3] Factor Capital Humano [En línea]. Julio 2019 [Fecha de Consulta: septiembre 201] Disponible en https://factorcapitalhumano.com/emprendedores/cuanto-debe-presupuestar-una-pyme-para-ciberseguridad/2018/05/

2. JUSTIFICACIÓN

El mundo de las amenazas informáticas continúa expandiéndose con mayor velocidad, con cada tecnología nueva también viene con nuevas amenazas, las consecuencias de los sistemas inseguros y la información vulnerable son casi siempre costosas y molestas[4].

Por lo anterior es de gran importancia que los sistemas de información y la infraestructura que usan las empresas estén preparadas para afrontar ataques de los ciberdelincuentes que quieran perjudicar las compañías para sus propios beneficios.

Es de suma importancia realizar una evaluación de vulnerabilidades, en la infraestructura utilizando las mismas tácticas que usaría un delincuente Informático para así identificar cuáles son las brechas de seguridad que tiene la empresa y estar preparado ante cualquier ataque informático, todo esto enfocado en una metodología de pruebas de penetración de seguridad enfocado en la identificación de vulnerabilidades que se encuentren presentes en la red, por medio de la metodología OSSTMM, los analistas de seguridad y los pentester pueden realizar las pruebas adecuadas de acuerdo a las necesidades de la organización y ofrece las soluciones más óptimas para la toma de planes de acción para asegurar y proteger la empresa. [5]

[4] Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio [En línea]. Octubre 2010 [Fecha de Consulta: octubre 2020] Disponible en http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

[5] OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad [En línea]. Noviembre 2016 [Fecha de Consulta: septiembre 2020] Disponible en https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Realizar una propuesta de aseguramiento como mecanismo de seguridad para la empresa de la empresa NOSTRADAMUS S.A.S, que permita el descubrimiento de vulnerabilidades encontradas mediante técnicas de ethical hacking.

3.2. OBJETIVOS ESPECÍFICOS

4. Ejecutar el plan de actividades usando técnicas de hacking ético, para el hallazgo de vulnerabilidades.
5. Presentar un reporte de resultados de vulnerabilidades encontradas, haciendo algunas recomendaciones que minimicen las vulnerabilidades.
6. Realizar el análisis de la propuesta de seguridad para la empresa.
7. Definir los lineamientos de la propuesta de aseguramiento.

4. MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

Pruebas de Penetración (pentest o pentesting)

Una prueba de penetración o test es la forma como las organizaciones pueden realizar las mediciones de sus sistemas de información por medio de herramientas o procesos, de la misma forma como lo realizaría un delincuente informático; de cómo este logra acceder o tener acceso a la información de la organización, estas pruebas de penetración se realizan con el fin de identificar las posibles vulnerabilidades o brechas de seguridad que puede ser aprovechas por los atacantes.[6]

Tipos de pentesting

1. **Caja Negra:** En este tipo de pentesting los analistas de seguridad no conocen como es el funcionamiento interno en los sistemas por lo que intentan con sus propios conocimientos y herramientas para ganar el acceso al sistema.
2. **Caja Blanca:** En este tipo de pentesting los analistas de seguridad cuentan con pleno conocimiento de cada uno de los procesos involucrados y el funcionamiento de la organización, es posible que se realice la actividad junto con el personal interno de la organización.
3. **Caja gris:** En este tipo de pentesting los analistas de seguridad conocen algunas funcionalidades internas de la organización y otras son desconocidas.

[6] Dragónjar [En línea]. Octubre 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.dragonjar.org/pruebas-de-penetracion.xhtml

Para la realización De estas pruebas de penetración los analistas de seguridad pueden hacer uso de diferentes metodologías prácticas y guías las cuales faciliten el desarrollo de esta actividad dependiendo de la necesidad de la organización:

Metodología ISSAF.

El ISSAF (*Information System Security Assessment Framework*) también conocida como el Marco de Evaluación de Seguridad de Sistemas de Información, Esta metodología permite realizar los criterios de evaluación de acuerdo con 3 fases que comprenden lo siguiente:[7]

- **Fase 1 Planificación y preparación**: En esta fase es donde se realiza la extracción de información inicial o planificación con el fin dar inicio con la evaluación.
- **Fase 2 Evaluación:** en esta fase es donde se inicia con el desarrollo de las pruebas de seguridad establecidas en la metodología.
- **Fase 3 Reportes**: en esta fase finalmente es donde se realiza la generación de informes de los resultados esperados, destrucción y limpieza de las pruebas aplicadas.

NIST SP 800-115.

NIST SP 800-115 (*Technical Guide to Information Security Testing and Assessment*), El Instituto nacional de estándares y tecnología realiza la publicación de esta guía en el año 2008 en las que define las pruebas de penetración y establece 4 fases para su desarrollo.

[7] Revista Cubana de Ciencias Informáticas [En línea]. Octubre 2018 [Fecha de Consulta: octubre 2020] Disponible en http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992018000400005&lng=pt&nrm=iso

- **Fase de planificación**: En esta fase principalmente se centra en que la evaluación de seguridad sea exitosa por lo que permite orientar los temas logísticos, recomendaciones y planes de acción que se llevará a cabo para esta actividad.[8]

- **Fase de descubrimiento**: En esta fase que realizar la validación de las vulnerabilidades de acuerdo con previa identificación y análisis, su objetivo principal es demostrar la existencia de una vulnerabilidad y su exposición cuando ésta se materializa. [9]
- **Fase de ejecución**: En esta fase una vez en identifica las vulnerabilidades es fundamental que se realice su evaluación de acuerdo con el plan establecido, También se realiza proceso de análisis se proporcionan recomendaciones transmisión y destrucción de materiales. [10]
- **Fase documentación y reporte:** Una vez terminada la fase de ejecución los hallazgos se expresan en forma de vulnerabilidades y se presentan a la organización con el fin de adoptar medidas que mejore la seguridad y mitiguen los eventos.

PTES

Esta metodología es un estándar que permite la ejecución de pruebas las cuales van desde la comunicación inicial recopilación y modelado de amenazas explotación entre otros, el cual consta de 7 secciones:

- **Interacciones de pre-compromiso**: en esta sección su objetivo es presentar las herramientas y técnicas que se utilizarán, de definen objetivos y alcance.[11]

[8] NIST [En línea]. Octubre 2018 [Fecha de Consulta: octubre 2020] Disponible en https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf pág. 4.1
[9] NIST [En línea]. Octubre 2018 [Fecha de Consulta: octubre 2020] Disponible en https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf pág. 3.1
[10] NIST [En línea]. Octubre 2018 [Fecha de Consulta: octubre 2020] Disponible en https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf pág. 7.1
[11] Ptes [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Pre-engagement

- **Recolección de información:** Esta sección consiste en realizar un reconocimiento de la mayor cantidad de información que pueda ser utilizada durante las bases de evaluación y explotación de las vulnerabilidades [12]
- **Modelado de amenazas:** En esta sección se desglosa cada 1 los activos y procesos de la organización las cuales deben estar identificados y documentados para la realización de las pruebas de penetración. [13]
- **Análisis De vulnerabilidad:** En esta sección su objetivo de descubrir las fallas el sistemas y aplicaciones que puedan ser utilizadas por un atacante por lo que se ve realizaron análisis adecuado a profundidad para alcanzar el objetivo. [14]
- **Explotación:** En esta sección el objetivo está centrado en establecer el acceso a un sistema información o recurso evitando las restricciones de seguridad donde se establece un ventor de entrada y se identifican los objetos los activos más valorados.[15]
- **Post Explotación:** En esta sección se termina cuál es el valor de las máquinas que fueron comprometida y se mantiene el control para el uso posteriormente está fase que permite identificar y documentar cuáles son los ajustes de configuración, relaciones con otros dispositivos conectados en la red para obtener otros accesos[16].
- **Reporte**: En este documento se define cuáles fueron los criterios básicos en las pruebas de penetración qué proporcionar todos los elementos necesarios que aporten valor al lector. [17]

[12] PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Intelligence_Gathering
[13] PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Threat_Modeling
[14] PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Vulnerability_Analysis
[15] PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Exploitation
[16] PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Post_Exploitation
[17] PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Reporting

OWASP. La Guía de Pruebas de OWASP.

(*OWASP Testing Guide*) Esta comunidad abierta el mundo permite que las organizaciones puedan adoptar medidas sobre los riesgos de seguridad en sus aplicaciones esta metodología se encuentra días los siguientes aspectos.[18]

- **Recopilación de información**: Se basa en entender cómo está configurado el servidor donde se encuentra alojado la aplicación web, "se considera que en una cadena de aplicaciones es tan fuerte cómo se encuentre su eslabón más débil.[19]
- **Pruebas de gestión de configuración e infraestructura:** Conocer la información sobre la infraestructura datos relevantes de la aplicación web tales como el código fuente los métodos usados http formas de autentificación y como se encuentra configurada la infraestructura.[20]
- **Pruebas de gestión de identidad:** Identificar qué usuarios son los que han realizado un proceso de registro para validar su identidad dependiendo las tareas que se hayan establecido. [21]
- **Pruebas de autenticación:** Es la acción de confirmar o establecer la legitimidad y autenticidad sobre algún objeto o actividad, este proceso depende de varios factores de autentificación por lo que es necesario realizar las validaciones en el sistema para conocer su funcionamiento[22]
- **Pruebas de autorización:** Este concepto es el que concede el acceso y recursos solo a las personas que tengan permiso para acceder por ello es necesario

[18] OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en http https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf
[19] OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 38
[20] Owasp [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 85
[21] OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 91

[22] OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 121

entender su funcionamiento y de esta forma establecer cómo es posible saltarse estos mecanismos de autorización. [23]

- **Pruebas de gestión de sesión:** Esta prueba consiste en analizar cómo se realiza la gestión de sesiones entender su funcionamiento y determinar la forma de romper la sesión de usuario, Se pueden emplear métodos de ingeniería inversa, manipulación de cookies con el fin de robar las sesiones de usuario.[24]
- **Pruebas de validación de ingreso:** Estas pruebas es necesario que el analista realice diferentes peticiones al servidor esperando la respuesta procesada en el servidor.[25]
- **Manejo de errores:** Al realizar las pruebas de penetración en las diferentes aplicaciones web es posible que se encuentren errores en el código fuente En las aplicaciones, lo cual permite que los analistas pueden realizar pruebas de penetración durante el ejercicio y se encuentre información valiosa sobre servidores y bases de datos. **[26]**
- **Criptografía**: al Implementar el cifrado es necesario que exista un estándar de criptografía que sea capaz de soportar las peticiones realizadas. [27]
- **Pruebas de lógica del negocio:** Para la realización de estas pruebas de lógica de negocio es necesario identificar las posibles fallas mediante pruebas de abuso y mal uso. **[28]**
- **Pruebas del punto de vista del cliente**: Las pruebas del lado del cliente es donde las ejecuciones se realizan desde la perspectiva del cliente, normalmente

[23] OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 185
[24] OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 160
[25] Owasp [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 219
[26] OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 240
[27] Owasp [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 38
[28] OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 276

se realiza desde un navegador web por medio de ejecuciones de código con el fin de esperar una respuesta del lado del servidor.[29]

- **Seguridad informática**

La seguridad informática, también llamada Ciberseguridad la definimos como una disciplina encargada de diseñar procedimientos, normas, métodos y técnicas destinados a proteger los sistemas informáticos, teniendo como prioridad sus tres pilares los cuales son la confidencialidad, la integridad y la disponibilidad.
Esto implica un proceso de identificar y mitigar vulnerabilidades que se presenten en los sistemas informáticos.[30]

La seguridad informática establece estándares que minimizar al máximo los riesgos en la información o la infraestructura informática. En los estándares vienen representadas horas, operaciones Estos estándares incluyen horas de operación, restricciones, aprobaciones, denegaciones, configuraciones, planes de contingencia, protocolos y todo lo necesario para permitir un alto nivel de seguridad minimizando en la medida posible el desempeño del trabajador y la organización en general[31].

Seguridad de la Información

La seguridad de la información se define como "un estado de bienestar de la información y la infraestructura en el que la posibilidad de robo, alteración e interrupción de la información y los servicios se mantiene baja o tolerable". Se basa en cinco elementos principales: confidencialidad, integridad, disponibilidad, autenticidad y no repudio.

[29] OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 294

[30] 3ciencias [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

[31] 3ciencias [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

- **Confidencialidad**: La confidencialidad es la garantía de que la información sólo es para aquellas personas que esta previamente autorizadas a tener acceso. Se pueden producir infracciones de confidencialidad debido a un manejo incorrecto de datos o un intento de piratería. Los controles de confidencialidad incluyen la clasificación de datos, el cifrado de datos y la eliminación adecuada del equipo (es decir, de DVD, CD, etc.[32]

- **Integridad**: La integridad es la confiabilidad de los datos o recursos en la prevención de cambios impropios y no autorizados, la seguridad de que la información es lo suficientemente precisa para su propósito. Las medidas para mantener la integridad de los datos pueden incluir una suma de comprobación (un número producido por una función matemática para verificar que un bloque de datos determinado no se modifique) y control de acceso que garantiza que solo las personas correctas puedan actualizar, agregar y eliminar datos para proteger su integridad).[33]

- **Disponibilidad**: La disponibilidad es la garantía de que los sistemas responsables de entregar, almacenar y procesar la información son accesibles cuando lo requieren los usuarios autorizados. Medidas para mantener la disponibilidad de los datos puede incluir matrices de discos de sistemas redundantes y máquinas en clúster, software antivirus para evitar que los gusanos destruyan redes y sistemas de prevención de denegación de servicio (DDoS) distribuidos.[34]

- **Autenticidad**: Autenticidad se refiere a la característica de una comunicación, documento o cualquier dato que garantice la calidad de ser genuino o no corrompido. La función principal de la autenticación es confirmar que un usuario

[32] 3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf pág. 22
[33] 3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf pág. 26
[34] 3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf pág. 27

es quien dice ser. Los controles como la biometría, las tarjetas inteligentes y los certificados digitales garantizan la autenticidad de los datos, las transacciones, las comunicaciones o los documentos.

- **No repudio**: El no repudio es una forma de garantizar que el remitente de un mensaje no pueda negar haber enviado el mensaje y que el destinatario no haya recibido el mensaje de denegación. Las personas y la organización usan firmas digitales para garantizar el no repudio.

- **Hacking:**

El Hacking en el campo de la seguridad informática se refiere a explotar las vulnerabilidades del sistema y poner en peligro los controles de seguridad para obtener acceso no autorizado o inapropiado a los recursos del sistema. Implica modificar las características del sistema o de la aplicación para lograr un objetivo fuera del propósito original de su creador. Se puede hackear para robar y redistribuir la propiedad intelectual, lo que lleva a la pérdida de negocios. El Hacking en redes de computadoras generalmente se realiza por medio de scripts u otra programación de red. Las técnicas de Hacking de redes incluyen crear virus y gusanos, realizar ataques de denegación de servicio (DoS), establecer conexiones de acceso remoto no autorizadas a un dispositivo que usa troyanos, puertas traseras, crear redes de bots, detección de paquetes, phishing y descifrado de contraseñas. El motivo detrás del Hacking podría ser robar información o servicios críticos, por emoción, desafío intelectual, curiosidad, experimentación, conocimiento, ganancia financiera, prestigio, poder, reconocimiento de pares, venganza y más.[35]

[35] 3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Hacker Ético

Hacker ético es aquel hacker que se emplean ya sea a través de contratos o empleo directo para probar la seguridad de una organización. Utilizan las mismas habilidades y tácticas como un cracker, pero con el permiso del propietario del sistema para llevar a cabo su ataque contra el Sistema. Además, los hackers éticos no revelan las debilidades de un sistema de evaluación a cualquier persona que no sea el propietario del sistema. Por último, los hackers éticos trabajan bajo contrato para una empresa o cliente, y sus contratos especifican lo que está fuera de los límites y lo que se espera de ellos. Su papel depende de las necesidades específicas de una organización determinada.[36]

Fases del Hacking

En general, hay cinco fases de Hacking las cuales son: Reconocimiento, Escaneo, Ganar acceso, Mantener el acceso, Limpieza de registro.[37]

Reconocimiento: Reconocimiento se refiere a la fase preparatoria en la cual un atacante reúne la mayor cantidad de información posible sobre el objetivo antes de lanzar el ataque. En esta fase, el atacante recurre a la inteligencia competitiva para aprender más sobre el objetivo. Esta fase también puede implicar escaneo de red, ya sea externo o interno, sin autorización. Esta fase permite a los atacantes planear el ataque. Esto puede llevar algo de tiempo ya que el atacante reúne la mayor cantidad de información posible. Parte de este reconocimiento puede implicar ingeniería social. Un ingeniero social es una persona que convence a las personas para que revelen información como números de teléfono, contraseñas y otra información confidencial que no figura en la lista. Por ejemplo, el hacker podría llamar al proveedor de servicios de Internet del objetivo y, utilizando la información personal obtenida previamente, convencer al representante del

[36] ETSINF [En línea]. [Fecha de Consulta: octubre 2020] Disponible en https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1

[37] HACKING CERO AÑO 2011 [En línea]. [Fecha de Consulta: octubre 2020] Disponible en http://www.tugurium.com/docs/HakingCero.pdf

servicio al cliente de que el hacker es realmente el objetivo y, al hacerlo, obtener aún más información sobre el objetivo.[38]

Escaneo: escanear es la fase inmediatamente anterior al ataque. Aquí, el atacante usa los detalles recopilados durante el reconocimiento para identificar vulnerabilidades específicas. El escaneo es una extensión lógica del reconocimiento activo, y, de hecho, algunos intentos no diferencian el escaneo del reconocimiento activo. Sin embargo, hay una ligera diferencia en que el escaneo implica un sondeo más profundo por parte del atacante. A menudo, las fases de reconocimiento y exploración se superponen, y no siempre es posible separar las dos. Información de red como el mapeo de sistemas, enrutadores y cortafuegos utilizando herramientas simples como la utilidad estándar de Windows Traceroute. De forma nativa, pueden usar herramientas como Cheops para agregar información adicional a los resultados de Traceroute. Los escáneres de puertos detectan los puertos de escucha para encontrar información sobre la naturaleza de los servicios que se ejecutan en la máquina de destino. La técnica principal de defensa contra los escáneres es cerrar los servicios que no son necesarios, así como implementar un filtro de puerto apropiado. Sin embargo, los atacantes aún pueden usar herramientas para determinar las reglas implementadas por el filtro de puertos. Las herramientas más comúnmente utilizadas son los escáneres de vulnerabilidad, que pueden buscar miles de vulnerabilidades conocidas en una red objetivo. Esto le da al atacante una ventaja porque él o ella solo tienen que encontrar un solo medio de entrada, mientras que el profesional de sistemas tiene que asegurar la mayor vulnerabilidad posible aplicando parches. Las organizaciones que usan sistemas de detección de intrusos aún deben permanecer atentos, porque los atacantes pueden usar y usarán técnicas de evasión en cada paso del camino.[39]

Ganar acceso: Esta es la fase en la que se produce el hackeo real. Los atacantes usan

[38] INCIBE [En línea]. [Fecha de Consulta: enero 2020] Disponible en https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces
[39] HACKING CERO AÑO 2011 [En línea]. [Fecha de Consulta: octubre 2020] Disponible en http://www.tugurium.com/docs/HakingCero.pdf pág. 114

durante la fase de reconocimiento y exploración para obtener acceso al sistema y la red de destino. A pesar de que los hackers pueden causar mucho daño sin obtener acceso al sistema, el impacto del acceso no autorizado es catastrófico. Por ejemplo, los ataques externos de denegación de servicio pueden agotar los recursos o impedir que los servicios se ejecuten en el sistema de destino. Los atacantes usan una técnica llamada suplantación para explotar el sistema pretendiendo ser un usuario legítimo o sistemas diferentes. Pueden usar esta técnica para enviar un paquete de datos que contenga un error al sistema de destino con el fin de explotar una inundación y también se rompe la disponibilidad de servicios esenciales. Una vez que un atacante obtiene acceso al sistema objetivo, él / ella intenta escalar los privilegios para tomar el control completo del sistema objetivo.[40]

Mantener el acceso: una vez que un atacante obtiene acceso al sistema de destino con privilegios de administrador / nivel de raíz (siendo el propietario del sistema), puede utilizar el sistema y sus recursos a voluntad, y puede usar el sistema como una plataforma de lanzamiento para explorar y explotar otros sistemas, o para perfilar y continuar explotando el sistema. Ambas acciones pueden causar gran cantidad de problemas. Por ejemplo, el hacker podría implementar un rastreador para capturar una sesión de tráfico de red y sesiones de FTP (protocolo de transferencia de archivos) con otros sistemas, y luego transmitir esos datos donde le plazca. Los atacantes que eligen no ser detectados eliminan la evidencia de ellos e instalan una entrada en su totalidad para repetir el acceso. También pueden instalar a nivel de núcleo el acceso administrativo del sistema a los rotitos de destino en el nivel de troyanos en operación, mientras que en la computadora. Los rotitos obtienen acceso a los rotitos y requieren que los usuarios obtengan acceso al caballo de Troya en el nivel de la aplicación. Ambos para instalarlos localmente. En los sistemas Windows, la mayoría de los troyanos se instalan como un servicio y se ejecutan como sistema local, con acceso administrativo. Los hackers pueden usar troyanos para transferir nombres de usuario, contraseñas y cualquier otra información almacenada en

[40] ELHACK.INFO [En línea]. [Fecha de Consulta: octubre 2020] Disponible en https://ehack.info/las-fases-del-hacking-etico/

el sistema. Pueden mantener el control del sistema durante mucho tiempo mediante el cierre de vulnerabilidades para evitar que otros hackers tomen el control de ellos, y en ocasiones, en el proceso, ofrecen cierto grado de protección al sistema frente a otros ataques.[41]

Limpieza de registro: Por razones obvias, como evitar problemas legales y mantener el acceso futuro, los atacantes generalmente intentan borrar toda evidencia de sus acciones. Los atacantes utilizan utilidades como las herramientas, netcat o troyanos para borrar sus huellas de los archivos de registro del sistema. Una vez que los troyanos están en su lugar, es probable que el atacante haya obtenido el control total del sistema. Los atacantes pueden ejecutar scripts en el troyano o rootkit para reemplazar el sistema crítico y los archivos de registro para ocultar su presencia en el sistema. Otras técnicas incluyen estenografía y tunelización. La estenografía es el proceso de ocultar datos en otros datos, por ejemplo, archivos de imagen y sonido. El túnel aprovecha el protocolo de transmisión al llevar un protocolo sobre otro. Los atacantes pueden usar incluso una pequeña cantidad de espacio adicional en los encabezados TcP e IP del paquete de datos para ocultar información. Un atacante puede usar el sistema comprometido para lanzar nuevos ataques contra otros sistemas o como un medio para alcanzar otro sistema en la red sin ser detectado. Por lo tanto, esta fase del ataque puede convertirse en la fase de reconocimiento de otro ataque. Los administradores del sistema pueden implementar identificadores basados en host (sistemas de detección de intrusiones) y software antivirus para detectar troyanos y otros archivos y directorios aparentemente comprometidos. Como hacker ético, debe conocer las herramientas y técnicas que despliegan los atacantes para que pueda defender e implementar contramedidas, detalladas en los módulos posteriores. [42]

[41] ETSINF [En línea]. [Fecha de Consulta: octubre 2020] Disponible en https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1 pág. 74

[42] ETSINF [En línea]. [Fecha de Consulta: octubre 2020] Disponible en https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1 pág. 74

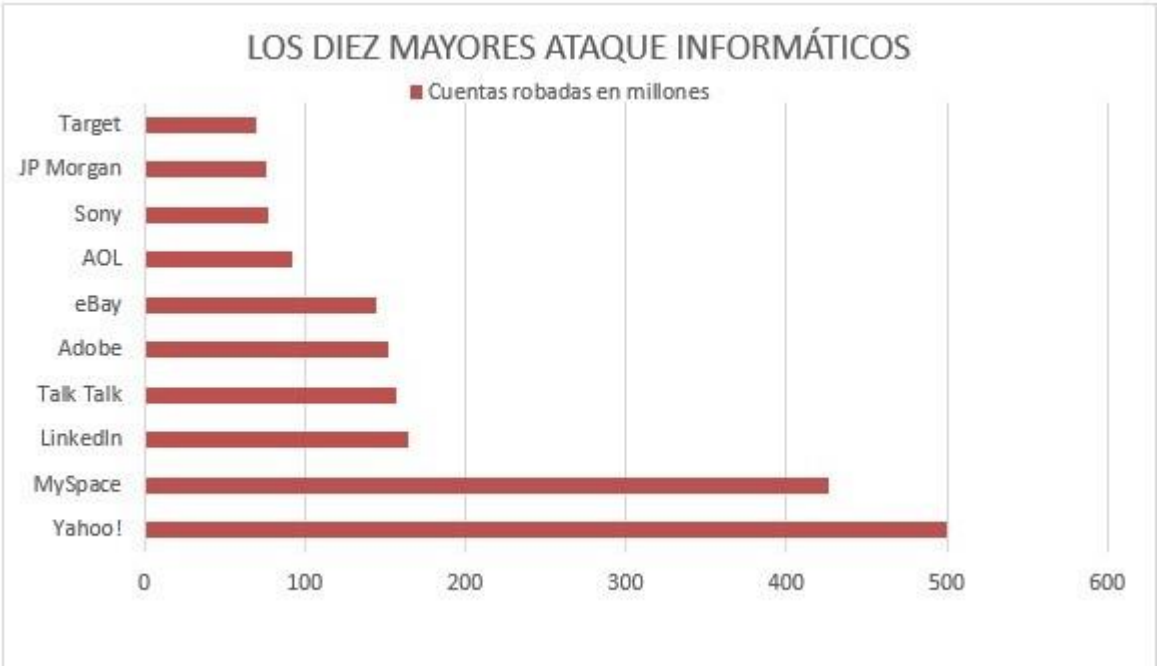
4.2 MARCO TEORICO

La seguridad en los activos de una organización es fundamental para todo tipo de entidad, sin embargo, no es una tarea fácil de ejecutarse ya que son muchos los factores que deben tenerse en cuenta para cumplir a cabalidad y mitigar la mayor cantidad de riesgos posibles que afecten de manera significativa la confidencialidad, integridad y disponibilidad,

A continuación, se evidencian las brechas de seguridad que fueron explotadas por los ciberdelincuentes en grandes organizaciones

4.2.1 Brecha de Datos en eBay

Figura 1. Los diez mayores ataques informáticos



4. **Fuente 1.** Financial Times

Problema: eBay Inc. Es una corporación multinacional americana y empresa de comercio electrónico que proporciona al consumidor servicios de venta a través de internet. eBay inc. Reveló que un incidente de seguridad recientemente tuvo lugar, hackers comprometieron 145 millones de usuarios con contraseñas, direcciones de correos electrónicos, fechas de cumpleaños, direcciones de envió, y otra información personal contenidos en archivos, que resultó en una de las mayores violaciones de datos en la historia.

Causa: Los hackers entraron al sistema después de obtener las credenciales de inicio de sesión de un pequeño número de empleados, permitiéndoles el acceso a la red corporativa de eBay, luego llevaron a cabo un ataque de scripting entre sitios y con código malicioso que se utilizó para desviar los clientes a un falso sitio web que preguntaba usuario y contraseña. De este modo, los hackers registraron las credenciales de todos estos usuarios.

Solución: eBay aconsejó a sus clientes el cambio inmediato de contraseñas, indicando que el suyo estaba entre los datos robados por los Ciber criminales Google Play [43]

4.2.2 Brecha de Datos en Google play.

Problema**:** El hacker turco Ibrahim Balic derribó todo el sistema de Google Play's dos veces, previniendo a desarrolladores de subir nuevas aplicaciones y actualizando las aplicaciones existentes, y previniendo que usuarios descargan contenido.

Causa: Balic, quien previamente había hackeado la página Apple Developer, escribió un APK mal formada para probar la vulnerabilidad de la base de datos de aplicaciones de

[43] WELIVESECURITY [En línea]. Mayo 2014 [Fecha de Consulta: septiembre 2020] Disponible en https://www.welivesecurity.com/la-es/2014/05/21/ebay-confirma-brecha-seguridad-recomienda-cambiar-contrasenas/

Android, el cual, al subirlo a Google Play, afectó el todo el sistema, causando un ataque de DoS.

Balic no detuvo ese primer intento. El subió de nuevo para confirmar que era su trabajo que había derribado el sistema. Este resultó en un segundo ataque de DoS, una vez que causó el choque de la base de datos. Como resultado, desarrolladores y los usuarios fueron incapaces de subir o descargar alguna aplicación.

4.2.3 Brecha de Datos en The Home Depot.

Problema: The Home Depot es un minorista americano de remodelación de casas y productos y servicios de construcción. Recientemente en los últimos meses fue revelado un incidente de seguridad, afectando a 56 millones de cuentas de tarjetas débito y crédito.

Causa: De acuerdo con el reporte de investigación, el hacker instaló un software malicioso llamado “BlackPOS” en el sistema de auto pago en las tiendas, con este capturaban datos de las tarjetas de los clientes cuando usaban las terminales, y al hacerlo, comprometían la información confidencial.

Solución: The Home Depot advirtió a los clientes de protegerse de fraudes de phishing el cual te pide que proporciones información personal vía email y telefónico. En particular, esto causó que los clientes no hicieran clic en links de correos de origen no confiable.

4.2.4 Brecha de Seguridad en JPMorgan Chase & Co.

Problema: JPMorgan Chase & Co. es una firma líder global de servicios financieros, y el instituto bancario más grande de estados unidos. Hackers llevaron a cabo un ciberataque en la compañía comprometiendo las cuentas de 76 millones de hogares y 7 millones de pequeñas empresas.

Causa: De acuerdo con el reporte forense, hackers obtuvieron información de programas y aplicaciones que se ejecuta en computadoras de JPMorgan's, y encontraron vulnerabilidades en cada programa y aplicación web que les proporcionó un punto negro de entrada en el sistema del banco. Eventualmente, los hackers ganaron acceso a los nombres, direcciones, números telefónicos, y mails de cuentas bloqueadas de JPMorgan.

Solución: Uno debe regularmente monitorear todas las cuentas y debe leer cada transacción en la declaración de crédito todos los meses para mantenerse libre de robos en línea al poder identificar información errónea.

4.3 MARCO LEGAL

Legislaciones vigentes en Ciberseguridad

Se selecciona como legislación la ley 599 de 2000 artículo 195 del código penal en la que se manifiesta que es considerado un delito el acceder a sistema informático que en este caso estaba protegido por ser el sistema del banco, por lo tanto, el trabajador será sancionado con una multa. Según el Artículo 25. De la Ley 1288 de 2009 se modifican las penas delitos de acceso a un sistema informático con el artículo con el artículo 420 en la que indica que haber utilizado indebidamente la información privilegiada de la entidad administrativa o entidad pública y si lo hizo con conocimiento en sus funciones, en los que claramente su fin fue el de obtener beneficios para sí mismo o para personas terceras tiene como consecuencia de la pérdida de su empleo una y la multa por el valor que aplique según el delito [44]

El artículo 269A encontramos también la multa que incurre al tener acceso sistema informático que en este caso de se debe cumplir una pena de prisión que varía desde

[44] COLOMBIA CODIGO PENAL. Ley 599 DE 2000 art 195 año 2019

los 48 a 96 meses y deberá pagar una multa de 100 a 1000 salarios mínimos legales vigentes, como consecuencia de sus actos criminales al haber implementado un malware para vulnerar los sistemas de los cajeros electrónicos este empleado del banco deberá cumplir la pena mencionar anteriormente, adicionalmente la ley también indica que cometer este delito se pierde el empleo inmediatamente. [45]

Esta es una ley básicamente se regula el sector de tecnología de la información y comunicaciones en protección al usuario, calidad de servicio, versión en el sector administración de recursos control y vigilancia por lo tanto vamos a tomar el artículo 63 que trata sobre las infracciones y sanciones de las normas de esta ley mandó como primera instancia el número uno de no respetar la confidencialidad observar las comunicaciones, este empleado de la compañía violó la confidencialidad en los cajeros automáticos ya que accedió y permitió el acceso a personas o por medio de programas externos para poder vulnerar y así modificar la información en el caso de que al momento de ingresar la transacción el cajero arrojar todo el dinero que tenía almacenado, según el artículo 65 de las acciones a las que incurrió este esta persona en cuanto al artículo 64 es una multa equivalente a 2000 salarios mínimos mensuales legales vigentes igualmente se le suspende la operación de su trabajo y la cancelación o licencia de ingeniero teniendo en cuenta según el artículo 66 que esto es una falta de gravedad alta.[46]

En están ley hace referencia sobre el convenio de Budapest o también conocido como el convenio de la ciber delincuencia este es un tratado internacional elaborado en Europa en el que se estipulan las infracciones de seguridad fraudes informáticos, pornografía, violaciones de seguridad y cuyo objetivo es aplicar medidas penales para proteger a la

[45] COLOMBIA MINISTERIO DE LAS TECNOLOGIAS Ley 1273 de 2009 mintic, año 2019. Por medio se crea un nuevo bien jurídico tutelado “De la protección de la información y de los datos”
[46] COLOMBIA MINISTERIO DE LAS TECNOLOGÍAS. Ley 1341 de 2009, por la cual se establecen los conceptos y principios de Seguridad de la información.

sociedad en caso de crimen crímenes. En el año 2018 acogió este convenio para así adoptar las medidas a las leyes del país. [47]

En el artículo 6 que habla sobre el uso de los dispositivos es considerado cualquier delito el uso de algún dispositivo o programa informático que esté diseñado atado o que tenga acceso ilícito, interceptación de datos, yo terceras personas hacer de forma ilegal a la información y configuración de los cajeros electrónicos a nivel nacional.

En el artículo 8 se considera un delito todo tipo de alteración borrado supresión de datos o interferencia en el funcionamiento del sistema informático con el fin de obtener algún beneficio económico para el delincuente terceras personas.

4.4 MARCO ESPACIAL

Zero Day Ltda. Es una empresa que tiene como objeto la consultoría de seguridad informática en Colombia. Uno de sus clientes; NOSTRADAMUS S.A.S, es una empresa del sector tecnológico que brinda servicios a los sectores: educativo, corporativo y gubernamental en temas relacionados con proyectos de educación y capacitación a través del uso de TIC desde la implementación y configuración de plataformas de aprendizaje brindando capacitación y soporte 24/7En la semana anterior NOSTRADAMUSS.A.S, sufrió un ataque informático que afecto la imagen corporativa de la organización presentándose robo de información a partir de ataques remotos. Qué tiene como objeto la consultoría de seguridad informática en Colombia. Uno de sus clientes; NOSTRADAMUS S.A.S, es una empresa del sector tecnológico que brinda servicios a los sectores: educativo, corporativo y gubernamental en temas relacionados con proyectos de educación y capacitación a través del uso de TIC desde la implementación y configuración de plataformas de aprendizaje brindando capacitación y soporte 24/7.

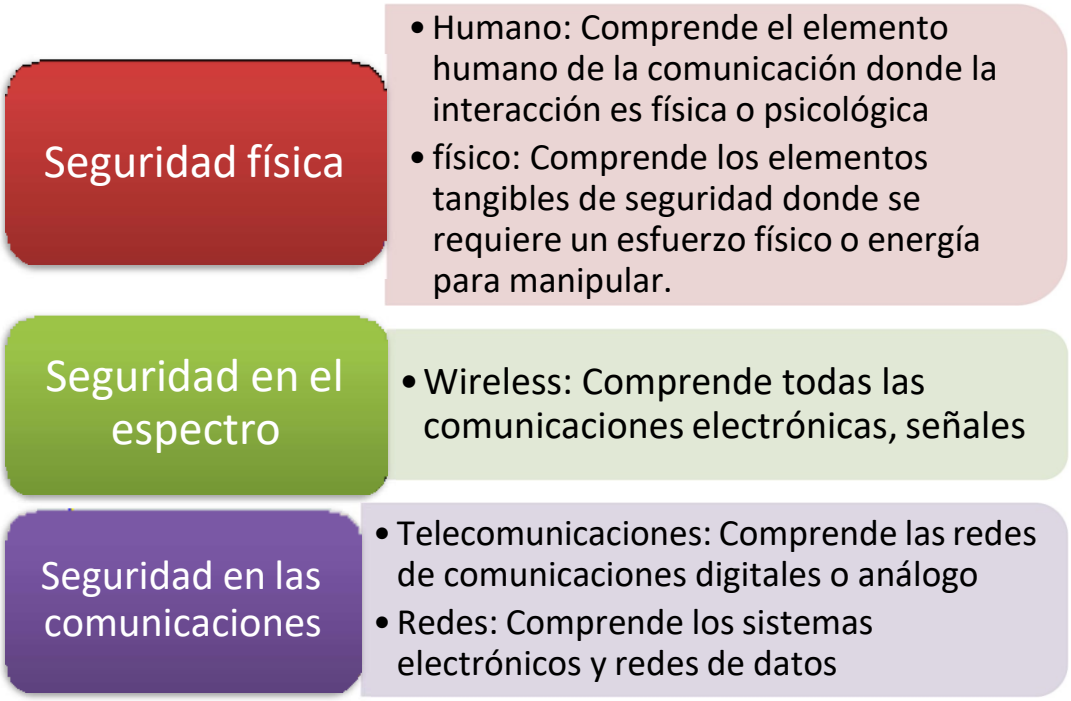
[47] COLOMBIA MINISTERIO DE LAS TECNOLOGÍAS. Ley 1928 24 julio 2018 Por la cual se aprueba el convenio sobre la Ciberdelincuencia

5 MARCO TECNOLOGICO

5.1 Canales de la metodología osstmm

Para el inicio de la metodología de OSSTMM es necesario conocer los canales y las respectivas divisiones las cuales están representadas en gráfico, siguiente lo cual permite reconocer y facilitar los procesos de prueba. [48]

Figura 2 Canales de la metodología OSSTMM



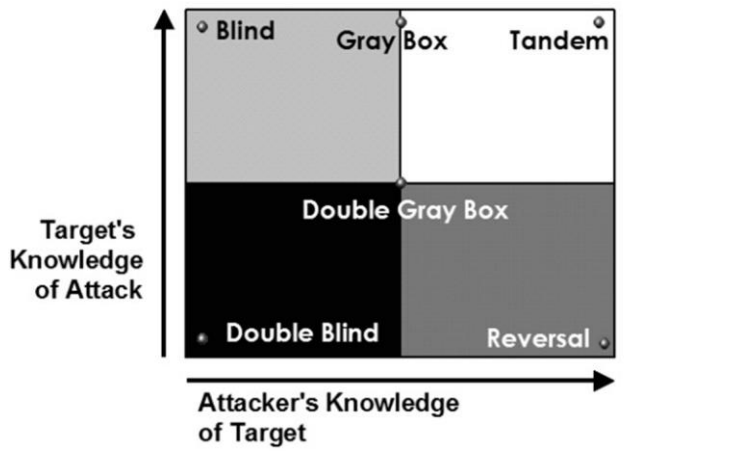
Fuente 2 El autor

5.2 Tipos comunes de test

OSSTMM cuenta con diferentes tipos de test que permiten al evaluador conocer los objetivos esperados en el test y su legitimidad.

[48] OSSTMM [En línea]. Marzo 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.isecom.org/OSSTMM.3.pdf

Figura 3 OSSTMM Tipos de test



Fuente 3 OSSTMM

- Blind: También conocida como ethical hacking y se realiza cuando el analista de seguridad no posee ningún conocimiento de los objetivos a auditar, lo cual es considerado como “una auditoria ciega”.
- Doble Blind: También conocida como prueba de caja negra, al igual que el tipo blind el analista no tiene conocimiento alguno de los objetivos lo cual permite que el analista realice las evaluaciones al equipo de seguridad forma de respuesta.
- Gray Box: En este tipo el analista tiene algún conocimiento de los canales a evaluar ya que en muchas ocasiones inicia como una autoevaluación y el equipo está preparado para la auditoria
- Double Gray Box: también es conocida como White box, donde se tiene pleno conocimiento de los activos y conocimiento de los canales, se notifican los objetivos, pero no los detalles de la auditoria.
- Tandem: También es conocido como auditoría interna donde el analista como el objetivo están preparados para la realización de la auditoria conociendo todos los detalles

- Reversal: Conocido como los ejercicios de Red Team donde se tiene pleno conocimiento de procesos y operaciones de seguridad donde se pretende evaluar a los equipos de defensa. [49]

5.1.1 Módulos de prueba

Con el fin de realizar el Test apropiado es necesario comprender cómo opera cada uno de ellos, lo cual varía dependiendo de cada línea de negocio y los tiempos destinados para cada auditoria, en la metodología se encuentran las siguientes fases:

A. Fase de inducción
B. Fase de interacción
C. Fase de investigación
D. Fase de intervención

5.1.2 Fase de inducción

En la fase de inducción los analistas inician con identificación de los requerimientos de la auditoría, tales como el alcance y limitaciones. [50]

> A.1 Posture review: (Revisión previa): Es la revisión de reglas, normas, culturas, legislaciones, políticas que son aplicables a los objetivos, es conocer que se puede y debe hacer
>
> A.2 Logistic (Logística): Es la medición de las interacciones tales como distancia, velocidad, precisión en los resultados, lo cual permite conocer las limitaciones en la auditoria lo cual permite minimizar errores y ser más eficientes.

[49] OSSTMM [En línea]. Marzo 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.isecom.org/OSSTMM.3.pdf pág. 37
[50] OSSTMM [En línea]. Marzo 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.isecom.org/OSSTMM.3.pdf pag 99

A.3 Active Detection verification (Detección Activa): Conoce cuales son los controles activos y pasivos, es posible que estén alerta de los tipos de pruebas a realizar.

5.1.3 Fase de interacción

En esta fase de seguridad se requiere conocer el alcance con relación a las interacciones con los objetivos, básicamente se define el alcance.

B.4 Visibility Audit (Visibilidad): Se determinan los objetivos dentro del alcance.
B.5 Access verification (verificación de acceso): Es la medición de los puntos de acceso, se verifica todo lo relacionado con un punto de acceso.
B.6 Trust verification: (verificación de confianza): Es la medición Conocer cuáles son las relaciones de confianza entre los objetivos, existe una relación de confianza cuando se acepta la interacción entre objetivos del alcance.
B.7 Control Verification (verificación de control): es la medición para determinar la efectividad de controles de no repudio, confidencialidad, privacidad e integridad

6 DISEÑO METODOLOGICO

6.1 TIPO DE INVESTIGACIÓN

Proyecto aplicado

6.2 TÉCNICAS DE RECOLECCIÓN Y ANÁLISIS DE LA INFORMACIÓN

las técnicas de recolección de la información son las siguientes:
La primera de ellas la observación que de forma sistemática se capta por medio de la vista de los fenómenos que se están presentando.

En la observación se encuentran los siguientes ítems qué son básicamente los que se tienen en cuenta al momento de realizar este tipo de técnica

- Lugares
- Personas

La entrevista que permite realizar un diálogo entre el entrevistador y el entrevistado sobre un tema relacionado con él tipo de las entrevistas que se clasifican en los siguientes tipos:

- Entrevistas no estructuradas qué es aquella en la que la persona que realiza la entrevista no contiene un listado de preguntas seleccionadas, sino que la entrevista se desarrolla de una forma informal.
- Las entrevistas semi estructuradas que son aquellas que se realizan utilizando un guion con preguntas abiertas las cuales son realizadas al entrevistado no tienen un orden determinado y dejan que la entrevista fluya libremente
- Las entrevistas estructuradas son aquellas en las que el entrevistador se está realizando preguntas aleatorias al entrevistado en base a un cuestionario que ya se tiene previamente preparadas este guion de preguntas suelen ser cerradas elaboradas y de formas de secuencia las respuestas deben ser bien concretas sobre el tema que se está interrogando.

6.3 POBLACIÓN ESTUDIADA

La población estudiada en este trabajo básicamente se encuentra en la empresa Nostradamus cómo se va a realizar un escaneo de vulnerabilidades es necesario identificar que las personas están bien concientizadas de los riesgos que pueden existir al abrir correos electrónicos de fuentes desconocidas por tal motivo esta población son todas las personas que elaboran en la compañía.

6.4 PROPUESTA METODOLOGICA PARA EL DESARROLLO DEL TESTEO

METODOLOGÍA ABIERTA DE PRUEBA DE SEGURIDAD A PARTIR DE LA METODOLOGIA OSSTMM

Esta metodología se encarga de realizar seguimientos a los objetivos de prueba utilizando herramientas con esta metodología es posible realizar una recopilación de datos de forma activa y pasiva

OSSTMM (Open Source Security Testing Methodology Manual) es una metodología para realizar pruebas de seguridad de forma exhaustiva ya que realiza de forma precisa en un nivel operativo, esta es una metodología fue creado como un proyecto de fuente abierta facilita que cualquier profesional en temas de seguridad pueda realizar y contribuir al desarrollo de pruebas mucho más eficientes.[51]

Esta metodología está basada en detalles técnicos los cuales deben ser evaluados, Y permite resolver interrogantes como que se debe hacer antes durante y después de realizar una prueba de seguridad igualmente permite medir de forma eficaz los resultados, OSSTMM está dividida en seis grupos los cuales se mencionan a continuación:[52]

1. seguridad de la información
2. seguridad de los procesos

[51] INTRODUCCIÓN A OSSTMM (Open-Source Security Testing Methodology Manual) [En linea]. Noviembre 2015 [Fecha de Consulta: septiembre 2020] Disponible en http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual#:~:text=OSSTMM%20(Open%20Source%20Security%20Testing%20Methodology%20Manual)%20proporciona%20una%20metodolog%C3%ADa,evita%20suposiciones%20y%20evidencia%20anecd%C3%B3tica.

[52] TEST DE INTRUSIÓN: METODOLOGÍAS OSSTMM E ISSAF [En línea]. Marzo 2011 [Fecha de Consulta: octubre 2020] Disponible en https://www.isacavalencia.org/docs/Eventos/2011/201103_25_Carlos.pdf

3. seguridad en las tecnologías de internet
4. seguridad en las comunicaciones
5. seguridad inalámbrica
6. seguridad física

7 DESARROLLO DE LOS OBJETIVOS

7.1 DESARROLLO OBJETIVO ESPECIFICO 1

Ejecutar el plan de actividades usando técnicas de hacking ético, para el hallazgo de vulnerabilidades. METODOLOGIA OSSTMM se determinan las siguientes fases:

- **Planeación y especificación**: Corresponde a la reunión inicial de apertura donde se socializan las actividades a realizar, se determina el alcance del proyecto y lo más relevantes, para este caso de estudio aplica para la ejecución de los escenarios correspondientes a los ataques que fue víctima la empresa NOSTRADAMUS SAS

  - Elevación de privilegios con Lazagne.
  - Denegación de servicios.
  - Ransomware.
  - Ingeniería social con metasploit.
  - Inyección de código SQL

- **Alcance y riesgos**: Se realizará la evaluación junto con la empresa NOSTRADAMUS SAS los riesgos a los que se expone si se materializan estos ataques. En caso de materializarse estos ataques la empresa NOSTRADAMUS SAS puede perder información.,
- **Levantamiento de información**: Se realizará la recolección de la información de la empresa NOSTRADAMUS ya sea pública o privada y se identificaran los vectores de ataque.

Para el desarrollo de los diferentes escenarios se cuenta con un equipo con las siguientes características:

- Sistema operativo MacOS High Sierra
- versión 10.13.6 2.5 GHZ Intel core i5
- 6 GB de RAM

Figura 4 Características equipo anfitrión

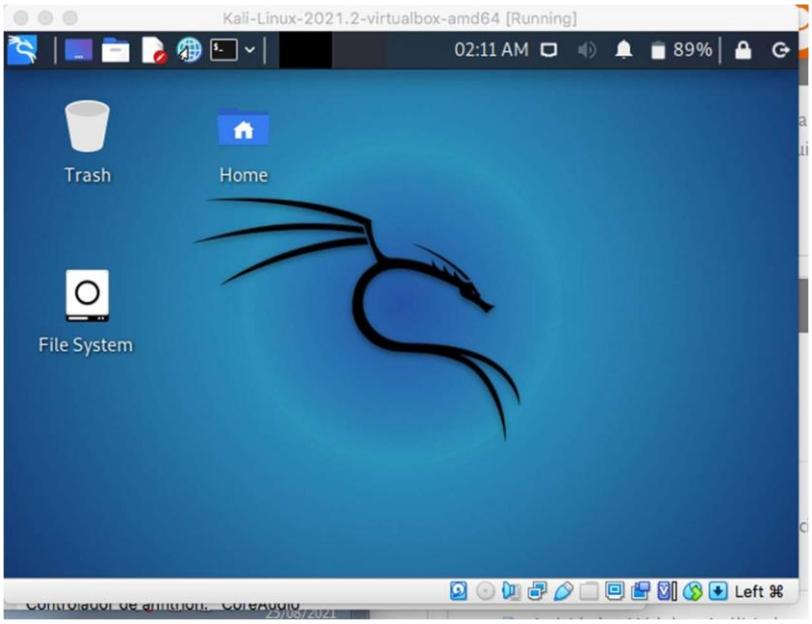
Fuente 4 El autor

Las maquinas se crean sobre ambiente virtualizado en el software libre virtual box como se evidencia en las figuras 5 y 6 con las siguientes características:

Maquina atacante

- Sistema operativo Debian Linux de 64 bytes
- 2 GB de RAM
- Disco duro tipo SATA de 80 Gigabytes

Figura 5 Maquina atacante – Kali Linux

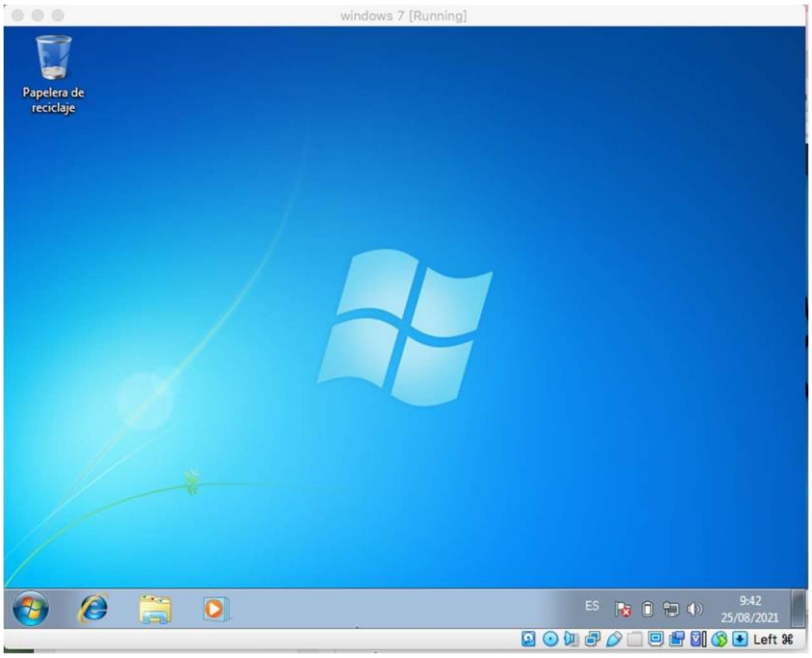


Fuente 5 el autor

Maquina victima

Windows 7 de 64 bytes
□ 2 GB de RAM
□ Disco duro tipo SATA de 32 Gigabytes

Figura 6 Maquina Victima – Windows 7

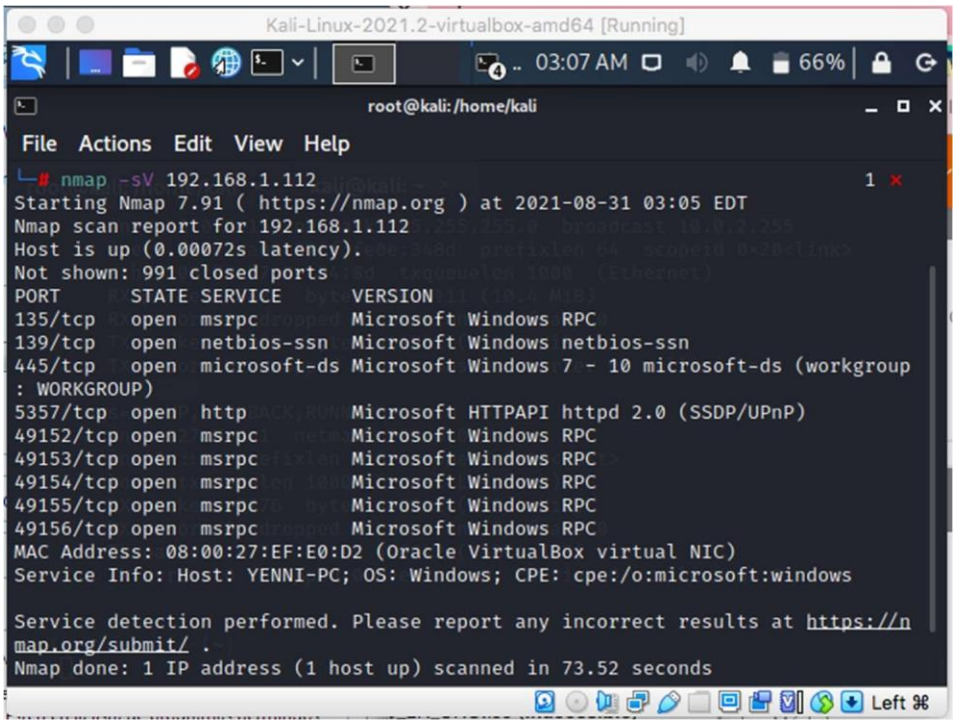


Fuente 6 EL autor

- **Escaneos**: En esta fase se realizarán las respectivas revisiones de los equipos comprometidos, para identificar las vulnerabilidades presentes, posibles causas que permitieron la materialización del ataque.

  Para esta actividad de escaneo se va a realizar una evaluación de la maquina víctima, con el fin de identificar los puertos que tenga abiertos y otra información relevante que pueda ser de utilidad, para ello se realizara con la ayuda de la herramienta NMAP y por medio del comando nmap -sV que nos indica los puertos y la versión del sistema operativo, tal como lo que se evidencia en la figura 7

Figura 7 Escaneo con Nmap



Fuente 7 El autor

- **Revisión de vectores de ataque**: Se realiza el trabajo de campo con la colaboración de los especialistas y de entornos controlados basándose en la

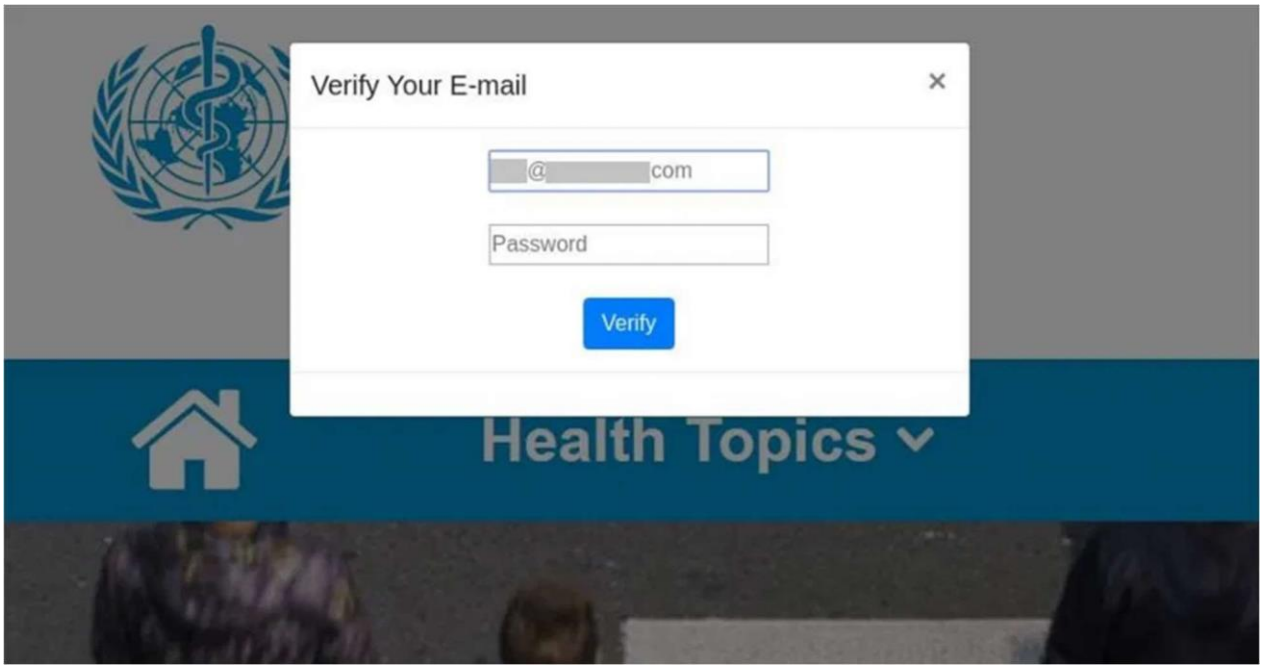
información recolectada, cuyo objetivo es establecer el vector de ataque del ciberdelincuente e identificar posibles cómplices internos dentro de la empresa.

- **Explotación**: Se realiza la explotación de las vulnerabilidades presentes y se deja evidencia de como el atacante logro vulnerar los sistemas de la empresa NOSTRADAMUS S.A.S.

  - **Ingeniería social con metasploit.**

  Este ataque está compuesto por dos partes, la primera de ellas corresponde a la ingeniería social y la segunda al exploit por el navegador, para la realización de la campaña de ingeniería social solo es suficiente que el ciberdelincuente diseñe un mensaje atractivo para la víctima en donde le manifiesta que debe ingresar a una URL sospechosa o confirmar los datos tal como se evidencia en la imagen.

Figura 8. Email suplantando a la OMS con un enlace malicioso.



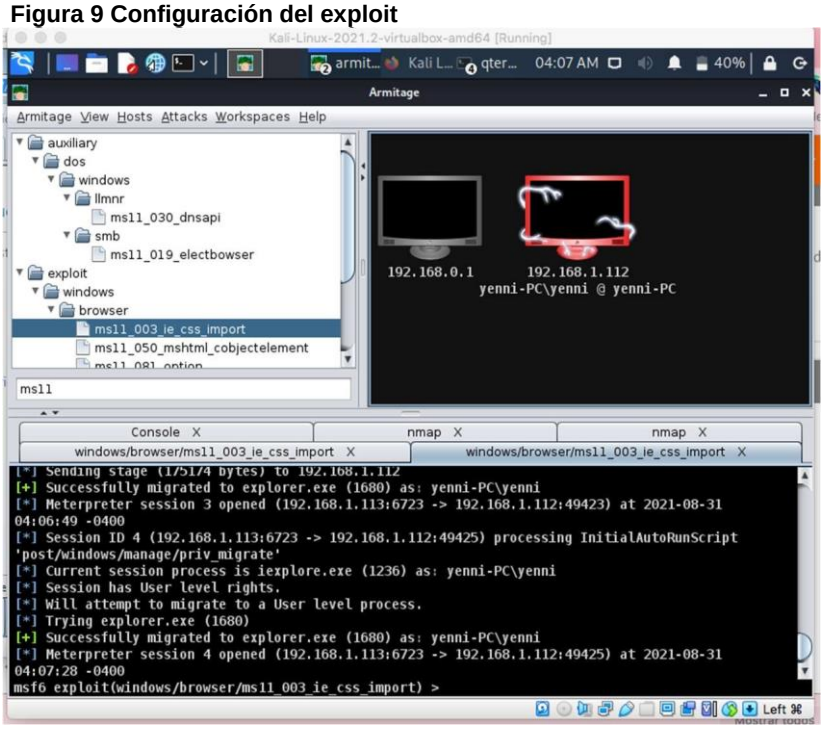
Fuente 8 Agencia española protección de datos

La siguiente parte corresponde al uso de la herramienta metasploit que ejecuta el exploit *ms11_003_ie_css_import*[53]

Es posible ejecutar este exploit gracias a la vulnerabilidad de corrupción de memoria dentro del motor HTML. Ya que cuando se analiza la página HTML con importación recursivas de CSS, es decir, un objeto C ++ se elimina y luego se reutiliza, lo que permite la ejecución de códigos de forma arbitraria y es posible ejecutarlo cuando las maquinas Windows tienen instalado la versión. NET 2.0.50727.[54]

Al realizar este ataque de forma exitosa es posible tener realizar una exploración completa del equipo, con la herramienta armitage se evidencia que se puede realizar la ejecución del exploit en la maquina victima tal como se evidencia en la figura 9.

Figura 9 Configuración del exploit



Fuente 9 El autor

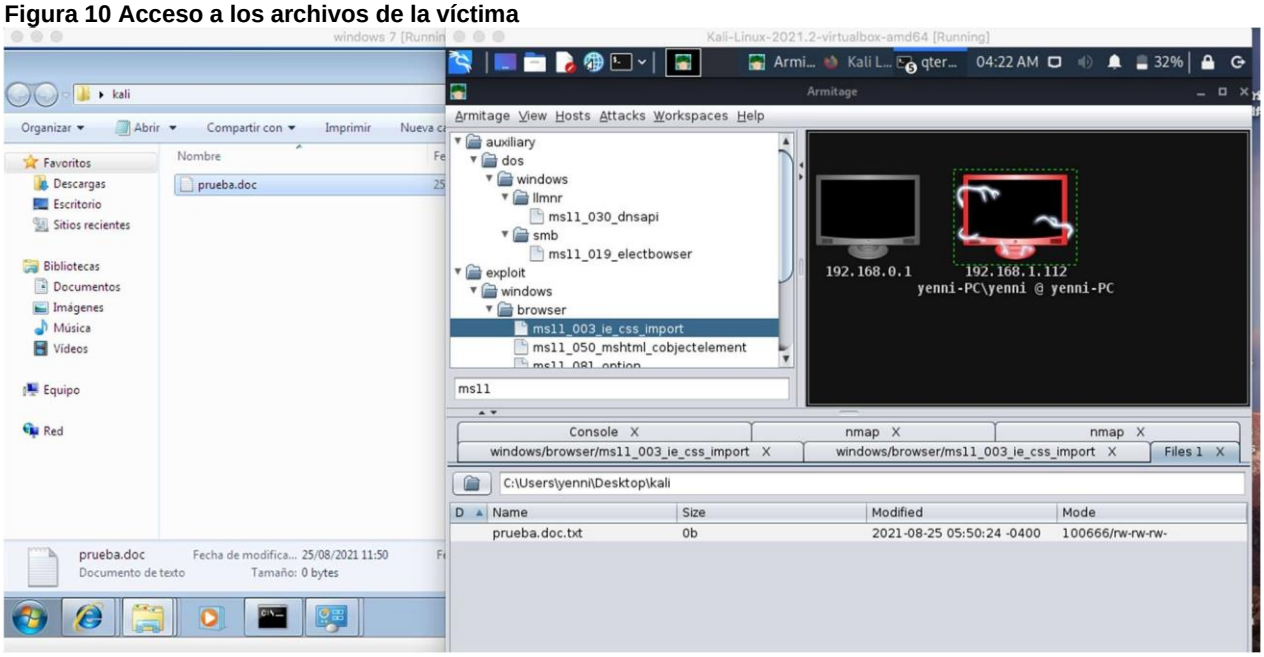
[53] Cyber Shield, *Exploit Internet Explorer 8 on win 7*, [en línea] [Fecha de consulta] agosto de 2021, disponible en https://www.youtube.com/watch?v=h8xOnfQlxDE.

[54] Exploiting MS11_003 Internet Explorer Vulnerability Using Metasploit Framework [En línea]. Noviembre 2011 [Fecha de Consulta: agosto 2021] Disponible en https://www.hacking-tutorial.com/hacking-tutorial/exploiting-ms11_003-internet-explorer-vulnerability-using-metasploit-framework/#sthash.3XBwvXTW.dpbs

De la misma forma es posible acceder a las carpetas y demás archivos que se tengan en la maquina victima tal como se evidencia en la figura 10.

.

Figura 10 Acceso a los archivos de la víctima



Fuente 10 el autor

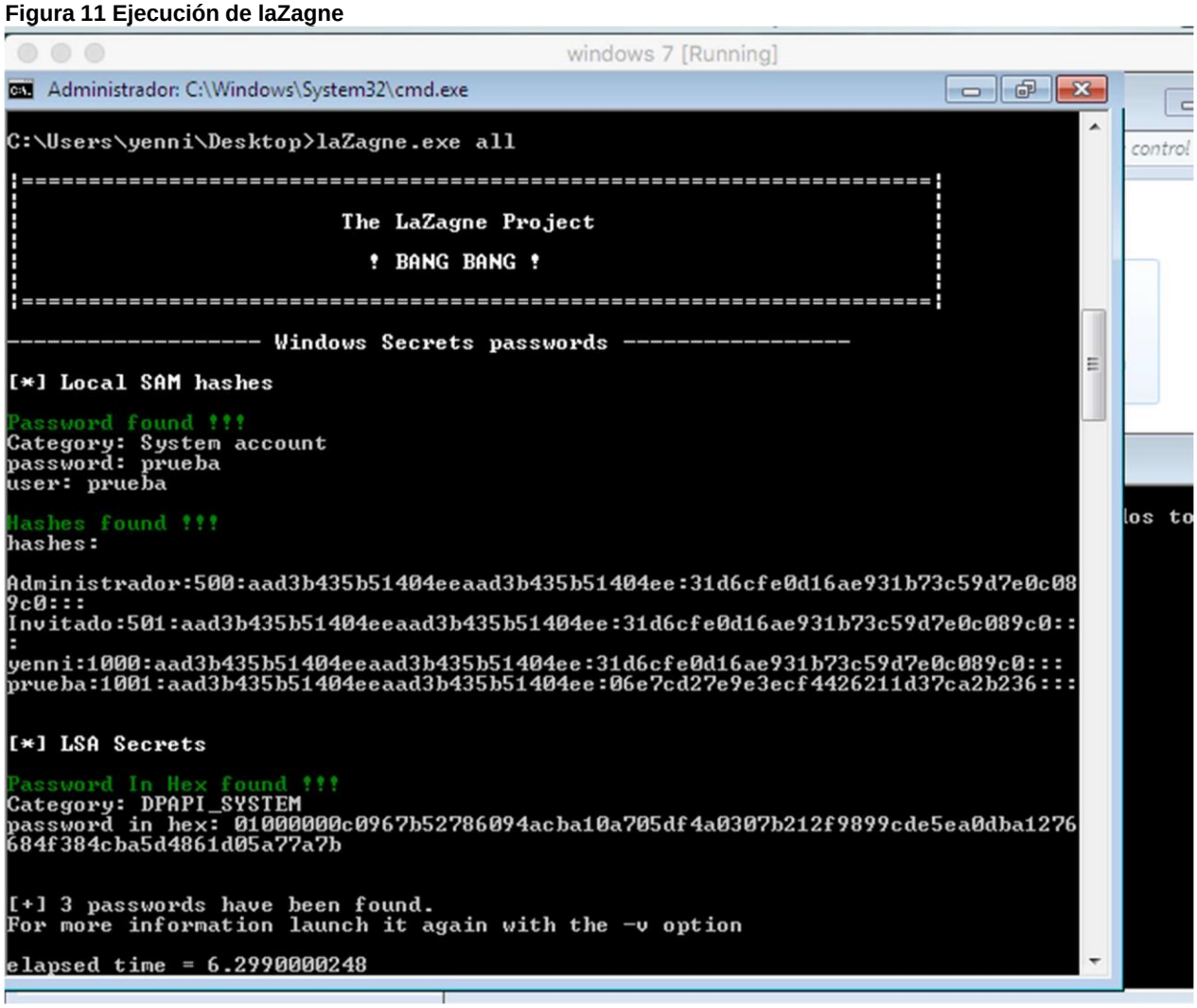
- **Elevación de privilegios con Lazagne.**

La herramienta LaZagne permite recuperar contraseñas en los sistemas operativos de linux y Windows este proyecto de código abierto revela las contraseñas almacenadas en los equipos locales, navegadores, correos electrónicos entre otros[55].

[55] Backtrackacademy [En línea]. Marzo 2016 [Fecha de Consulta: agosto 2021] Disponible en https://backtrackacademy.com/articulo/lazagne-la-herramienta-para-obtener-credenciales-almacenadas-en-el-sistema

Una vez se tiene instalado el ejecutable lazagne.exe desde la ruta donde se descargó se evidencia la maquina victima tiene configurado un usuario llamado prueba y se visualiza la contraseña tal como se evidencia en la figura 11.

Figura 11 Ejecución de laZagne

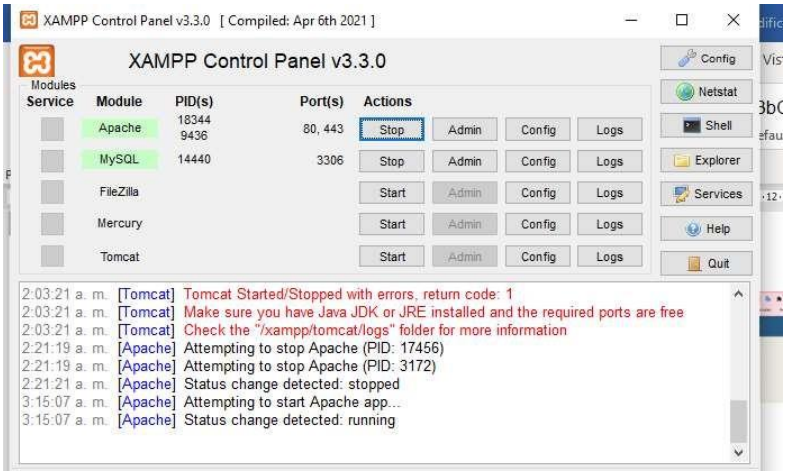


Fuente 11 El autor

- **Denegación de servicios.**

Para realizar el ataque de denegación de servicios es necesario tener instalado en nuestra maquina victima el servidor de servicios Xampp el cual será configurado como el localhost como se evidencia en la figura 12.

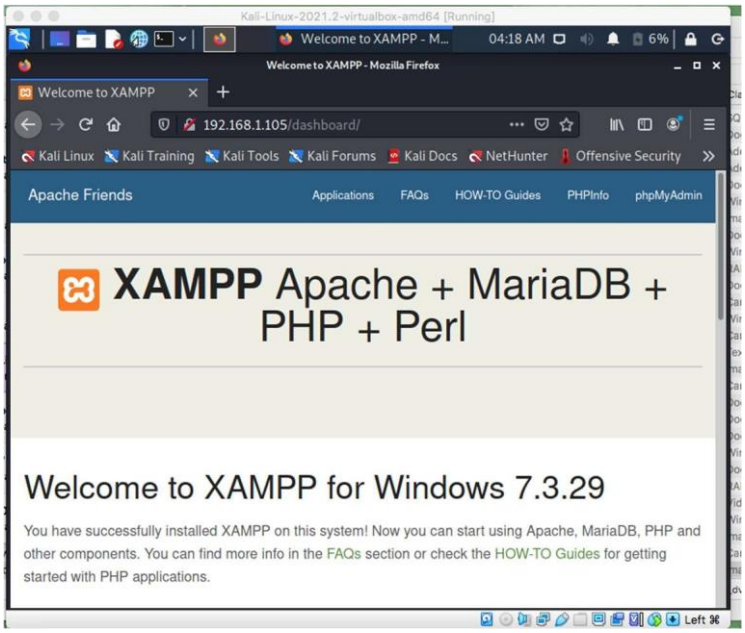
Figura 12 Panel de control XAMPP



Fuente 12 El autor

Para la ejecución de este ataque se usará el programa de slowloris el cual permite a los atacantes establecer comunicación con el servidor objetivo y realizar muchas conexiones HTTP de forma simultánea por el mayor tiempo posible, cuando se supera el número de conexiones permitidas en el servidor colapsa y ocurre la denegación de servicios

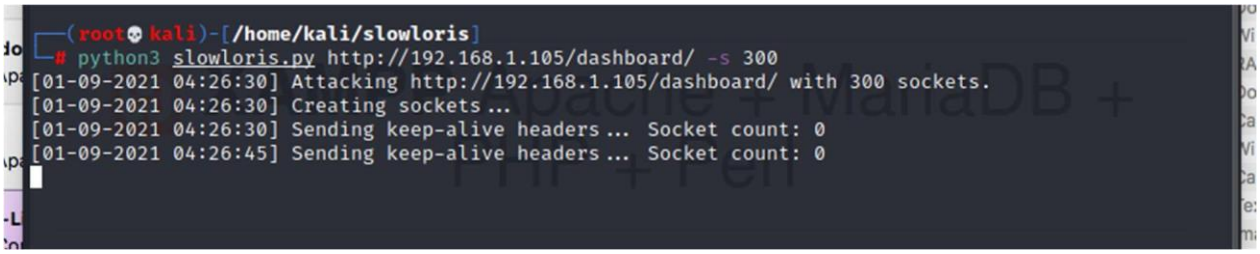
Figura 13 Localhost maquina victima



Fuente 13 El autor

Una vez realizada la instalación y se valide la conexión con la máquina de Windows como se evidencia en la figura 13 y se inicia el ataque de denegación de servicios desde la máquina virtual de Kali Linux con los siguientes comandos.

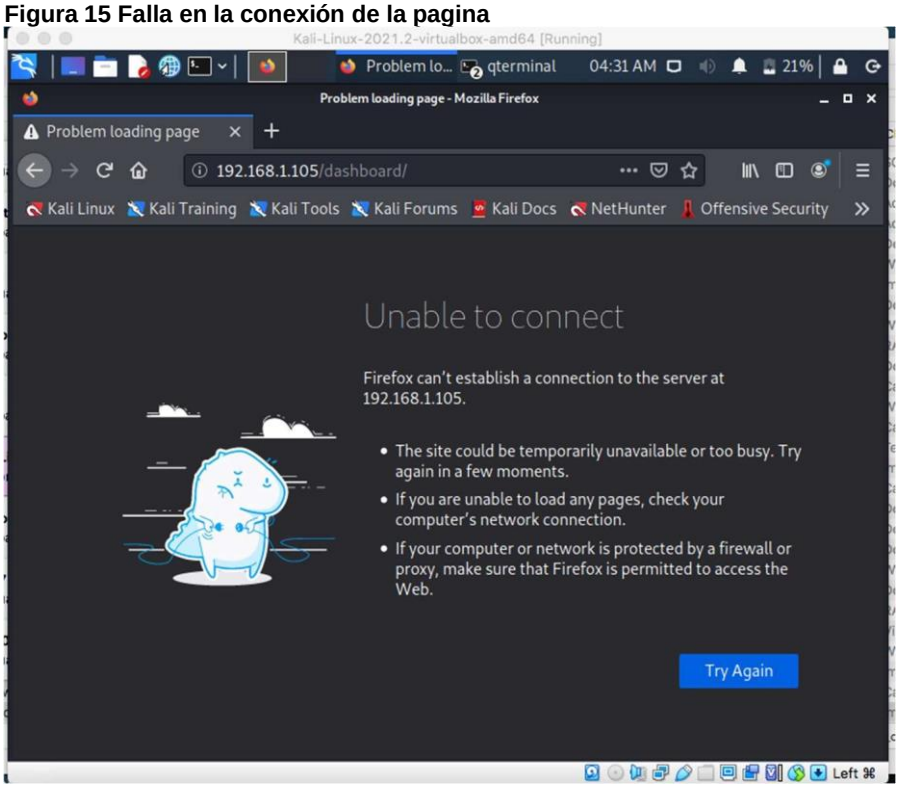
Figura 14 ejecución del comando slowloris



Fuente 14 El autor

Finalmente se evidencia que la conexión con la página esta caída por causa de las múltiples peticiones realizadas a la misma como se aprecia en la figura 15.

Figura 15 Falla en la conexión de la pagina



Fuente 15 El autor

- **Ransomware.**

Con la actualización de Windows MS17-010 se puede eliminar la vulnerabilidad que se identificó en marzo del año 2017 el cual permite la ejecución forma remota de códigos a los servidores de Microsoft, gracias a esta vulnerabilidad es como se difundió el llamado ransomware con WannaCry.[56]

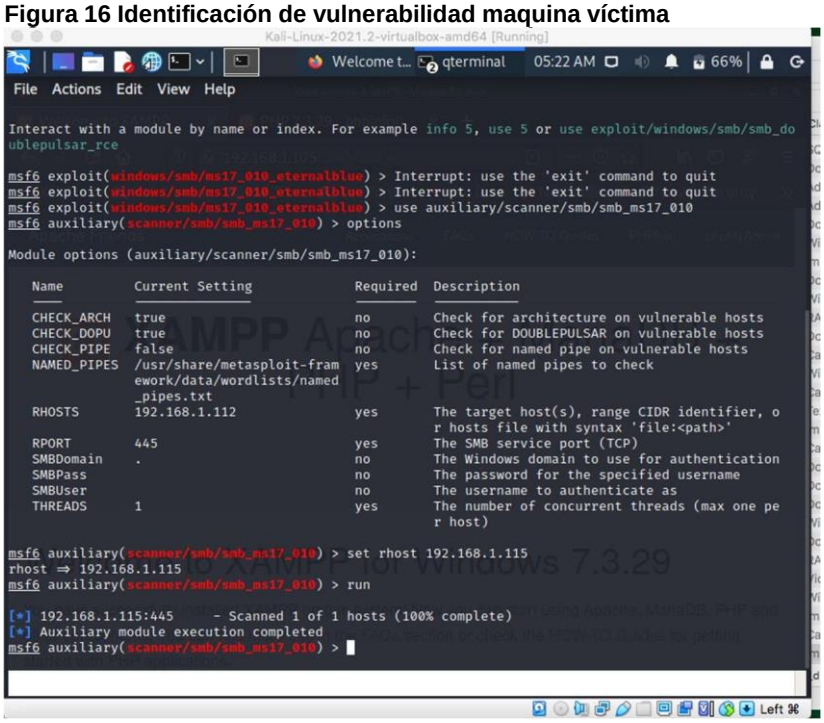
Al realizar la explotación de MS17010, que también es conocido como eternalblue permite el acceso al sistema por medio de la ejecución de código (RCE), esta vulnerabilidad permite al atacante explotar la vulnerabilidad mediante el módulo Windows/smb/ms17_010_eternablue de Metasploit77.

Para la realización de este escenario se hará uso de la herramienta te meterpreter con los siguientes comandos, donde se evidencia que la maquina presenta la vulnerabilidad mencionada anteriormente

.

[56] Microsoft [En línea] [Fecha de Consulta: agosto 2021] Disponible en https://support.microsoft.com/es-es/topic/ms17-010-actualizaci%C3%B3n-de-seguridad-para-windows-server-de-smb-14-de-marzo-de-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655

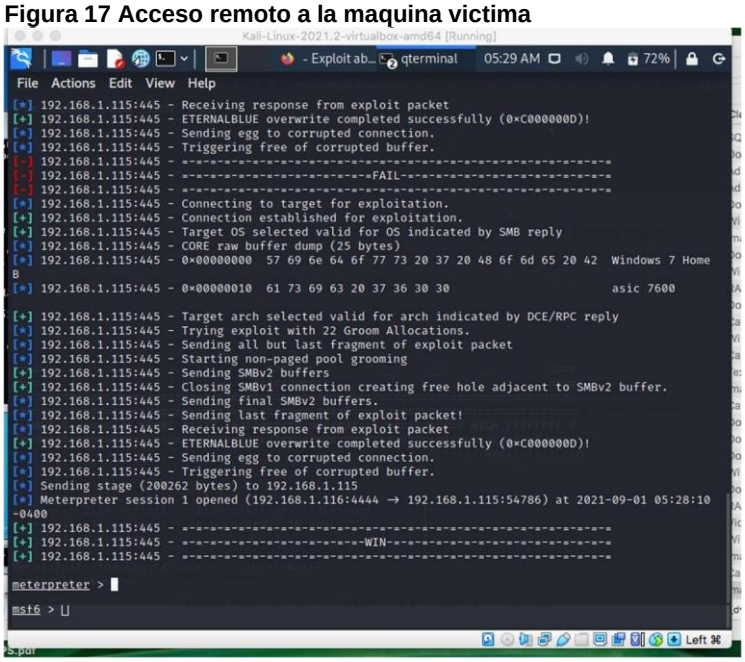
Figura 16 Identificación de vulnerabilidad maquina víctima



Fuente 16 el autor

Al presentarse en la maquina victima la vulnerabilidad, es posible obtener el acceso de forma remota tal como se evidencia a continuación:

Figura 17 Acceso remoto a la maquina victima



Fuente 17 El autor

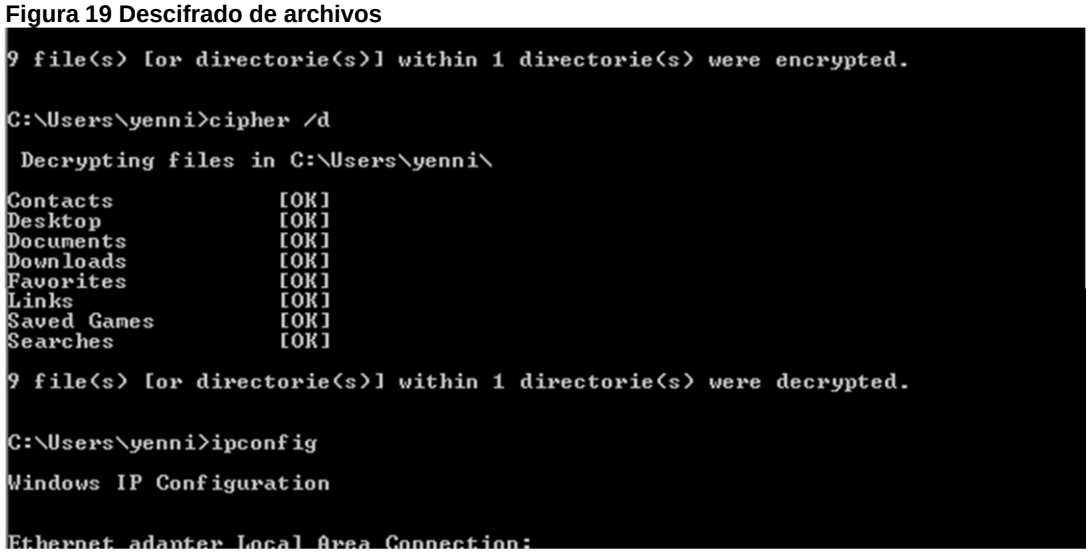
Una vez obtenido el acceso se procede a realizar el cifrado de los archivos por medio del comando cipher /e como se aprecia en la figura 18.

Figura 18 Cifrado de los archivos

Fuente 18 El autor

Igualmente es posible realizar el descifrado de los archivos por medio del comando cipher /d como se evidencia a continuación.

Figura 19 Descifrado de archivos



Fuente 19 El autor

- **Inyección de código SQL**

Para la realización de las pruebas de inyección de código SQL se tiene como base la siguiente base de datos que se encuentra en la ruta (http://104.236.31.57/Test_SQLInj/index.php), la cual pertenece a la empresa NOSTRADAMUS S.A.S y fue víctima de un ataque de inyección de código SQL, por su configuración insegura lo que permitió al ciberdelincuente obtener acceso a las tablas de la base de datos robando información confidencial de la empresa.

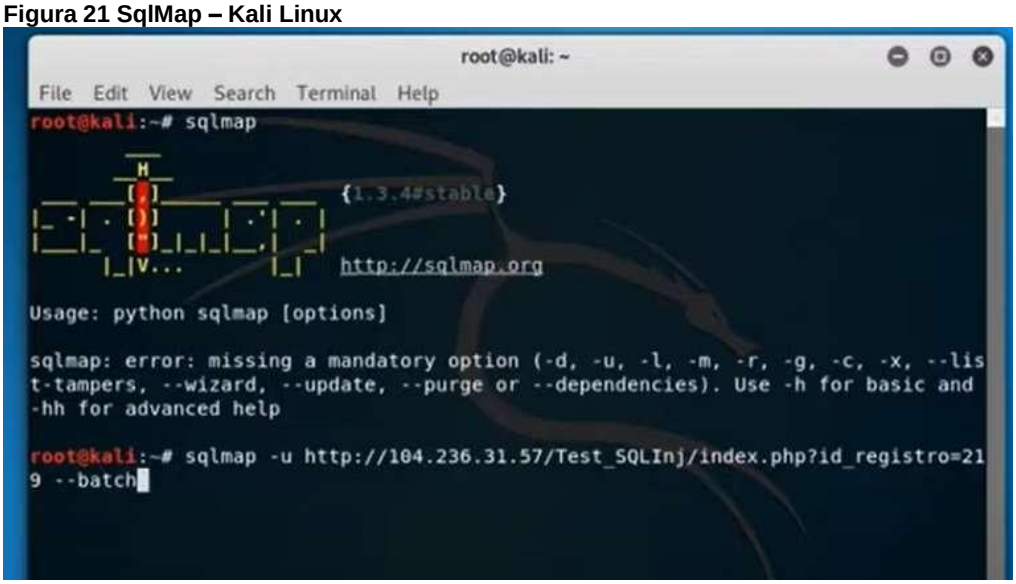
Figura 20 Aplicativo Web vulnerable

Fuente 20 El autor

Para la realización de este escenario se hará uso de la herramienta de SQLMap [57] que permite realizar la prueba de penetración para detectar y ejecutar códigos de SQL inyección, para identificar información como el motor de base de datos, usuarios y contraseñas.

[57] Creadpag [En línea] mayo 2018] [Fecha de Consulta: agosto 2021] Disponible en https://www.creadpag.com/2018/05/inyeccion-sql-en-kali-linux-usando.html

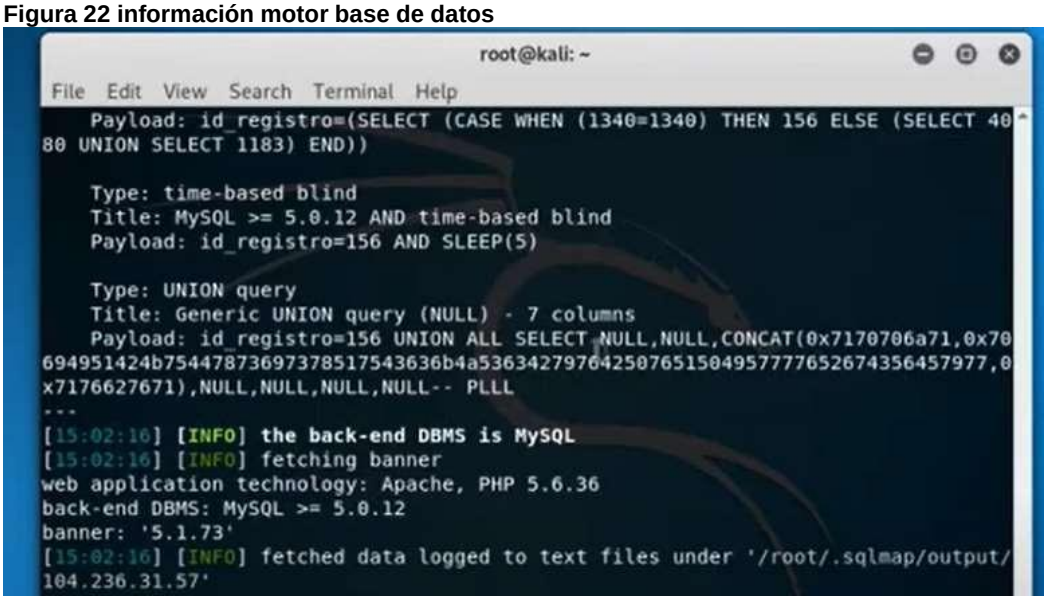
Figura 21 SqlMap – Kali Linux



Fuente 21 El autor

En la siguiente figura se puede identificar que la aplicación está conformada por una base de datos MYSQL 5.0.12 sobre un servidor de aplicaciones apache y lenguaje de programación PHP 5.6.36

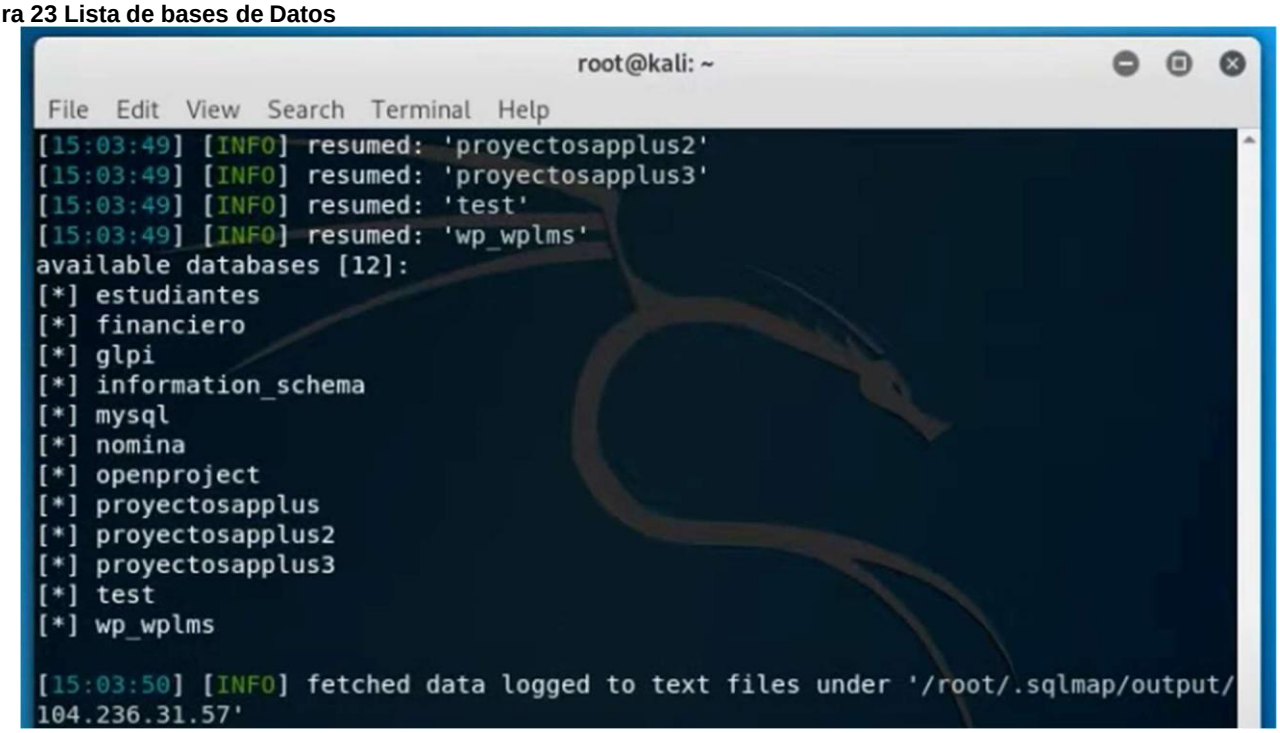
Figura 22 información motor base de datos



Fuente 22 El autor

A continuación, se puede visualizar el listado de las bases de datos creadas en la aplicación web de la empresa NOSTRADAMUS S.A.S

Figura 23 Lista de bases de Datos



Fuente 23 El autor

- **Análisis de resultados**: En esta fase de establecen los falsos positivos, amenazas u observaciones de la empresa.

Una vez finalizada la realización de todos los escenarios de los cuales fue víctima la empresa NOSTRADAMUS S.A.S se puede identificar que las siguientes brechas de seguridad:

Actualizaciones

- Falta de actualización en los navegadores WEB
- Falta de actualización en los sistemas operativos

Configuraciones

- Baja configuración de las reglas de firewall
- Uso inadecuado de los antivirus

- Malas configuración en las bases de datos

Desarrollo de aplicaciones

- No se hace uso de buenas prácticas de desarrollo seguro
- Falta de pruebas de seguridad en aplicaciones Web

7.2 DESARROLLO OBJETIVO ESPECIFICO 2

7.2.1 Matriz de riesgos

Para el caso de estudio de la empresa NOSTRADAMUS S.A.S se hace uso de la metodología MAGERIT que permite conocer el estado en que se encuentran los sistemas de la organización en cuanto a su integridad, disponibilidad, integridad y trazabilidad, con el uso de las guías de esta metodología se pretende establecer los lineamientos de seguridad y reducir en gran medida las vulnerabilidades.

En el caso planteado y de forma de ejemplo se determinan los siguientes activos de información.

Tabla 1 Definición de los activos

ACTIVO	DESCRIPCIÓN	UBICACIÓN	CANTIDAD
SERVIDOR WEB Y BASE DE DATOS:	Equipo de cómputo que permite el alojamiento de la aplicación web y sus respectivas bases de datos	Oficina principal	2
SERVIDOR DE ARCHIVOS:	Equipo de cómputo donde se tiene alojado la administración de los archivos con lo proyecto de educación y capacitación de las plataformas de aprendizaje como lo	Oficina principal	1
PÁGINA WEB	La página web institucional donde se tiene publicados todos los servicios de la empresa, contactos y proyectos de educación, se cuenta con alojamiento con el proveedor	Empresa Godaddy	1

	La infraestructura del servidor es Apache, PHP, MySQL.		
SERVIDOR DE APLICACIONES **SISTEMA OPERATIVO WINDOWS**	Tiene como función la administración de la intranet y demás aplicaciones internas de la organización	Oficina principal	1
SERVIDOR DHCP	Su función es administrar el direccionamiento de la red de forma dinámica dentro de la empresa	Oficina principal	1
EQUIPOS DE CÓMPUTO SISTEMA OPERATIVO WINDOWS 7	Equipos de cómputo	Oficinas internas	3
FIREWALL	Sistema de protección, que protege la red ante intrusiones de la red	Sistema de seguridad que protege la red ante intrusiones de la red	1
PUNTOS DE ACCESO ALÁMBRICOS (HUB)	Dispositivos de red encargados de la interconexión de la red de datos	Red de datos del centro	4
SWITCHES CISCO CATALYST 2960	Dispositivos de red encargados de la interconexión de la red de datos	Red de datos del Centro	6
TÉCNICOS DE MANTENIMIENTO	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de computo	Departamento de Sistemas	2
PUNTOS DE ACCESO	Puntos de acceso al servicio de internet la organización	Oficina de informática	2
CABLEADO	Red cableada para la conexión de los equipos		
BACKUP DE LA INFORMACIÓN	generación de copias de respaldo de la información relevante	Oficina de informática	1
SERVICIO DE CONEXIÓN DE INTERNET	Conectividad a internet		1

Fuente 24 El autor

Identificación de las amenazas

Valoración de las Amenazas

Con el fin de identificar los riesgos más relevantes se evalúan las siguientes vulnerabilidades las cuales pueden materializarse como amenazas definiendo su impacto y probabilidad para cada activo y se tiene en cuenta la siguiente información de valor y probabilidad de ocurrencia.

Tabla 2 Degradación de valor

DEGRADACIÓN DE VALOR	
T	TOTAL
MA	MUY ALTA
A	ALTA
M	MEDIA
B	BAJA
MB	MUY BAJA

Fuente 25 Herramienta PILAR 7.2.3

Tabla 3 Probabilidad de Ocurrencia

PROBABILIDAD DE OCURRENCIA	
CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	SIGLOS
MR	MUY RARA

Fuente 26 Realizado con la herramienta PILAR 7.2.3

Tabla 4 tipos de amenaza

Activos	Amenazas	P	[D]	[I]	[C]	[A]
[files] ficheros de datos	[E,15] Alteración de la Información	M	B	M	A	T
	[E,18] Destrucción de la Información	M	--	B	--	--
	[E,19] Fugas de Información	M	B	--	--	--
	[A,5] Suplantación de identidad	A	--	M	A	T
	[A,6] Abuso de privilegios de acceso	A	B	M	A	--
	[A,11] Acceso no autorizado	MA	--	M	A	--
[backup] copias de respaldo	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	B	--	--	--
	[E,19] Fugas de Información	M	--	--	M	--
	[A,5] Suplantación de identidad	A	--	M	A	T
	[A,6] Abuso de privilegios de acceso	A	B	M	A	--
	[A,11] Acceso no autorizado	MA	--	M	A	--
[int] datos de gestión interna	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	B	--	--	--
	[E,19] Fugas de Información	M	--	--	M	--
	[A,5] Suplantación de identidad	A	--	M	A	T
	[A,6] Abuso de privilegios de acceso	A	B	M	A	--

	[A,11] Acceso no autorizado	MA	--	M	A	--
[password] credenciales	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	B	--	--	--
	[E,19] Fugas de Información	M	--	--	M	--
	[A,5] Suplantación de identidad	A	--	M	A	T
	[A,6] Abuso de privilegios de acceso	A	B	M	A	--
	[A,11] Acceso no autorizado	MA	--	M	A	--
[log] registro de actividad	[E,3] Errores de Monitorización (log)	M	--	B	--	--
	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	B	--	--	--
	[A,3] Manipulación de los registros de actividad (log)	MA	--	A	--	--
	[A,5] Suplantación de identidad	A	--	M	A	T
	[A,6] Abuso de privilegios de acceso	A	B	M	A	--
	[A,11] Acceso no autorizado	MA	--	M	A	--
[multimedia] multimedia	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	B	--	--	--
	[E,19] Fugas de Información	M	--	---	M	--
	[A,5] Suplantación de identidad	A	--	M	A	T
	[A,6] Abuso de privilegios de acceso	A	B	M	A	--

	[A,11] Acceso no autorizado	MA	--	M	A	--
[source]código fuente	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	B	--	--	--
	[E,19] Fugas de Información	M	--	---	M	--
	[A,5] Suplantación de identidad	A	--	M	A	T
	[A,6] Abuso de privilegios de acceso	A	B	M	A	--
	[A,11] Acceso no autorizado	MA	--	M	A	--
[exe] código ejecutable	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	B	--	--	--
	[E,19] Fugas de Información	M	--	---	M	--
	[A,5] Suplantación de identidad	A	--	M	A	T
	[A,6] Abuso de privilegios de acceso	A	B	M	A	--
	[A,11] Acceso no autorizado	MA	--	M	A	--
[www] world wide web	[E,1] Errores de los usuarios	M	M	M	M	--
	[E,2] Errores del administrador del sistema / de la seguridad	M	M	M	M	--
	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	M	--	--	--
	[E,19] Fugas de Información	M	--	--	M	--
	[E,24] Caída del sistema por agotamiento de recursos	A	A	--	--	--

	[A,5] Suplantación de identidad	M	--	A	A	T
	[A,6] Abuso de privilegios de acceso	M	B	M	M	T
	[A,7] Uso no previsto	M	B	M	M	T
	[A,11] Acceso no autorizado	M	--	M	A	T
	[A,13] Repudio (negación de actuaciones)	A	--	--	--	--
	[A,15] Modificación de la Información	A	--	A	--	--
	[A,18] Destrucción de Información	M	A	--	--	--
	[A,24] Denegación de servicio	A	A	--	--	--
[email] correo electrónico	[E,1] Errores de los usuarios	M	M	M	M	--
	[E,2] Errores del administrador del sistema / de la seguridad	M	M	M	M	--
	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	M	--	--	--
	[E,19] Fugas de Información	M	--	--	M	--
	[E,24] Caída del sistema por agotamiento de recursos	A	A	--	--	--
	[A,5] Suplantación de identidad	M	--	A	A	T
	[A,6] Abuso de privilegios de acceso	M	B	M	M	T
	[A,7] Uso no previsto	M	B	M	M	T
	[A,11] Acceso no autorizado	M	--	M	A	T
	[A,13] Repudio (negación de actuaciones)	A	--	--	--	--

	[A,15] Modificación de la Información	A	--	A	--	--
	[A,18] Destrucción de Información	M	A	--	--	--
	[A,24] Denegación de servicio	A	A	--	--	--
[file] almacenamiento de ficheros	[E,1] Errores de los usuarios	M	M	M	M	--
	[E,2] Errores del administrador del sistema / de la seguridad	M	M	M	M	--
	[E,15] Alteración de la Información	M	--	B	--	--
	[E,18] Destrucción de la Información	M	M	--	--	--
	[E,19] Fugas de Información	M	--	--	M	--
	[E,24] Caída del sistema por agotamiento de recursos	A	A	--	--	--
	[A,5] Suplantación de identidad	M	--	A	A	T
	[A,6] Abuso de privilegios de acceso	M	B	M	M	T
	[A,7] Uso no previsto	M	B	M	M	T
	[A,11] Acceso no autorizado	M	--	M	A	T
	[A,13] Repudio (negación de actuaciones)	A	--	--	--	--
	[A,15] Modificación de la Información	A	--	A	--	--
	[A,18] Destrucción de Información	M	A	--	--	--
	[A,24] Denegación de servicio	A	A	--	--	--
[ISP] proveedor de acceso a internet	[I,8] Fallo de servicios de comunicaciones	M	T	--	--	--
	[E,15] Alteración de la información	M	--	M	--	--

	[E,18] Destrucción de la información	M	M	--	--	--
	[E,19] Fugas de Información	M	--	--	M	--
	[A,5] Suplantación de identidad	B	--	T	T	T
	[A,13] Repudio (negación de actuaciones)	M	--	--	--	--
	[A,15] Modificación de la Información	M	--	A	--	--
	[A,18] Destrucción de Información	M	A	--	--	--
	[A,19] Revelación de información	M	--	--	A	--
	[A,24] Denegación de servicio	M	A	--	--	--
[www] alojamiento servidor web	[I,9] Interrupción de otros servicios o suministros esenciales	M	A	--	--	--
	[E,15] Alteración de la información	M	--	M	--	--
	[E,18] Destrucción de la información	M	M	--	--	--
	[E,19] Fugas de Información	M	--	--	M	--
	[A,5] Suplantación de identidad	B	--	T	T	T
	[A,13] Repudio (negación de actuaciones)	M	--	--	--	--
	[A,15] Modificación de la Información	M	--	A	--	--
	[A,18] Destrucción de Información	M	A	--	--	--
	[A,19] Revelación de información	M	--	--	A	--
	[A,24] Denegación de servicio	M	A	--	--	--

[hosting] alojamiento de aplicaciones	[I,9] Interrupción de otros servicios o suministros esenciales	M	A	--	--	--
	[E,15] Alteración de la información	M	--	M	--	--
	[E,18] Destrucción de la información	M	M	--	--	--
	[E,19] Fugas de Información	M	--	--	M	--
	[A,5] Suplantación de identidad	B	--	T	T	T
	[A,13] Repudio (negación de actuaciones)	M	--	--	--	--
	[A,15] Modificación de la Información	M	--	A	--	--
	[A,18] Destrucción de Información	M	A	--	--	--
	[A,19] Revelación de información	M	--	--	A	--
	[A,24] Denegación de servicio	M	A	--	--	--
[prp] desarrollo propio	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[E,8] Difusión de software dañino	M	M	M	M	--
	[E,20] Vulnerabilidades de los programas (Software)	M	B	M	M	--
	[E,21] Errores de mantenimiento / actualización de programas (software)	A	B	B	--	--
	[A,8] Difusión de software dañino	M	T	T	T	--
	[A,22] Manipulación de programas	M	A	T	T	--
[browser] navegador web	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[E,8] Difusión de software dañino	M	M	M	M	--

	[E,20] Vulnerabilidades de los programas (Software)	M	B	M	M	--
	[E,21] Errores de mantenimiento / actualización de programas (software)	A	B	B	--	--
	[A,8] Difusión de software dañino	M	T	T	T	--
	[A,22] Manipulación de programas	M	A	T	T	--
[os] sistemas operativos	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[E,8] Difusión de software dañino	M	M	M	M	--
	[E,20] Vulnerabilidades de los programas (Software)	M	B	M	M	--
	[E,21] Errores de mantenimiento / actualización de programas (software)	A	B	B	--	--
	[A,8] Difusión de software dañino	M	T	T	T	--
	[A,22] Manipulación de programas	M	A	T	T	--
[av] antivirus	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[E,8] Difusión de software dañino	M	M	M	M	--
	[E,20] Vulnerabilidades de los programas (Software)	M	B	M	M	--
	[E,21] Errores de mantenimiento / actualización de programas (software)	A	B	B	--	--
	[A,8] Difusión de software dañino	M	T	T	T	--
	[A,22] Manipulación de programas	M	A	T	T	--
[app] servidor de aplicaciones	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[E,8] Difusión de software dañino	M	M	M	M	--

	[E,20] Vulnerabilidades de los programas (Software)	M	B	M	M	--
	[E,21] Errores de mantenimiento / actualización de programas (software)	A	B	B	--	--
	[A,8] Difusión de software dañino	M	T	T	T	--
	[A,22] Manipulación de programas	M	A	T	T	--
[host] grandes equipos	[N,1] Fuego	B	T	--	--	--
	[N,2] Daños por agua	B	A	--	--	--
	[N, *] Desastres naturales	B	T	--	--	--
	[I,1] Fuego	M	T	--	--	--
	[I,2] Daños por agua	M	A	--	--	--
	[I, *] Desastres industriales	M	T	--	--	--
	[I,3] Contaminación medioambiental	B	A	--	--	--
	[I,4] Contaminación electromagnética	M	M	--	--	--
	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[I,6] Corte del suministro eléctrico	M	T	--	--	--
	[I,7] Condiciones inadecuadas de temperatura o humedad	M	T	--	--	--
	[I,11] Emanaciones electromagnéticas	M	--	--	B	--
	[E,23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	--	--	--
	[E,24] Caída del sistema por agotamiento de recursos	A	A	--	--	--
	[E,25] Pérdida de equipos	B	T	--	T	--
	[A,7] Uso no previsto	M	B	B	M	--
	[A,11] Acceso no autorizado	M	M	M	A	--
	[A,23] Manipulación del hardware	M	A	--	A	--

	[A,24] Denegación del servicio	M	T	--	--	--
	[A,25] Robo de equipos	B	T	--	T	--
	[A,26] Ataque destructivo	M	T	--	--	--
[pc] Informática personal	[N,1] Fuego	B	T	--	--	--
	[N,2] Daños por agua	B	A	--	--	--
	[N, *] Desastres naturales	B	T	--	--	--
	[I,1] Fuego	M	T	--	--	--
	[I,2] Daños por agua	M	A	--	--	--
	[I, *] Desastres industriales	M	T	--	--	--
	[I,3] Contaminación medioambiental	B	A	--	--	--
	[I,4] Contaminación electromagnética	M	M	--	--	--
	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[I,6] Corte del suministro eléctrico	M	T	--	--	--
	[I,7] Condiciones inadecuadas de temperatura o humedad	M	T	--	--	--
	[I,11] Emanaciones electromagnéticas	M	--	--	B	--
	[E,23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	--	--	--
	[E,24] Caída del sistema por agotamiento de recursos	A	A	--	--	--
	[E,25] Pérdida de equipos	B	T	--	T	--
	[A,7] Uso no previsto	M	B	B	M	--
	[A,11] Acceso no autorizado	M	M	M	A	--
	[A,23] Manipulación del hardware	M	A	--	A	--
	[A,24] Denegación del servicio	M	T	--	--	--
	[A,25] Robo de equipos	B	T	--	T	--
	[A,26] Ataque destructivo	M	T	--	--	--

[modem] modem	[N,1] Fuego	B	T	--	--	--
	[N,2] Daños por agua	B	A	--	--	--
	[N, *] Desastres naturales	B	T	--	--	--
	[I,1] Fuego	M	T	--	--	--
	[I,2] Daños por agua	M	A	--	--	--
	[I, *] Desastres industriales	M	T	--	--	--
	[I,3] Contaminación medioambiental	B	A	--	--	--
	[I,4] Contaminación electromagnética	M	M	--	--	--
	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[I,6] Corte del suministro eléctrico	M	T	--	--	--
	[I,7] Condiciones inadecuadas de temperatura o humedad	M	T	--	--	--
	[I,11] Emanaciones electromagnéticas	M	--	--	B	--
	[E,23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	--	--	--
	[E,24] Caída del sistema por agotamiento de recursos	A	A	--	--	--
	[E,25] Pérdida de equipos	B	T	--	T	--
	[A,7] Uso no previsto	M	B	B	M	--
	[A,11] Acceso no autorizado	M	M	M	A	--
	[A,23] Manipulación del hardware	M	A	--	A	--
	[A,24] Denegación del servicio	M	T	--	--	--
	[A,25] Robo de equipos	B	T	--	T	--
	[A,26] Ataque destructivo	M	T	--	--	--
[firewall] cortafuegos	[N,1] Fuego	B	T	--	--	--
	[N,2] Daños por agua	B	A	--	--	--
	[N, *] Desastres naturales	B	T	--	--	--
	[I,1] Fuego	M	T	--	--	--

	[I,2] Daños por agua	M	A	--	--	--
	[I, *] Desastres industriales	M	T	--	--	--
	[I,3] Contaminación medioambiental	B	A	--	--	--
	[I,4] Contaminación electromagnética	M	M	--	--	--
	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[I,6] Corte del suministro eléctrico	M	T	--	--	--
	[I,7] Condiciones inadecuadas de temperatura o humedad	M	T	--	--	--
	[I,11] Emanaciones electromagnéticas	M	--	--	B	--
	[E,23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	--	--	--
	[E,24] Caída del sistema por agotamiento de recursos	A	A	--	--	--
	[E,25] Pérdida de equipos	B	T	--	T	--
	[A,7] Uso no previsto	M	B	B	M	--
	[A,11] Acceso no autorizado	M	M	M	A	--
	[A,23] Manipulación del hardware	M	A	--	A	--
	[A,24] Denegación del servicio	M	T	--	--	--
	[A,25] Robo de equipos	B	T	--	T	--
	[A,26] Ataque destructivo	M	T	--	--	--
[hub] concentrador	[N,1] Fuego	B	T	--	--	--
	[N,2] Daños por agua	B	A	--	--	--
	[N, *] Desastres naturales	B	T	--	--	--
	[I,1] Fuego	M	T	--	--	--
	[I,2] Daños por agua	M	A	--	--	--
	[I, *] Desastres industriales	M	T	--	--	--
	[I,3] Contaminación medioambiental	B	A	--	--	--

	[I,4] Contaminación electromagnética	M	M	--	--	--
	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[I,6] Corte del suministro eléctrico	M	T	--	--	--
	[I,7] Condiciones inadecuadas de temperatura o humedad	M	T	--	--	--
	[I,11] Emanaciones electromagnéticas	M	--	--	B	--
	[E,23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	--	--	--
	[E,24] Caída del sistema por agotamiento de recursos	A	A	--	--	--
	[E,25] Pérdida de equipos	B	T	--	T	--
	[A,7] Uso no previsto	M	B	B	M	--
	[A,11] Acceso no autorizado	M	M	M	A	--
	[A,23] Manipulación del hardware	M	A	--	A	--
	[A,24] Denegación del servicio	M	T	--	--	--
	[A,25] Robo de equipos	B	T	--	T	--
	[A,26] Ataque destructivo	M	T	--	--	--
[wap] punto de acceso Wireless	[N,1] Fuego	B	T	--	--	--
	[N,2] Daños por agua	B	A	--	--	--
	[N, *] Desastres naturales	B	T	--	--	--
	[I,1] Fuego	M	T	--	--	--
	[I,2] Daños por agua	M	A	--	--	--
	[I, *] Desastres industriales	M	T	--	--	--
	[I,3] Contaminación medioambiental	B	A	--	--	--
	[I,4] Contaminación electromagnética	M	M	--	--	--
	[I,5] Avería de origen físico o lógico	M	A	--	--	--
	[I,6] Corte del suministro eléctrico	M	T	--	--	--

	[I,7] Condiciones inadecuadas de temperatura o humedad	M	T	--	--	--
	[I,11] Emanaciones electromagnéticas	M	--	--	B	--
	[E,23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	--	--	--
	[E,24] Caída del sistema por agotamiento de recursos	A	A	--	--	--
	[E,25] Pérdida de equipos	B	T	--	T	--
	[A,7] Uso no previsto	M	B	B	M	--
	[A,11] Acceso no autorizado	M	M	M	A	--
	[A,23] Manipulación del hardware	M	A	--	A	--
	[A,24] Denegación del servicio	M	T	--	--	--
	[A,25] Robo de equipos	B	T	--	T	--
	[A,26] Ataque destructivo	M	T	--	--	--
	[I,8] Fallo de servicios de comunicaciones	M	A	--	--	--
	[E,2] Errores del administrador del sistema / de la seguridad	M	M	M	M	--
	[E,9] Errores de [re-]encaminamiento	M	--	--	M	--
	[E,10] Errores de secuencia	M	--	M	--	--
	[E,15] Alteración de información	M	--	B	--	--
	[E,19] Fugas de información	M	--	--	M	--
	[E,24] Caída del sistema por agotamiento de recursos	M	A	--	--	--
	[A,5] Suplantación de identidad	M	--	M	A	T
	[A,7] Uso no previsto	M	M	M	M	--
	[A,9] [Re-]encaminamiento de mensajes	M	--	--	M	--

[X25] red de datos	[A,10] Alteración de secuencia	M	--	M		
	[A,11] Acceso no autorizado	M	--	M	A	T
	[A,12] Análisis de tráfico	M	--	--	B	--
	[A,14] Interceptación de información (escucha)	M	--	--	M	--
	[A,15] Modificación de la información	M	--	M	--	--
	[A,18] Destrucción de la información	M	A	--	--	--
	[A,24] Denegación de servicio	A	A	--	--	--
[wifi] Wifi	[I,8] Fallo de servicios de comunicaciones	M	A	--	--	--
	[E,2] Errores del administrador del sistema / de la seguridad	M	M	M	M	--
	[E,9] Errores de [re-]encaminamiento	M	--	--	M	--
	[E,10] Errores de secuencia	M	--	M	--	--
	[E,15] Alteración de información	M	--	B	--	--
	[E,19] Fugas de información	M	--	--	M	--
	[E,24] Caída del sistema por agotamiento de recursos	M	A	--	--	--
	[A,5] Suplantación de identidad	M	--	M	A	T
	[A,7] Uso no previsto	M	M	M	M	--
	[A,9] [Re-]encaminamiento de mensajes	M	--	--	M	--
	[A,10] Alteración de secuencia	M	--	M		
	[A,11] Acceso no autorizado	M	--	M	A	T
	[A,12] Análisis de tráfico	M	--	--	B	--
	[A,14] Interceptación de información (escucha)	M	--	--	M	--
	[A,15] Modificación de la información	M	--	M	--	--
	[A,18] Destrucción de la información	M	A	--	--	--

	[A,24] Denegación de servicio	A	A	--	--	--
[LAN] red local	[I,8] Fallo de servicios de comunicaciones	M	A	--	--	--
	[E,2] Errores del administrador del sistema / de la seguridad	M	M	M	M	--
	[E,9] Errores de [re-]encaminamiento	M	--	--	M	--
	[E,10] Errores de secuencia	M	--	M	--	--
	[E,15] Alteración de información	M	--	B	--	--
	[E,19] Fugas de información	M	--	--	M	--
	[E,24] Caída del sistema por agotamiento de recursos	M	A	--	--	--
	[A,5] Suplantación de identidad	M	--	M	A	T
	[A,7] Uso no previsto	M	M	M	M	--
	[A,9] [Re-]encaminamiento de mensajes	M	--	--	M	--
	[A,10] Alteración de secuencia	M	--	M		
	[A,11] Acceso no autorizado	M	--	M	A	T
	[A,12] Análisis de tráfico	M	--	--	B	--
	[A,14] Interceptación de información (escucha)	M	--	--	M	--
	[A,15] Modificación de la información	M	--	M	--	--
	[A,18] Destrucción de la información	M	A	--	--	--
	[A,24] Denegación de servicio	A	A	--	--	--
Discos Extraíbles	[N,1] Fuego	PP	T	--	--	--
	[I,2] Daños por agua	P	A	--	--	--
	[I,3] Contaminación medioambiental	P	A	--	--	--
	[I,5] Avería de origen físico o lógico	P	A	--	--	--

	[I,7] Condiciones inadecuadas de temperatura o humedad	P	T	--	--	--
	[A,23] Manipulación del hardware	PP	A	--	A	--
	[A,25] Robo de equipos	P	M	--	T	--
	[A,26] Ataque destructivo	P	M	--	--	--
Información Impresa	[N,1] Fuego	PP	T	--	--	--
	[I,2] Daños por agua	P	A	--	--	--
	[I,3] Contaminación medioambiental	P	A	--	--	--
	[I,7] Condiciones inadecuadas de temperatura o humedad	P	T	--	--	--
	[E,15] Alteración de la información	P	--	B	--	--
	[E,18] Destrucción de la información	P	T	--	--	--
	[E,19] Fugas de información	P	--	M	--	--
	[A,11] Acceso no autorizado	P	--	B	A	--
	[A,15] Modificación de la información	MA	--	T	--	--
	[A,18] Destrucción de la información	P	T	--	--	--
	[A,25] Robo de equipos	P	M	--	T	--
	[A,26] Ataque destructivo	P	M	--	--	--
[wire] cable eléctrico	[N,1] Fuego	B	T	--	--	--
	[N,2] Daños por agua	B	A	--	--	--
	[N, *] Desastres naturales	B	T	--	--	--
	[I,1] Fuego	M	T	--	--	--
	[I,2] Daños por agua	M	A	--	--	--
	[I, *] Desastres industriales	M	T	--	--	--
	[I,3] Contaminación medioambiental	B	A	--	--	--
	[I,4] Contaminación electromagnética	M	M	--	--	--
	[I,11] Emanaciones electromagnéticas	M	--	--	B	--

	[E,23] Errores de mantenimiento / actualización de equipos	M	M	--	--	--
	[A,7] Uso no previsto	M	A	B	B	--
	[A,11] Acceso no autorizado	M	--	M	A	--
	[A,23] Manipulación del hardware	M	A	--	A	--
	[A,25] Robo de equipos	M	T	--	0	--
	[A,26] Ataque destructivo	M	T	--	--	--
[UE] usuarios externos	[E,15] Alteración de la información	M	--	M	--	--
	[E,18] Destrucción de la información	M	B	--	--	--
	[E,19] Fugas de información	M	--	--	M	--
	[A,15] Modificación de información	M	--	A	--	--
	[A,19] Revelación de información	M	M	--	--	--
	[A,28] Indisponibilidad del personal	B	M	--	--	--
	[A,29] Extorsión	M	M	M	M	--
	[A,30] Ingeniería social (picaresca)	M	M	M	M	--
[ui] usuarios internos	[E,15] Alteración de la información	M	--	M	--	--
	[E,18] Destrucción de la información	M	B	--	--	--
	[E,19] Fugas de información	M	--	--	M	--
	[A,15] Modificación de información	M	--	A	--	--
	[A,19] Revelación de información	M	M	--	--	--
	[A,28] Indisponibilidad del personal	B	M	--	--	--
	[A,29] Extorsión	M	M	M	M	--
	[A,30] Ingeniería social (picaresca)	M	M	M	M	--
	[E,15] Alteración de la información	M	--	M	--	--
	[E,18] Destrucción de la información	M	B	--	--	--

[op] operadores	[E,19] Fugas de información	M	--	--	M	--
	[E,28] Indisponibilidad del personal	M	M	--	--	--
	[A,15] Modificación de información	M	--	A	--	--
	[A,19] Revelación de información	M	M	--	--	--
	[A,28] Indisponibilidad del personal	B	M	--	--	--
	[A,29] Extorsión	M	M	M	M	--
	[A,30] Ingeniería social (picaresca)	M	M	M	M	--
[adm] administradores de sistemas	[E,15] Alteración de la información	M	--	M	--	--
	[E,18] Destrucción de la información	M	B	--	--	--
	[E,19] Fugas de información	M	--	--	M	--
	[E,28] Indisponibilidad del personal	M	M	--	--	--
	[A,15] Modificación de información	M	--	A	--	--
	[A,19] Revelación de información	M	M	--	--	--
	[A,28] Indisponibilidad del personal	B	M	--	--	--
	[A,29] Extorsión	M	M	M	M	--
	[A,30] Ingeniería social (picaresca)	M	M	M	M	--

Fuente 27 realizado con la herramienta PILAR 7.2.3

Teniendo en cuenta lo anterior se identifican como vulnerabilidades las siguientes:

- El cableado físico de las redes se encuentra sin un óptimo mantenimiento y auditoria.
- En la configuración del firewall no se cuenta con la experiencia de configuración adecuada.

- Los servidores no están alojados en un lugar optimo que cumpla con las condiciones de climatización necesaria
- No se realizan las respectivas actualizaciones de software
- Los usuarios no están debidamente protegidos y es posible la suplantación al no tener los debidos perfilamientos
- No se cuenta con las respectivas validaciones de generación de contraseña seguras en los usuarios de las aplicaciones
- Se permite de las sesiones abiertas donde es de fácil acceso capturar las contraseñas y usuarios
- Deficiencia en los mantenimientos de la estructura de red
- Al no contar con sistemas biométrico de seguridad no se tiene control en la zona de sistemas
- Las redes eléctricas pueden fallar y no se cuenta con sistemas de respaldo
- Se cuenta con antivirus actualizado, pero no se realizan seguimiento de control de actualizaciones o estados
- El firewall no tiene correctamente configuradas las reglas para la denegación de conexión o trasmisión de los datos

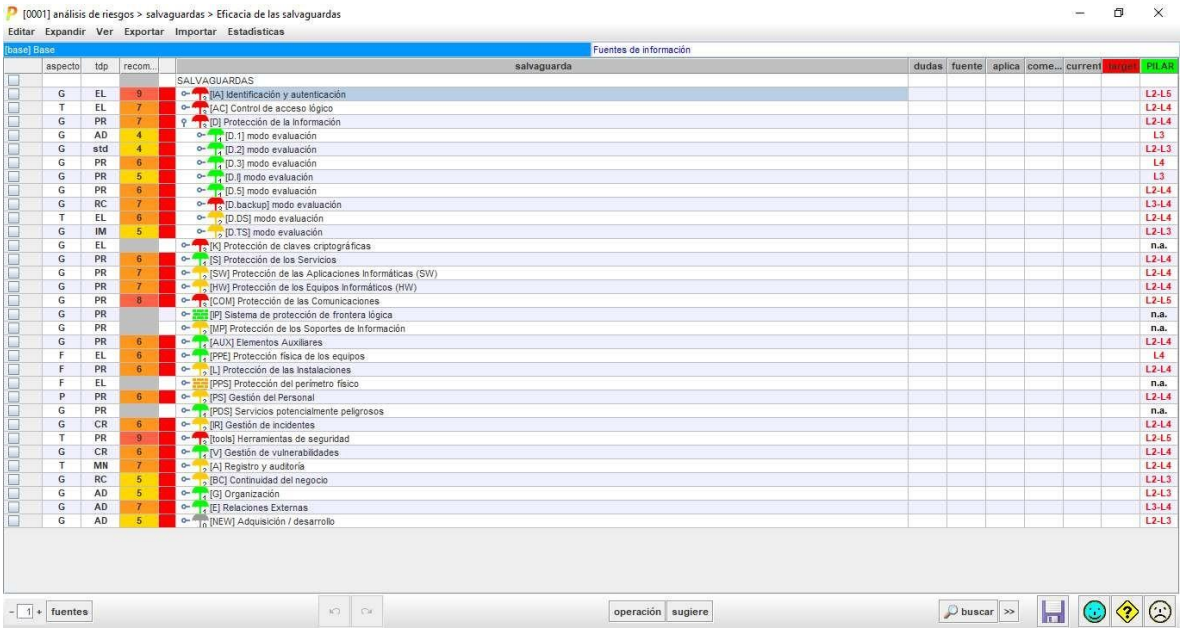
Caracterización de las Salvaguardas

Estos mecanismos o procedimientos permiten que se reduzcan los riesgos ante las amenazas identificadas, comuna correcta organización y otros elementos técnicos, como seguridad física, programas o equipos es posible mitigar este tipo de riesgos.

Identificación de salvaguardas

Se identificarán las salvaguardas más convenientes que permitirán proteger el sistema y para ellos se contará con la ayuda de la herramienta PILAR 7.2.3, la cual permitirá elegir las salvaguardas más adecuados para contrarrestar las amenazas encontradas.

Figura 24 Identificación de las salvaguardas



Fuente 28 Herramienta PILAR 7.2.3

[IA] Identificación y autenticación

- Las salvaguardas seleccionadas son las siguientes:
- [IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido).
- [IA.4.2] Alta, activación, modificación y baja de las cuentas de usuario.
- [IA.4.2.5.1] Las cuentas que ya no son necesarias se eliminan o se bloquean.
- [IA. 4.a] Las cuentas se suspenden al ser comprometidas o existir sospecha de ello.
- [IA.5.2] Hay cuentas específicas para administradores de seguridad.

Son aplicables a la siguiente clase de activos:

[S] Servicios: Correo corporativo, navegación a Internet.

[SW] Aplicaciones: Desarrollos propios, Sistemas Operativos.

[P] Personal: Usuarios internos, usuarios externos, operadores y administradores del sistema.

[AC] Control de acceso lógico

Aplicables a las siguientes clases de activos:

[S] Servicios: Correo corporativo, navegación a internet

[D] Datos / Información: Ficheros de datos, copias de respaldo, datos de gestión interna, gestión de contraseñas, registro de actividad (log), audios generados en reuniones, asambleas y otro tipo de encuentros, código fuente y código de ejecutables de todos los desarrollos propios.

[SW] Aplicaciones: Desarrollos propios, Servidores de aplicaciones, como Internet Information Services IIS.

[P] Personal: Usuarios internos, usuarios externos, operadores y administradores del sistema.

[D] Protección de la Información

Aplicables a las siguientes clases de activos:

[D] Datos / Información: Ficheros de datos, copias de respaldo, datos de gestión interna, gestión de contraseñas, registro de actividad (log), audios generados en reuniones, asambleas y otro tipo de encuentros, código fuente y código de ejecutables de todos los desarrollos propios.

[S] Protección de los Servicios

Aplicables a las siguientes clases de activos:

[S] Servicios: Correo corporativo, navegación a Internet

[3rd] Servicios Contratados a Terceros: G-Suite Empresarial Google apps, Proveedores de internet, Goodaddy.com.

[SW] Protección de las Aplicaciones Informáticas (SW)

Aplicables a las siguientes clases de activos:

[SW] Aplicaciones: Desarrollos propios, navegadores, Sistemas Operativos.

[IR] Gestión de incidentes

Es Aplicable para todos los activos.

[tools] Herramientas de seguridad

Es aplicable para todos los activos.

[V] Gestión de vulnerabilidades

Aplicables a las siguientes clases de activos:

[S] Servicios: Correo corporativo, navegación a internet

[SW] Aplicaciones: Desarrollos propios, Sistemas Operativos, y antivirus.

[A] Registro y auditoría

Es aplicable para todos los activos.

[BC] Continuidad del negocio

Es aplicable para todos los activos.

[G] Organización

Es aplicable para todos los activos.

[E] Relaciones Externas

Es aplicable para todos los activos.

[NEW] Adquisición / desarrollo

Es aplicable para todos los activos.

Sistema de Control de Interno Informático

Tabla 5 Anexo a ISO 27002

Dominio	Objetivo	Control	Implantado si y/o No
05. Política de Seguridad	5.1. Política de seguridad de la información	5.1.1. Documento de política de seguridad de la información	No
		5.1.2. Revisión de la política de seguridad de la información	No
06. Organización de la Seguridad de Información	6.1. Estructura para la seguridad de la información	6.1.1. Comité de gestión de seguridad de la información	No
		6.1.2. Coordinación de seguridad de la información	No
		6.1.3. Asignación de responsabilidades para la seguridad de la información	No
		6.1.4. Proceso de autorización de recursos para el tratamiento de la información	No
		6.1.5. Acuerdos de confidencialidad	No
		6.1.6. Contacto con las autoridades	No
		6.1.7. Contacto con organizaciones de especial interés	No
		6.1.8. Revisión independiente de la seguridad de la información	No
	6.2. Terceros	6.2.1. Identificación de los riesgos derivados del acceso de terceros	No
		6.2.2. Tratamiento de la seguridad en la relación con los clientes	No
		6.2.3. Tratamiento de la seguridad en contratos con terceros	No
07. Gestión de Activos	7.1. Responsabilidad sobre los activos.	7.1.1. Inventario de activos.	No
		7.1.2. Responsable de los activos.	No
		7.1.3. Acuerdos sobre el uso aceptable de los activos.	No
	7.2. Clasificación de la información	7.2.1. Directrices de clasificación.	No
		7.2.2. Marcado y tratamiento de la información.	No
08. Seguridad ligada a los Recursos Humanos	8.1. Seguridad en la definición del trabajo y los recursos.	8.1.1. Inclusión de la seguridad en las responsabilidades laborales.	No
		8.1.2. Selección y política de personal.	No

		8.1.3. Términos y condiciones de la relación laboral.	No
	8.2. Seguridad en el desempeño de las funciones del empleo.	8.2.1. Supervisión de las obligaciones.	No
		8.2.2. Formación y capacitación en seguridad de la información.	No
		8.2.3. Procedimiento disciplinario.	No
	8.3. Finalización o cambio del puesto de trabajo.	8.3.1. Cese de responsabilidades.	No
		8.3.2. Restitución de activos.	No
		8.3.3. Cancelación de permisos de acceso.	No
09. Seguridad Física y del Entorno	9.1. Áreas seguras.	9.1.1. Perímetro de seguridad física.	Si
		9.1.2. Controles físicos de entrada.	No
		9.1.3. Seguridad de oficinas, despachos y recursos.	No
		9.1.4. Protección contra amenazas externas y del entorno.	No
		9.1.5. El trabajo en áreas seguras.	No
		9.1.6. Áreas aisladas de carga y descarga.	No
	9.2. Seguridad de los equipos.	9.2.1. Instalación y protección de equipos.	No
		9.2.2. Suministro eléctrico.	Si
		9.2.3. Seguridad del cableado.	Si
		9.2.4. Mantenimiento de equipos.	No
		9.2.5. Seguridad de equipos fuera de los locales de la Organización.	No
		9.2.6. Seguridad en la reutilización o eliminación de equipos.	No
		9.2.7. Traslado de activos.	No
10. Gestión de Comunicaciones y Operaciones	10.1. Procedimientos y responsabilidades de operación.	10.1.1. Documentación de procedimientos operativos.	No
		10.1.2. Control de cambios operacionales.	No
		10.1.3. Segregación de tareas.	No
		10.1.4. Separación de los recursos para desarrollo y producción.	No
	10.2. Supervisión de los servicios contratados a terceros.	10.2.1. Prestación de servicios.	No
		10.2.2. Monitorización y revisión de los servicios contratados.	No
		10.2.3. Gestión de los cambios en los servicios contratados.	No

	10.3. Planificación y aceptación del sistema.	10.3.1. Planificación de capacidades.	No
		10.3.2. Aceptación del sistema.	No
	10.4. Protección contra software malicioso y código móvil.	10.4.1. Medidas y controles contra software malicioso.	Si
		10.4.2. Medidas y controles contra código móvil.	Si
	10.5. Gestión interna de soportes y recuperación.	10.5.1. Recuperación de la información.	Si
	10.6. Gestión de redes.	10.6.1. Controles de red.	Si
		10.6.2. Seguridad en los servicios de red.	Si
	10.7. Utilización y seguridad de los soportes de información.	10.7.1. Gestión de soportes extraíbles.	No
		10.7.2. Eliminación de soportes.	No
		10.7.3. Procedimientos de utilización de la información.	No
		10.7.4. Seguridad de la documentación de sistemas.	No
	10.8. Intercambio de información y software.	10.8.1. Políticas y procedimientos de intercambio de información y software.	No
		10.8.2. Acuerdos de intercambio.	No
		10.8.3. Soportes físicos en tránsito.	No
		10.8.4. Mensajería electrónica	No
		10.8.5. Sistemas de información empresariales.	No
	10.9. Servicios de comercio electrónico.	10.9.1. Seguridad en comercio electrónico.	No
		10.9.2. Seguridad en transacciones en línea.	No
		10.9.3. Seguridad en información pública.	No
	10.10. Monitorización	10.10.1. Registro de incidencias.	No
		10.10.2. Seguimiento del uso de los sistemas.	No
		10.10.3. Protección de los registros de incidencias.	No

		10.10.4. Diarios de operación del administrador y operador.	No
		10.10.5. Registro de fallos.	No
		10.10.6. Sincronización de reloj.	No
11. Control de Accesos	11.1. Requisitos de negocio para el control de accesos.	11.1.1. Política de control de accesos.	No
	11.2. Gestión de acceso de usuario.	11.2.1. Registro de usuario.	No
		11.2.2. Gestión de privilegios.	No
		11.2.3. Gestión de contraseñas de usuario.	Si
		11.2.4. Revisión de los derechos de acceso de los usuarios.	No
	11.3. Responsabilidades del usuario.	11.3.1. Uso de contraseña.	Si
		11.3.2. Equipo informático de usuario desatendido.	No
		11.3.3. Políticas para escritorios y monitores sin información.	No
	11.4. Control de acceso en red.	11.4.1. Política de uso de los servicios de red.	No
		11.4.2. Autenticación de usuario para conexiones externas.	No
		11.4.3. Autenticación de nodos de la red.	No
		11.4.4. Protección a puertos de diagnóstico remoto.	No
		11.4.5. Segregación en las redes.	No
		11.4.6. Control de conexión a las redes.	No
		11.4.7. Control de encaminamiento en la red.	No
	11.5. Control de acceso al sistema operativo.	11.5.1. Procedimientos de conexión de terminales.	No
		11.5.2. Identificación y autenticación de usuario.	No
		11.5.3. Sistema de gestión de contraseñas.	No
		11.5.4. Uso de los servicios del sistema.	No

		11.5.5. Desconexión automática de terminales.	No
		11.5.6. Limitación del tiempo de conexión.	No
	11.6. Control de acceso a las aplicaciones.	11.6.1. Restricción de acceso a la información.	No
		11.6.2. Aislamiento de sistemas sensibles.	No
	11.7. Informática móvil y teletrabajo.	11.7.1. Informática móvil.	No
		11.7.2. Teletrabajo.	No
12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	12.1. Requisitos de seguridad de los sistemas.	12.1.1. Análisis y especificación de los requisitos de seguridad.	No
	12.2. Seguridad de las aplicaciones del sistema.	12.2.1. Validación de los datos de entrada.	No
		12.2.2. Control del proceso interno.	No
		12.2.3. Autenticación de mensajes.	No
		12.2.4. Validación de los datos de salida.	No
	12.3. Controles criptográficos.	12.3.1. Política de uso de los controles criptográficos.	No
		12.3.2. Cifrado.	No
	12.4. Seguridad de los ficheros del sistema.	12.4.1. Control del software en explotación.	No
		12.4.2. Protección de los datos de prueba del sistema.	No
		12.4.3. Control de acceso a la librería de programas fuente.	No
	12.5. Seguridad en los procesos de desarrollo y soporte.	12.5.1. Procedimientos de control de cambios.	No
		12.5.2. Revisión técnica de los cambios en el sistema operativo.	No
		12.5.3. Restricciones en los cambios a los paquetes de software.	No
		12.5.4. Canales encubiertos y código Troyano.	No
		12.5.5. Desarrollo externalizado del software.	No
	12.6. Gestión de las	12.6.1. Control de las vulnerabilidades técnicas.	No

	vulnerabilidades técnicas.		
13. Gestión de Incidentes de Seguridad de la Información	13.1. Comunicación de eventos y debilidades en la seguridad de la información.	13.1.1. Comunicación de eventos en seguridad.	No
		13.1.2. Comunicación de debilidades en seguridad.	No
	13.2. Gestión de incidentes y mejoras en la seguridad de la información.	13.2.1. Identificación de responsabilidades y procedimientos.	No
		13.2.2. Evaluación de incidentes en seguridad.	No
		13.2.3. Recogida de pruebas.	Si
14. Gestión de Continuidad del Negocio	14.1. Aspectos de la gestión de continuidad del negocio.	14.1.1. Proceso de la gestión de continuidad del negocio.	No
		14.1.2. Continuidad del negocio y análisis de impactos.	No
		14.1.3. Redacción e implantación de planes de continuidad.	No
		14.1.4. Marco de planificación para la continuidad del negocio.	No
		14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad.	No
15. Conformidad	15.1. Conformidad con los requisitos legales.	15.1.1. Identificación de la legislación aplicable.	No
		15.1.2. Derechos de propiedad intelectual (IPR).	No
		15.1.3. Salvaguarda de los registros de la Organización.	No
		15.1.4. Protección de datos de carácter personal y de la intimidad de las personas.	No
		15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información.	No
		15.1.6. Reglamentación de los controles de cifrados.	No
	15.2. Revisiones de la política de seguridad y de	15.2.1. Conformidad con la política de seguridad.	No
		15.2.2. Comprobación de la conformidad técnica.	No

	la conformidad técnica.		
	15.3. Consideraciones sobre la auditoria de sistemas.	15.3.1. Controles de auditoría de sistemas.	No

Fuente 29 Norma ISO27001 Anexo A

Tabla 6 Tratamiento del Riesgo

Sección	Objetivo	Control	Estado	Justificación
A.5 Política de Seguridad				
A.5.1	Políticas de Seguridad de la información	5.1.1 Documento de política de seguridad de la información	Aplicar	La empresa NOSTRADAMUS SAS debe encargarse de elaborar el un manual con la política de seguridad de la información que sea acorde con los requisitos de la organización, las leyes y normas relevantes.
		5.1.2 Revisión de la política para la seguridad de la información	Aplicar	Esta política de seguridad debe ser revisada periódicamente y establecer los tiempos de revisión y divulgación a los empleados con el objetivo que sea idónea y e pueda adecuar de acuerdo con el crecimiento de la empresa.
A.6 Organización de la seguridad de la Información				
A.6.1	Organización de la Seguridad de la información	6.1.1 Compromiso de la Dirección con la seguridad de la información	Aplicar	La gerencia de la empresa NOSTRADMUS SAS debe respaldar la política adoptada en seguridad de la información, en el que se demuestra el apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades dentro de la Organización.
		6.1.3 Asignación de responsabilidades en seguridad de la información	Aplicar	Se deben definir de forma clara todas las responsabilidades para la seguridad de la información, teniendo en cuenta el manual de procesos y

				procedimientos de la empresa NOSTRADAMUS SAS, o los contratos de cada empleado, donde se mencionan las actividades a realizar y el tiempo de ejecución.
		6.1.5 Acuerdos de confidencialidad	Aplicar	Se debe identificar y realizar una revisión de los acuerdos anexos a los contratos, cuáles son los requisitos de confidencialidad y no divulgación que se deben contemplar de acuerdo y las necesidades de protección de la información en la compañía.
A.7 Gestión de Activos				
A.7.1	Responsabilidad sobre los activos	7.1.1 Inventario de Activos	Aplicar	Elaborar y mantener un inventario de activos de información indicando el propietario o el responsable de proteger los activos, mostrando detalles relevantes como ubicación, serial, modelo, marca, estado, etc., para conocer el estado real de los activos e implementar una estrategia de mitigación de riesgos de seguridad de la información dependiendo el caso.
		7.1.2 Propiedad de los activos	Aplicar	Exigido por UNE/ISO-IEC 27001
		7.1.3 Utilización aceptable de los activos	Aplicar	La empresa NOSTRDAMUS SAS necesita identificar, establecer e implementar las normas que regulan el uso adecuado y permitido de la información y de los activos de la compañía, considerando sanciones o causales de despido por el indebido uso de los recursos de la organización.
A.9 Seguridad Física y del Entorno				
A.9.1	Áreas Seguras	9.1.1 Perímetro de la Seguridad Física	Aplicar	Se debe definir un perímetro de seguridad resguardado por controles de entrada adecuados, que garanticen la protección de los servicios de

				procesamiento de la información contra los accesos no autorizados, daños e interferencias.
		9.1.2 Controles físicos de entrada	Aplicar	Verificación de la entrada y salida de las personas que ingresan a las oficinas de la empresa NOSTRADAMUS SAS, ya bien seaN visitantes, clientes o empleados, generando informes de inspecciones de seguridad física de la organización, asegurándose que el ingreso de las personas a las oficinas y/o lugares sea el permitido y/o autorizado
A.9.2	Seguridad de los Equipos	9.2.1 Emplazamiento y protección de equipos	Aplicar	Deben situarse en lugares seguros y protegidos contra incidentes y accidentes potenciales, lejos de ventanas y la caída de objetos pesados, con el fin de reducir los riesgos y la materialización de las amenazas en el entorno y las oportunidades de acceso no autorizado.
		9.2.2 Servicios de soporte	Aplicado	Se cuenta con servicios de soporte
		9.2.3 Seguridad del cableado	Aplicado	Cumple con los requerimientos establecidos para la seguridad
		9.2.4 Mantenimientos de los equipos	Aplicar	Se debe implementar un cronograma para el mantenimiento de los equipos.
A.10 Gestión de las comunicaciones y Operaciones				
A.10.4	Protección frente a código malicioso y código móvil	10.4.1 Controles contra código malicioso	Aplicado	Se cuenta con el antivirus Windows Defender y los equipos con los últimos patch de actualizaciones.
A.10.5	Copias de Seguridad	10.5.1Respaldo de la información	Aplicado	Es necesario para evitar pérdidas de información vital para la compañía
A.10.6	Gestión de la seguridad de la red	10.6.1 Controles de red	Aplicado	Se tiene implementado procedimientos de seguridad para redes y herramientas de red como un DMZ (Zona Desmilitarizada) y un firewall

				con las respectivas políticas para la seguridad perimetral.

Fuente 30 El autor

7.3 DESARROLLO OBJETIVO ESPECIFICO 3

Como resultado de las pruebas de ethical hacking realizadas anteriormente se establecen las siguientes estrategias que permitirán mitigar de manera significativa los riesgos que pueden llegar a materializarse en el futuro, teniendo en cuenta los incidentes presentados en la empresa NOSTRADAMUS S.A.S

7.3.1 Actualización de los navegadores de internet

Teniendo en cuenta uno de los ataques presentados en la empresa NOSTRADAMUS S.A.S, fue originario por medio de los navegadores de internet en los equipos de sistema operativo Windows 7, se hace necesario que se mantengan actualizados los respectivos navegadores, ya que se identificó que la empresa no cuenta con un adecuado programa de actualizaciones y no es muy frecuente que se realice este tipo de actividades, al tener navegadores de internet desactualizados se es más vulnerable a sufrir algún tipo de ataque, en este caso la empresa fue víctima de un ataque de ingeniería social el cual permitió el acceso a los delincuentes informáticos.

7.3.2 Actualización del sistema operativo

No solo es importante que se realicen las actualizaciones de seguridad en los navegadores, sino que es de suma importancia que se realice las actualizaciones de los sistema operativos en los equipos de cómputo de la empresa Nostradamus s.a.s, para el caso de estudio la organización fue víctima porque sus sistemas no contaban con los parches de seguridad necesarios, lo que permitió a los ciberdelincuentes que ejecutaran un ranmsonware de tipo WannaCry en los equipos con sistema operativo Windows 7 por

presentar una vulnerabilidad MS17-010 [58]en la instalación del acceso remoto, lo que les facilito el acceso a la información y posterior incidente de fuga de información por medio de una elevación de privilegios.

7.3.3 Instalación de antivirus y configuración de Firewall

Como puntos clave para contar con un robustecimiento de la seguridad de la información en cualquier organización es necesario tener instalado un buen antivirus que impida en gran medida cualquier incidente de seguridad, es claro que esta configuración no es 100% infalible ante cualquier eventualidad, pero si dificulta que se afecten los activos, ya sea por un análisis de heurística, vigilancia permanente o CRC, si se mitiga que se proliferen archivos con contenidos maliciosos, igualmente la configuración de las reglas del firewall es vital para establecer los permisos del tráfico de entrada y salida de comunicación.

7.4 DESARROLLO OBJETIVO ESPECIFICO 4

7.4.1 PROPUESTA DE ASEGURAMIENTO

7.4.1.1 IMPLEMENTACIÓN DE UTM

UTM (Unified Threat Management) gestión unificada de amenazas esto se refiere a una solución de seguridad que por lo general ofrece muchas funciones de protección incluyendo antivirus, antispyware, antispam, prevención y detección de intrusos, filtrados de contenidos, entre otras.

[58] Explotando Vulnerabilidad MS17-010 o WannaCry», *Juan Oliva* (blog), [En línea] 1 de junio de 2017, [Consultado] agosto 2021 Disponible en https://jroliva.net/2017/06/01/explotando-vulnerabilidad-wannacry-o-ms17-010/.

El UTM es importante ya que al contener varias funcionalidades de seguridad permite que su administración sea mucho más fácil ya que se encuentra todo en una sola consola, se evita la comunicación con diferentes proveedores.

Uno de los problemas que puede traer el instalar el UTM es que, al ser el único dispositivo, también constituye como el único dispositivo de falla también se puede presentar que la herramienta no posea todas las características que puede tener un dispositivo individual, puede presentar problemas de rendimiento al momento de realizar actualizaciones de todas las aplicaciones, Y que no todas las plataformas soportan todos los tipos de aplicaciones requeridas. Una UTM permite el equilibrio de cargas, protección, actualizaciones, identificar y controlar usuarios en la red, gestionar políticas, controlar amenazas en tiempo real, auditorias y controles de fugas de datos, creación de DMZ, protege contra malware y spyware.

7.5 Funciones UTM

Tabla 7 Funciones del UTM

Función	***Abreviatura***	***Descripción***
Firewall	FW	Permite tener controles y filtros en el flujo del tráfico proveyendo una barrera de protección en la Red interna desde una Red insegura
IPS	IPS	su función es monitorear toda la actividad de la Red observando contenidos maliciosos, realiza hacer firmas estadísticas inspecciona anomalías en protocolos, archivos de descarga, de análisis entre otros, si hay un paquete sospechoso muy alto es

		detectado y ellos pueden identificar reportar y dependiendo la clase de configuración del IPS puede realizar acciones para detener el contenido malicioso
Control de aplicaciones	AppCtrl	políticas de seguridad y recursos de la Red en los servidores, ancho de banda, restringe el control con el tráfico de aplicaciones que pueden pasar a través del UTM usualmente en otras direcciones la aplicación puede intentar reducir ocurrencia de infección en contenidos de ataques maliciosos
Protocolo de hipertexto Proxy antivirus	Http/Proxy/AV	La seguridad en un dispositivo desde Proxy controlando el tráfico HTTP es donde el cliente realiza sus peticiones Get, La funcionalidad de inspección de tipo cliente servidor escanea y realiza un handshake de transferencia de datos
Unified threat management	UTM	Contiene múltiples funciones de rendimiento del mismo modo del expositivo de seguridad zinc las 11 en el cine básicamente incluyen favor y PS a B VPN control filtrado de contenido y prevención de pérdida de datos

Fuente 31. El autor

En el ambiente controlado se selecciona la instalación de modsecurity para configurar las reglas y proteger la aplicación de la empresa SAS modsecurity permite controlar los accesos de la aplicación web y su ventaja principal es que opera sobre las capas de aplicación de modelo OSI, por ello constituye una protección más allá de los dispositivos tradicionales.

Tabla 8 Cuadro comparativo UTM.

Modsecurity	Características
características	Las características de este UTM son las siguientes: • Filtrado de las peticiones: Que permite que aquellas peticiones entrantes sean analizadas antes de que lleguen al servidor o cualquier modelo de nuestro servidor apache • Técnicas anti-evasión: Permite que los Path y los parámetros sean normalizados antes de que se ejecute el análisis esto con el fin de evitar las técnicas que se pueden presentar de evasión • Comprende los protocolos HTTP: Con esta funcionalidad se pueden realizar filtrados específicos y de forma granular • Registros de auditoría: Es posible encontrar el detalle incluso de las peticiones post para análisis posteriores • Filtrado HTTPs: Esta funcionalidad están inmersa en el modelo y permite tener acceso a los datos una vez los datos sean descifrados

Ventajas

- Una de las ventajas que tiene este UTM es que proteger las aplicaciones complejas donde el código fuente pudo ser modificado y que sea difícil securizarlas
- Es Open Source y de acceso libre
- Permítete de una curva de aprendizaje muy rápida
- Es muy eficiente con sus funcionalidades
- Tiene fácil configuración
- Permite evitar un mayor número de ataques con unas pocas líneas de configuración
- Es de tipo portable y puede funcionar en casi todos los sistemas operativos del mercado

Desventajas

- Se han presentado perdidas en el servicio cuando se cae el Proxy, en este caso se modificar el NAT, para que las peticiones de internet se vayan directamente a los servidores y no se pierda en la configuración del servicio
- Balanceo: No permite tener un único punto de fallos por lo general Center al menos dos Proxy para repartir las peticiones
- Falsos positivos: En este caso hay que revisar todas las funcionalidades del servicio web que continué funcionando correctamente en particular en casos de envío de ficheros envío de

		correos formularios hay ocasiones en que dejan de funcionar y se consideran falsos positivos
PFsense	Características	• Estas características es que cuenta con una tabla está en la que se configura en todas las reglas y se ve el estado que están disponibles las configuraciones • Balanceo: Cuenta con equilibrio carga en el servidor para disminuir el trabajo entre varios servidores • NAT: Cuentas con reenvío de puertos • Muestra informes históricos de los servicios utilizados • Realiza monitoreo en tiempo real • Y se pueden instalar paquetes de seguridad monitoreo redes servicios y enrutamiento simplemente con hacer clic en la instalación de paquetes
	Ventajas	• es opensource y tiene licencia FreeBSD • Es práctico porque puede ser usado desde una USB • Tiene funcionalidades como firewall, NAt, balanceo de cargas VPN, servidor dns, servidor DHCP y cuenta con generación de Backus fácil y rápido

Desventajas	• Al ser un desarrollo reciente no tiene buena documentación no se encuentra amplios conocimientos de configuración ni tutoriales • Le mande alta disponibilidad en su configuración • Se encontró un fallo de seguridad con Meltdown y spectre los cuales fueron mitigados a nivel del kernel • Fallos en Xss ese ese Cross site scripting en la interfaz web del sistema operativo en la consola administración los cuales también fueron solucionadas en la versión 2.4.3.

Fuente 32. El autor

Generalmente los resultados van acompañados con las soluciones y recomendaciones que proporciona el analista con respecto a las pruebas de seguridad realizadas estos resultados por lo general contienen un informe del estado actual y de los procesos la cual contiene la siguiente información:

1. Fecha y hora de la prueba
2. Duración de la prueba
3. Nombres de analistas responsables
4. Tipo de prueba
5. Alcance de la prueba
6. Índice (método de enumeración de objetivos)
7. Canal probado
8. Vector de prueba
9. Métrica de superficie de ataque
10. Qué pruebas se han completado, no completado o completado parcialmente, y en qué medida
11. Cualquier problema relacionado con la prueba y la validez de los resultados.

12. Cualquier proceso que influya en las limitaciones de seguridad.
13. Cualquier incógnita o anomalía [59]

7.6 Instalación de Modsecurity

Con el fin de realizar la instalación de UTM se realizará la prueba con un servidor Ubuntu server en el que se realizará la instalación de modsecurity y con esta forma realizar un seguimiento al tráfico de la red.

En esta ventana vemos el comando de instalación de modsecurity que es el UTM seleccionado para esta actividad.

Se realiza la instalación desde Linux con el comando install libapache2-modsecurity

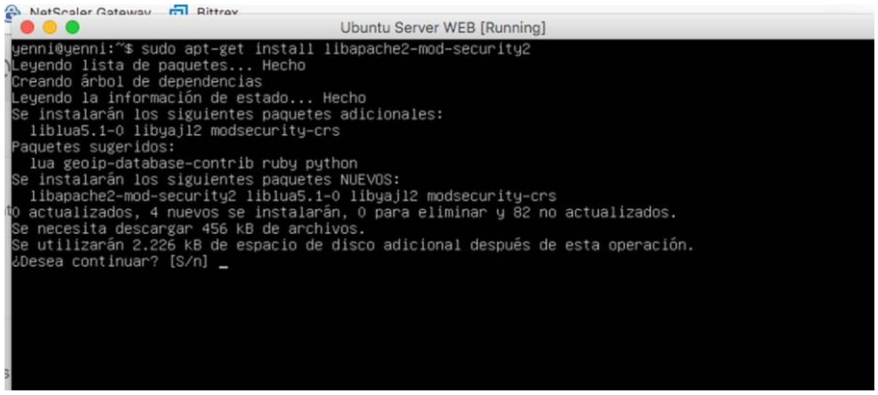
Figura 25 instalación de ModSecurity en ubuntu

Fuente 33 El autor

La acción anterior empezara con la instalación de los paquetes de modsecurity

[59] OSSTMM [En línea]. Marzo 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.isecom.org/OSSTMM.3.pdf pag 50

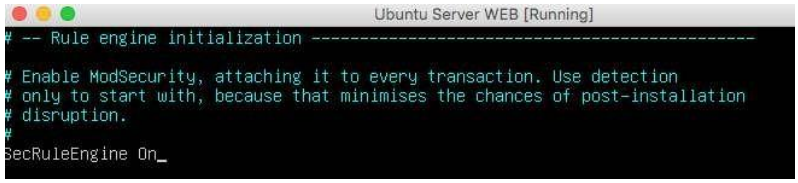
Figura 26 instalación de paquetes



Fuente 34 El autor

Una vez instalado debemos ir a la ruta de configuración del archivo y modificar las siguientes líneas en esta parte lo que se realiza es la configuración de las reglas que se definirán con el finde controlar el tráfico entrante y saliente de la red.

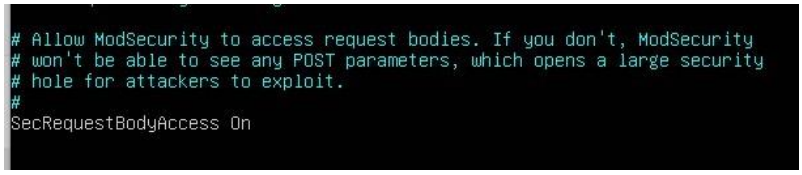
Figura 27 configuración de reglas de Off



Fuente 35 El autor

Se debe cambiar las reglas del estado on al estado off

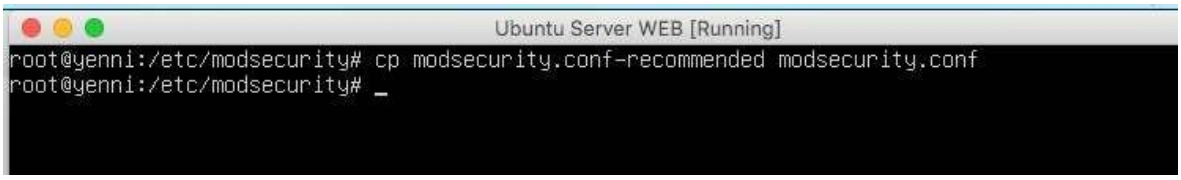
Figura 28 configuración de reglas on



Fuente 36 El autor

Antes de realizar cualquier modificacion es importante copiar el archivo

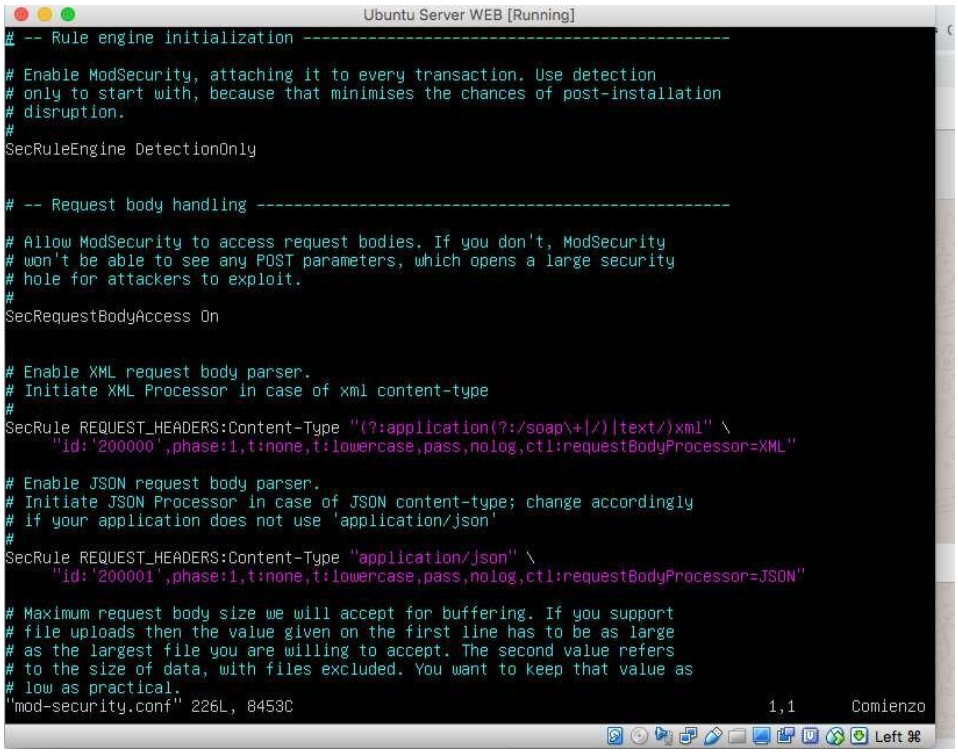
Figura 29 Archivo de configuración modsecurity.conf



Fuente 37 El autor

Para realizar esta modificacion es importante que se realice una copia del archivo de configuracion

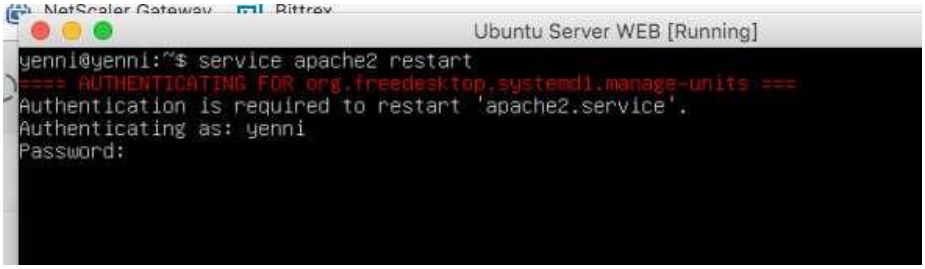
Figura 30 Copia del archivo de configuración



Fuente 38 El autor

Una vez configuradas las reglas se debe reiniciar el servicio de apache

Figura 31 Reinicio servicio apache



Fuente 39 El autor

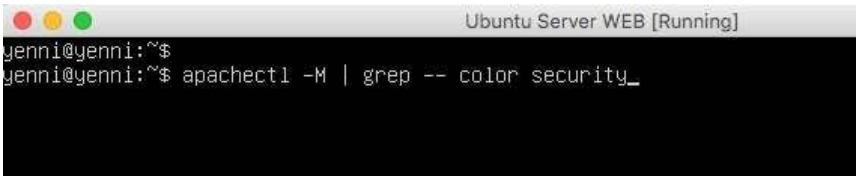
Ingresar las contraseñas para completar

Figura 32 Ingreso de credenciales

Fuente 40 el autor

Para realizar la respectiva configuración de las reglas de modSecurity

Figura 33 configuración de reglas

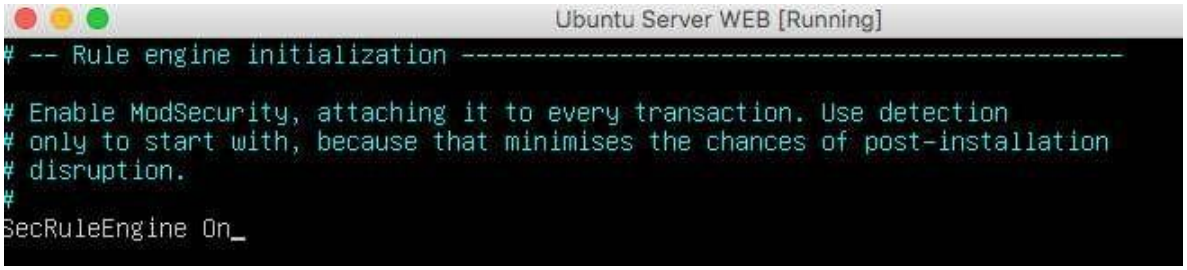


Fuente 41 El autor

Figura 34 Reglas en estado detectivo

Fuente 42 El autor

Figura 35 Estado On de las reglas



Fuente 43 El autor

8 CONCLUSIONES

8. Ejecutar el plan de actividades usando técnicas de hacking ético, para el hallazgo de vulnerabilidades.
9. Presentar un reporte de resultados de vulnerabilidades encontradas, haciendo algunas recomendaciones que minimicen las vulnerabilidades.
10. Realizar el análisis de la propuesta de seguridad para la empresa.
11. Definir los lineamientos de la propuesta de aseguramiento.

- El uso de herramientas de pentesting permiten que se realicen pruebas en ambientes controlados y de esta forma simular los ataques efectuados en la empresa NOSTRADAMUS S.A.S, donde se pudo establecer cuáles fueron las vulnerabilidades presentes en la infraestructura y aplicaciones de la organización y de los servicios que se exponen en internet.

- Al realizar el ethical hacking en la empresa NOSTRADAMUS S.A.S se pudo identificar el vector de entrada del atacante con el fin de mitigar estas vulnerabilidades y tomar medidas de aseguramiento, monitoreo y privilegios en todos los sistemas de la empresa.

- Con la identificación de las vulnerabilidades, riesgos y amenazas de los activos de la organización permite evidenciar los agentes externos e internos que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información de empresa NOSTRADAMUS S.A.S

- Se definen los respectivos controles de seguridad para la empresa NOSTRADAMUS S.A.S con el fin de mitigar las vulnerabilidades presentes y establecer buenas prácticas y parámetros de seguridad que resguardaran los activos de la organización

- De realiza la propuesta de seguridad, que corresponde a la instalación y configuración de MODSecurity con las respectivas especificaciones para ser implementado en la empresa el cual ofrece las funcionalidades de antivirus, prevención y detección de intrusos, filtrado de contenido entre otras.

9 RECOMENDACIONES

Recomendaciones finales para la empresa está el NOSTRADAMUS S.A.S se realizan las siguientes:

- Realizar frecuentemente evaluaciones de seguridad en los activos, con énfasis en el seguimiento de los controles que se hayan establecido de forma interna y externa

- Teniendo en cuenta que cada día aumentan las amenazas y se identifican nuevas vulnerabilidades en necesario que la compañía invierta tiempo y dinero en la implementación de diferentes controles; a razón de lo anterior se hace necesario que se realice la implementación del gestor unificado de amenazas (UTM) modsecurity.

- Es importante que se cree conciencia en los altos directivos y funcionarios de la organización para que constantemente se realicen las actualizaciones de seguridad en los equipos de cómputo y se capaciten en la detención de campañas de ingeniería social para evitar ser víctimas de los ciberdelincuentes.

- Asegurar que los funcionarios adopten medidas de prevención y no ejecuten links o descargar archivos de mensajes sospechosos y mantener la cultura de seguridad.

10 BIBLIOGRAFÍA

Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio [En línea]. Octubre 2010 [Fecha de Consulta: octubre 2020] Disponible en http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

COLOMBIA MINISTERIO DE LAS TECNOLOGIAS Ley 1273 de 2009 mintic, año 2019. Por medio se crea un nuevo bien jurídico tutelado “De la protección de la información y de los datos”

COLOMBIA MINISTERIO DE LAS TECNOLOGÍAS. Ley 1341 de 2009, por la cual se establecen los conceptos y principios de Seguridad de la información.

COLOMBIA MINISTERIO DE LAS TECNOLOGÍAS. Ley 1928 24 julio 2018 Por la cual se aprueba el convenio sobre la Ciberdelincuencia

DINERO [En línea]. Bogotá 2017 [Fecha de Consulta: junio 2019]Disponible en https://www.dinero.com/Item/ArticleAsync/250321?nextId=250338&nextId=250317

DRAGÓNJAR [En línea]. Octubre 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.dragonjar.org/pruebas-de-penetracion.xhtml

ETSINF [En línea]. [Fecha de Consulta: octubre 2020] Disponible en https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1

Elhack.info [En línea]. [Fecha de Consulta: octubre 2020] Disponible en https://ehack.info/las-fases-del-hacking-etico/

ETSINF [En línea]. [Fecha de Consulta: octubre 2020] Disponible en https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1 pág. 74

ETSINF [En línea]. [Fecha de Consulta: octubre 2020] Disponible en https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1 pág. 74

FACTOR CAPITAL HUMANO [En línea]. Julio 2019 [Fecha de Consulta: septiembre 201] Disponible en https://factorcapitalhumano.com/emprendedores/cuanto-debe-presupuestar-una-pyme-para-ciberseguridad/2018/05/

HACKING CERO AÑO 2011 [En línea]. [Fecha de Consulta: octubre 2020] Disponible en http://www.tugurium.com/docs/HakingCero.pdf

HACKING CERO AÑO 2011 [En línea]. [Fecha de Consulta: octubre 2020] Disponible en http://www.tugurium.com/docs/HakingCero.pdf pág. 114

INCIBE [En línea]. [Fecha de Consulta: enero 2020] Disponible en https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

INTRODUCCIÓN a OSSTMM (Open-Source Security Testing Methodology Manual) [En línea]. Noviembre 2015 [Fecha de Consulta: septiembre 2020] Disponible en http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual#:~:text=OSSTMM%20(Open%20Source%20Security%20Testing%20Methodology%20Manual)%20proporciona%20una%20metod

olog%C3%ADa,evita%20suposiciones%20y%20evidencia%20anecd%C3%B3tica.

Latam Kaspersky [En línea] Bogotá 2020 [Fecha de Consulta: septiembre 2020] Disponible en https://latam.kaspersky.com/about/press-releases/2018_la-falta-de-conocimiento-en-seguridad-informatica-pone-en-riesgo-a-las-empresas

LINUXITO. 2019. LINUXITO. [En línea] junio de 2019. https://www.linuxito.com/seguridad/562-como-instalar-y-configurar-modsecurity-en-apache-sobre-servidores-debian.

NIST [En línea]. Octubre 2018 [Fecha de Consulta: octubre 2020] Disponible en https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf pág. 4.1

NIST [En línea]. Octubre 2018 [Fecha de Consulta: octubre 2020] Disponible en https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf pág. 3.1

NIST [En línea]. Octubre 2018 [Fecha de Consulta: octubre 2020] Disponible en https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf pág. 7.1

Revista Cubana de Ciencias Informáticas [En línea]. Octubre 2018 [Fecha de Consulta: octubre 2020] Disponible en http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992018000400005&lng=pt&nrm=iso

Test de Intrusión: Metodologías OSSTMM e ISSAF [En línea]. Marzo 2011 [Fecha de Consulta: octubre 2020] Disponible en https://www.isacavalencia.org/docs/Eventos/2011/201103_25_Carlos.pdf

OSSTMM [En línea]. Marzo 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.isecom.org/OSSTMM.3.pdf

OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad [En línea]. Noviembre 2016 [Fecha de Consulta: septiembre 2020] Disponible en https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

OSSTMM [En línea]. Marzo 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.isecom.org/OSSTMM.3.pdf pág. 37

OSSTMM [En línea]. Marzo 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.isecom.org/OSSTMM.3.pdf pág. 99

OSSTMM [En línea]. Marzo 2010 [Fecha de Consulta: octubre 2020] Disponible en https://www.isecom.org/OSSTMM.3.pdf pág. 50

OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en http https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf

OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 38

OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 85

OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 91

OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 121

OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 185

OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 160

OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 219

OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 240

OWASP [En línea]. 2008 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf pág. 38

OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 276

OWASP [En línea]. Diciembre 2004 [Fecha de Consulta: octubre 2020] Disponible en Owasp https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml pág. 294

PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Pre-engagement

PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Intelligence_Gathering

PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Threat_Modeling

PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Vulnerability_Analysis

PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Exploitation

PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Post_Exploitation

PTES [En línea]. Agosto 2014 [Fecha de Consulta: octubre 2020] Disponible en http://www.pentest-standard.org/index.php/Reporting

WELIVESECURITY [En línea]. Mayo 2014 [Fecha de Consulta: septiembre 2020] Disponible en https://www.welivesecurity.com/la-es/2014/05/21/ebay-confirma-brecha-seguridad-recomienda-cambiar-contrasenas/

3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf pág. 22

3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf pág. 26

3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf pág. 27

3CIENCIAS [En línea]. Octubre 2018 [Fecha de Consulta: septiembre 2020] Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf