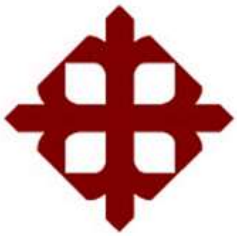


UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL.

TEMA:

Ciberataques en el Ecuador que afectan a las Pymes, y análisis de sus vulnerabilidades con Linux.

AUTOR:

Orozco Crespo, Samir Isaac

Trabajo de Integración Curricular previo a la obtención del título de
INGENIERO EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL

TUTOR:

Ing. Ricardo Xavier Ubilla González, MsC.

Guayaquil, 15 de febrero del 2024

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACION TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERIA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Orozco Crespo, Samir Isaac** como requerimiento para la obtención del título de **Ingeniero en Telecomunicaciones con mención en gestión empresarial**

TUTOR

f. _____

Ing. Ricardo Xavier Ubilla González, MsC.

DIRECTOR DE LA CARRERA

f. _____

MSC. Bohórquez Escobar, Celso Bayardo

Guayaquil, a los 15 días del mes de febrero del año 2024

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACION TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERIA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Orozco Crespo, Samir Isaac**

DECLARO QUE:

El Trabajo de Titulación: **Ciberataques en el Ecuador que afectan a las PYMES, y análisis de sus vulnerabilidades con Linux,** previo a la obtención del título de **Ingeniero en Telecomunicaciones con mención en gestión empresarial**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 15 días del mes de febrero del año 2024

EL AUTOR

Orozco Crespo, Samir Isaac

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACION TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERIA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Orozco Crespo, Samir Isaac**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación: **Ciberataques en el Ecuador que afectan a las PYMES, y análisis de sus vulnerabilidades con Linux**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 15 días del mes de febrero del año 2024

EL AUTOR:

Orozco Crespo, Samir Isaac

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACION TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERIA EN TELECOMUNICACIONES

CERTIFICADO COMPILATIO

La Dirección de las Carreras Telecomunicaciones, Electricidad y Electrónica y Automatización revisó el Trabajo de Integración Curricular, **Ciberataques en el Ecuador que afectan a las pymes, y análisis de sus vulnerabilidades con Linux** presentado por el estudiante **Orozco Crespo Samir Isaac**, de la carrera de **Ingeniería en Telecomunicaciones**, donde obtuvo del programa COMPILATIO, el valor de **2**% de coincidencias, considerando ser aprobada por esta dirección.

Certifican,


INFORME DE ANÁLISIS
magister

2024 tesis Samir Orozco

2% Textos sospechosos

2% Similitudes
< 1% similitudes entre comillas
< 1% entre las fuentes mencionadas
0% Idiomas no reconocidos

Nombre del documento: 2024 tesis Samir Orozco.docx
ID del documento: abd194e5b291241b586292e3cc6ec53d2259955a
Tamaño del documento original: 16,91 MB

Depositante: Ricardo Xavier Ubilla Gonzalez
Fecha de depósito: 6/2/2024
Tipo de carga: interface
fecha de fin de análisis: 6/2/2024

Número de palabras: 25.093
Número de caracteres: 174.038

Ing. Ricardo Xavier Ubilla González, MsC
Tutor

DEDICATORIA

Dedicado a mi Madre Gloria Crespo y a mi Padre Carlos Orozco los cuales me apoyaron durante toda esta trayectoria académica, dándome consejos y apoyo siempre incluso cuando mi ánimo a veces decaía, pero siempre estuvieron presentes para darme ese aliento e impulso de no dejarse doblegar ante las adversidades de la vida.

EL AUTOR

Orozco Crespo, Samir Isaac

AGRADECIMIENTO

Al concluir esta etapa maravillosa de mi vida quiero extender un profundo agradecimiento a Dios todopoderoso por tenerme con vida y permitirme alcanzar este objetivo de vida junto a mis seres queridos. A mi familia por haberme ayudado en todo momento y especialmente a mi madre Gloria Crespo Nieto, y a mi padre Carlos Orozco Sánchez por darme ese amor incondicional y su inquebrantable apoyo a lo largo de este viaje académico, deseo dedicar este espacio para reconocer su papel fundamental en mi vida y en la culminación de esta tesis, por ser mi fuente inagotable de fortaleza, por su sacrificio y por sus valores inculcados que han sido la base de mi éxito y me siento afortunado de tenerlo como modelos a seguir y enseñarme a no rendirme fácilmente aunque se complique cualquier situación en la vida, mientras estemos cerca de Dios y en familia no hay nada imposible, ustedes siempre son mi mayor motivación, gracias por haberme podido dar la oportunidad de haber estudiado en esta prestigiosa Universidad. A mi tutor Ing., Ricardo Xavier Ubilla González por su paciencia y guiarme en el trabajo de investigación; al Ing. Bohórquez Escobar Celso Bayardo que me ha extendido la mano cómo profesor y amigo desde que ingresé a la facultad, ya que es una excelente persona que sabe dar consejos a los alumnos, y con su experiencia dar su punto de vista profesional a la carrera. También a todos mis hermanos que me apoyaron con sus consejos, tiempo y espacio para lograr la realización de mi profesión. ¡Gracias por todo y vamos por más!

EL AUTOR

Orozco Crespo, Samir Isaac

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACION TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERIA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

Ing. Bayardo Bohórquez Escobar, MsC

DIRECTOR DE CARRERA

f. _____

Ing. Ricardo Xavier Ubilla González, MsC

COORDINADOR DEL ÁREA

f. _____

Ing. Heras Sánchez, Miguel Armando M.Sc

OPONENTE

INDICE DE CONTENIDOS

INDICE DE FIGURAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

Este proyecto de investigación tiene como objetivo analizar los ciberataques que afectan a las Pymes del Ecuador y sus vulnerabilidades utilizando Linux y sus herramientas como Nessus, para encontrar fallas en la red y luego poder parchearlas. Se centra en sistemas operativos mal configurados, la relevancia de las actualizaciones, la exposición a diversos ataques externos y el impacto de mantener parches de seguridad y actualizar sistemas e incluso registros para minimizar el riesgo de que los ciberataques no logren explotar los puertos abiertos y obtener control de forma remota para que no puedan escalar privilegios dentro de él. Al mismo tiempo, entender la importancia de no tener activos los servicios del sistema si no se van a utilizar ya que es una compuerta abierta a la fuga de datos. Se enfatiza la formación continua en ciberseguridad para prevenir ataques e identificarlos para no caer en manos de ciberdelincuentes por desconocimiento de los métodos de ataque.

PALABRAS CLAVES: Ciberseguridad, Ataques Informáticos, Ransomware, Phishing, Malware, Puertos, Vulnerabilidades

ABSTRACT

This research project aims to analyze the cyberattacks that affect SMEs in Ecuador and their vulnerabilities using Linux and its tools such as Nessus, to find faults in the network and then be able to patch them. It focuses on misconfigured operating systems, the relevance of updates, exposure to various external attacks, and the impact of maintaining security patches and updating systems and even logs to minimize the risk of cyberattacks failing to exploit open ports and gain control remotely so they can't escalate privileges within it. At the same time, understanding the importance of not having active system services if they are not going to be used since it is an open floodgate for data leaks. Continuous training in cybersecurity is emphasized to prevent attacks and identify them so as not to fall into the hands of cybercriminals for a lack of knowledge of attack methods.

KEY WORDS: Cybersecurity, Computer Attacks, Ransomware, Phishing, Malware, Ports, Vulnerabilities.

CAPÍTULO 1
INTRODUCCIÒN

1.1 Introducción

La tecnología tuvo un importante desarrollo a partir de la pandemia, ya que se tuvieron que incluir el modo de teletrabajo para sectores que no tenían conocimiento de herramientas tecnológicas para su negocio, además careciendo de conocimientos del mundo de la ciberseguridad.

Cuando los usuarios tuvieron que hacer funciones desde un acceso remoto para cumplir parámetros y así poder cumplir con los objetivos planteados, se presentaron entornos que benefician, pero de la misma manera también que perjudican ya que se exponen datos para posibles vulneraciones cuando se trata de ingresar de una manera externa a ella y en la cual hay un intercambio de información para certificar datos para ingresar al sistema.

Todo esto conlleva a que el usuario cotidiano siempre se está enfrentando a riesgos informáticos mientras se tenga un ingreso a internet a través de algún dispositivo y también a sus vulnerabilidades del sistema, robo de información, etc., donde cada uno debería de tener una idea clara sobre la protección de datos y aplicarlos en este mundo tecnológico, a través de varias herramientas.

El atacante, desde fuera de la red, explota las vulnerabilidades en las tecnologías de acceso remoto actuales o intenta descifrar contraseñas para ingresar a la máquina o servidor conectado. Su objetivo es infiltrarse en la red con la intención de robar datos y luego extorsionar. Durante los primeros ocho meses de 2021, los ciberataques experimentaron un aumento significativo, con un asombroso aumento del 78% en comparación con el mismo período del año anterior (Diazgranados, 2021).

1.2 Planteamiento del problema

Los robos de información siempre han estado latentes en el mundo, pero con la evolución de la tecnología también aparecieron nuevos términos

omo la ciberdelincuencia, que prospera con el pasar del tiempo en época de pandemia en la cual aumentó la aparición de piratas informáticos y varios ataques a equipos tecnológicos, usando varias tácticas como lo que es malware, la ingeniería social, phishing, ransomware.

Según el Informe de seguridad 2022 de ESET, casi la mitad de todas las empresas de América Latina experimentaron un incidente de seguridad, mientras que una de cada cuatro organizaciones de la región informó haber sido afectada por malware durante el último año (Harán, 2022).

Una revelación fascinante sobre las amenazas de América Latina es la disminución de los ataques de phishing. A pesar de esto, numerosos países de la región siguen siendo un objetivo importante y se encuentran entre los más atacados a nivel mundial. Al considerar el porcentaje de usuarios que han sufrido intentos de ataque en los primeros ocho meses del año, Brasil ocupa el lugar más alto del ranking con un 15,37% de los usuarios que informaron de este tipo de incidentes. Le siguen de cerca Ecuador con 13,36%, Panamá con 12,60%, Chile con 11,90% y Colombia con 11,09%. En particular, Venezuela (7,19%) y República Dominicana (5,62%) se encuentran entre los países que experimentan menos casos de ataques de ingeniería social a escala global. Las violaciones de datos ocurren como consecuencia del intento de robar credenciales de inicio de sesión, con técnicas que varían según las diferentes industrias. La carencia de ciberseguridad provoca que cualquier usuario y hackers que tenga conocimientos básicos de informática, pueda explotar una vulnerabilidad e ingresar al sistema (Diazgranados, 2021).

1.3 Justificación

Debido al poco conocimiento sobre la ciberseguridad en el sector de las pymes en el país, el incremento de la filtración de datos antes, durante y después de la pandemia deben ser conscientes de fomentar la seguridad de información, para crearse filtros de estabilidad y así evitar fuga de datos informáticos importantes.

De la misma manera con un poco de conocimiento básico del usuario se puede tapar un hueco de muchos que pueden presentar en la

vulnerabilidad de la red, donde el eslabón más débil es el usuario sin conocimiento informático.

Aplicando una serie de herramientas informáticas como el software de Kali Linux podríamos averiguar donde existen fallos de seguridad en el entorno de la pyme que está el usuario y así luego de obtener resultados luego de la auditoria se evitaría que los atacantes de la red puedan encontrar alguna vulneración. Este programa auditor de redes ayudaría a crear un entorno de más confianza al usuario con su información que incrementarían la privacidad de los datos.

1.4 Objetivos del problema de investigación

1.4.1 Objetivo General.

Analizar ciberataques que afectan a pymes del país con Kali Linux.

1.4.2 Objetivos Específicos.

Determinar las vulnerabilidades que utilizan los ciberataques en los sistemas informáticos en pymes.

Plantear puntos importantes para una guía de ciber-higiene para los ataques informáticos.

1.5 Metodología

Para este proyecto de grado se utilizará la investigación descriptiva y documental. El método descriptivo porque se utiliza para describir y analizar de manera detallada un fenómeno, un proceso o una situación. El objeto del método descriptivo es proporcionar una representación precisa y completa de la realidad, sin juzgar ni evaluar los aspectos observados, el proceso, como las encuestas, entrevistas, observación participante, entre otras. Estos datos se analizan y se presentan de manera clara y ordenada, permitiendo obtener conclusiones y aportar información útil para futuras investigaciones o para la toma de decisiones (Sampieri, 2010).

El método de investigación documental implica examinar diversas fuentes escritas, incluidos libros, artículos científicos y archivos, como medio para recopilar información sobre un tema en particular. Este enfoque permite un análisis crítico y reflexivo de los datos recopilados. Para llevar a cabo una investigación documental, es necesario seleccionar cuidadosamente los

documentos que se van a utilizar, teniendo en cuenta su relevancia y confiabilidad. Luego, se deben analizar los documentos de manera crítica y reflexiva, para obtener conclusiones y aportar información útil para futuras investigaciones o para la toma de decisiones (Arias, 2016).

1.6 Hipótesis

Es importante tener en cuenta que Kali Linux es una herramienta de seguridad informática avanzada que puede ser útil para mitigar ataques, pero no es una solución mágica que puede proteger a una pyme de todos los ciberataques. Por lo tanto, es necesario implementar una combinación de medidas de seguridad informática, como firewalls, contraseñas seguras y actualización de software, junto con el uso adecuado de Kali Linux para decrementar la vulnerabilidad de una pyme en un 95%.

Para solucionar este problema, es necesario implementar medidas de seguridad informática adecuadas en pymes y se puede maximizar en gran porcentaje la protección de datos si también el usuario se suma a concientizar sobre lo fundamental de la seguridad de la red.

Otra medida que podría ayudar a reducir el número de ciberataques es la creación de un guía de ciberhigiene de incidentes informáticos, que permita a las pymes detectar y responder rápidamente a cualquier tipo de amenaza informática. En cuanto a la herramienta Kali Linux, esta puede ser útil para mitigar los ciberataques y proteger a las pymes de vulnerabilidades, siempre y cuando se utilice de manera adecuada.

CAPÍTULO 2
FUNDAMENTACIÓN TEÓRICA

2.1 Marco teórico

El desafío que enfrentan los expertos en ciberseguridad es lograr un delicado equilibrio entre los sistemas informáticos, la seguridad de la información, y rendimiento empresarial. Es importante asegurar que las medidas de seguridad implementadas no afecten negativamente las operaciones normales de la empresa, es esencial mantener un equilibrio entre la seguridad y el rendimiento empresarial para garantizar operaciones ininterrumpidas y mitigar los riesgos que plantean las amenazas cibernéticas. La ciberseguridad es esencial para el éxito empresarial. Se busca maximizar la productividad y minimizar los riesgos.

2.2 Definiciones y conceptos fundamentales

2.2.1 Fundamentos de ciberseguridad.

En nuestra sociedad moderna, caracterizada por una amplia digitalización, no se puede subestimar la importancia de la ciberseguridad. Salvaguardar nuestra información y todos los aspectos relacionados con su gestión y transferencia es crucial para establecer un entorno seguro y sólido. Dentro del ámbito de la tecnología de la información, la ciberseguridad tiene suma importancia ya que garantiza la integridad y confiabilidad de las tecnologías digitales.

Según Thakur y Al-Sakib (2020) La ciberseguridad se define como la protección de los sistemas de software, hardware y recursos de datos que se encuentran interconectados y almacenados en Internet. Es una responsabilidad que se extiende desde los individuos hasta las grandes corporaciones, ya que todos desempeñan un papel para garantizar la seguridad de su información.

Se ha vuelto cada vez más frecuente encontrar en medios de comunicación noticias relacionadas con incidentes de seguridad cibernética, como ciberataques, filtraciones de datos y escándalos de privacidad (Elevenpaths, 2021). Estos problemas no solo afectan a grandes empresas o gobiernos importantes, sino también a usuarios finales desprotegidos y

Pymes. Dado que este es un problema creciente y evidente, la pregunta es: ¿existen medios de fortalecer nuestra seguridad cibernética en nuestra vida diaria?; y la simple respuesta para esa pregunta importante es que todo depende de cada persona y las ganas que se ponga en tener una protección adecuada.

Algunos procesos de seguridad que serían utilizados se los muestra en la **Figura 1,** en el cual contempla el uso de forma responsable, como las credenciales de acceso, conexiones y actualizaciones para poder realizar un trabajo debidamente seguro.

Figura 1. Medidas de seguridad

Nota. Adaptado de *Medidas de seguridad.* (Daasel, 2020).

2.2.2 Actualización.

Ignorar las notificaciones de actualización del sistema es un error común entre los usuarios, pero es crucial mantenerlo actualizado para proteger la información y evitar problemas de rendimiento. Además de corregir problemas de seguridad y vulnerabilidades, las actualizaciones también suelen incluir mejoras y características adicionales que mejoran la experiencia del usuario. No debemos subestimar la importancia de mantener el sistema actualizado y considerar la seguridad al utilizar dispositivos y aplicaciones.

Para garantizar el rendimiento óptimo del sistema y salvaguardar información valiosa, se recomienda seguir las instrucciones de actualización, ya que no hacerlo puede exponer a los usuarios a riesgos y pérdida de datos (Alfonso, 2019).

2.2.3 Configuración red wifi.

Por lo general siempre es bueno cambiar el nombre y la contraseña que vienen por defecto, muchas veces estas contraseñas son muy repetitivas en una red y otra en la cual sería sencillo acceder a ellas, es un paso sencillo para dar para la cual nos ahorraríamos un disgusto. Para mejorar la seguridad, es fundamental ocultar el nombre de la red WI-FI y desactivar la conexión Wi-Fi Protected Setup (WPS) por la seguridad que esto lleva (Valero, 2023).

2.2.4 Contraseñas seguras.

Es común usar fechas importantes, nombres de algún familiar o mascota que se tenga en casa, preferencias o gustos personales para poder elegir contraseñas que sean fáciles de recordar, pero de la misma manera son las más fáciles de adivinar. En lugar de esto se recomienda utilizar contraseñas robustas que incluyen una serie de caracteres alfanuméricos, mayúsculas, minúsculas y caracteres especiales. Además, no se debe usar la misma contraseña para todas las cuentas en la que se encuentra registrado, ya que, si es descubierta, es lo primero que intentan probar en el resto de las cuentas por lo mismo es primordial cambiar contraseñas periódicamente para mantener las cuentas más seguras y proteger los datos de posibles ataques informáticos o robos, tal como se muestra en la figura 2 (Incibe, 2019).

Figura 2. Consejos para contraseñas

Nota. Adaptado de *Consejos de contraseñas.* (Osi, 2019)

2.2.5 Utilizar gestor de contraseñas.

Un uso muy común es el de reutilizar las contraseñas una y otra vez continuamente, Lo ideal es precisar con una contraseña para cada aplicación, red social o sistema que se use. Es imposible recordar todas y cada una de las contraseñas con las que se cuenta, por eso existen gestores de contraseñas como por mencionar Lastpass o Keepass. Además, estos gestores tienen una aplicación móvil, así los puedes llevar a cualquier parte que te encuentre (Life, 2019).

2.2.6 Sentido común.

Es fundamental ser precavido y utilizar la lógica al momento de navegar en línea. Si algo suena demasiado bueno para ser verdad, probablemente no lo sea. Es importante investigar y buscar la opinión de expertos antes de tomar cualquier acción. Si se tiene sospecha de algo malicioso, es mejor evitar el riesgo y no caer en un ciberataque. Además, es recomendable mantenerse informado y actualizado sobre las últimas tácticas de los ciberdelincuentes para así no caer en algún posible robo de información (Camara, 2021).

2.2.7 Clasificación de ciberseguridad.

Para proteger una computadora conectada a Internet de ataques cibernéticos, es imperativo contar con medidas de ciberseguridad. Estas medidas son esenciales para proteger los sistemas, hardware, software y datos del acceso no autorizado por parte de ciberdelincuentes. No implementar un plan de seguridad sólido puede poner en peligro la información personal, los datos de los clientes y otra información comercial confidencial. La seguridad cibernética en las empresas es extremadamente peligrosa y puede tener consecuencias negativas para sus empleados y clientes. Es importante tener en cuenta la seguridad cibernética debido a la gran dependencia de los ordenadores y la existencia una amplia gama de amenazas cibernéticas (Rosenthal, 2018).

2.2.8 Seguridad de la infraestructura.

Las sociedades modernas dependen de sistemas ciberfísicos, que son vitales para su funcionamiento. Sin embargo, la infraestructura de red que respalda estos sistemas también los expone al riesgo de sufrir ciberataques. Es imperativo que las organizaciones que supervisan la infraestructura crítica identifiquen y protejan de manera proactiva las vulnerabilidades. La seguridad y la resiliencia de estas infraestructuras cruciales son fundamentales para garantizar la seguridad y el bienestar de la sociedad. Incluso las organizaciones que no son directamente responsables de la infraestructura crítica pero que dependen de ella para sus operaciones deberían desarrollar planes de contingencia para evaluar el impacto potencial de un ataque en la infraestructura de la que dependen (Rosenthal, 2018)

2.2.9 Seguridad de las aplicaciones.

Proteger sus sistemas requiere implementar una variedad de medidas de seguridad cruciales, incluida la seguridad de las aplicaciones. Durante la fase de desarrollo, la seguridad de las aplicaciones utiliza técnicas de software y hardware para combatir las amenazas externas que puedan surgir. Dada la mayor accesibilidad de las aplicaciones a través de las redes, es vital priorizar la integración de medidas de seguridad en las primeras etapas del proyecto. Además, las empresas pueden salvaguardar los activos de datos

confidenciales mediante la implementación de procesos de seguridad de aplicaciones específicos que se adapten a estos conjuntos de datos (Rosenthal, 2018).

2.2.10 Seguridad en la red.

La seguridad de la red juega un papel fundamental en la protección de las redes internas contra intrusiones no autorizadas originadas por intenciones maliciosas, a diferencia de la ciberseguridad, que se enfoca en las amenazas externas. Su objetivo principal consiste en proteger la infraestructura y restringir el acceso a la misma. Al mismo tiempo, los administradores de red se mantienen vigilantes en la implementación de políticas y procedimientos para prevenir el acceso no autorizado, la alteración y la explotación de la red (Peréz, 2020).

2.2.11 Seguridad en la nube.

El aumento de la popularidad de la nube se puede atribuir a su contribución a la mejora de la ciberseguridad. La seguridad en la nube implica una solución basada en software que protege y supervisa los datos almacenados en los recursos de la nube. Con el fin de ayudar a las empresas a proteger sus datos, los proveedores de servicios en la nube están constantemente desarrollando y poniendo en práctica herramientas de seguridad innovadoras (Galindo et al., 2019).

2.2.12 Seguridad del Iot (Internet de las cosas)

Desafortunadamente, muchos dispositivos de IoT se envían inicialmente con vulnerabilidades y carecen de las actualizaciones de seguridad adecuadas. La seguridad sigue siendo un obstáculo importante para la adopción generalizada de la tecnología IoT. Sin embargo, las empresas expresan optimismo con respecto al valor comercial potencial y el crecimiento asociado con IoT, con la expectativa de que aumentarían su compra de dispositivos IoT si las preocupaciones de seguridad se abordaran adecuadamente. La preservación de los datos es de suma importancia en el ámbito de la seguridad informática, ya que regula la forma en que las personas interactúan con los sistemas informáticos cuando encuentran actividades dudosas. Con la proliferación de dispositivos conectados a Internet, que van

desde electrodomésticos hasta automóviles, los ciberdelincuentes tienen ante sí una gran cantidad de posibilidades para desatar el caos. Sin embargo, a medida que los piratas informáticos evolucionan junto con los avances tecnológicos, los profesionales de la ciberseguridad están igualmente comprometidos con la salvaguardia de la información (Rosenthal, 2018).

2.3 Servicios de ciberseguridad más demandados

La mayoría de las empresas no invierten en la suficiente seguridad informática pensando que no son el objetivo de ciberdelincuentes. Sin embargo, uno nunca sabe y es mejor ser precavido para no lamentarse en un futuro alguna infiltración de la empresa independientemente del tamaño o del tipo de negocio que se maneja, ya que actualmente han incrementado los ataques a todo lo que está conectado a la red del internet y que mejor estar un paso adelante con varias funciones de seguridad. Las pymes se enfrentan a un número abrumador de ciberataques diarios que requieren su protección. Varios tipos de ataques, como phishing, DDoS, ransomware y malware, ya no son amenazas distantes, pero se han vuelto cada vez más frecuentes en los últimos años. Es fundamental que las empresas den prioridad a protegerse contra estos ataques potencialmente devastadores. (Toledo, 2019).

Por mencionar algunos:

- Servicio de Pentesting.- (también conocido como prueba de penetración) es un método de evaluación empleado por especialistas en seguridad informática que simula un ataque malévolo a un sistema o aplicación, con el objetivo de descubrir vulnerabilidades o deficiencias. Esta evaluación integral implica el uso de herramientas y técnicas especializadas para medir la resistencia del sistema o la aplicación frente a posibles ataques. El objetivo principal del pentesting es ayudar a las organizaciones a mejorar la seguridad de sus sistemas y salvaguardar sus valiosos datos y recursos digitales.
- Auditoría de Seguridad. - Durante el transcurso de esta auditoría, se examina y supervisa minuciosamente el sistema de la empresa para identificar, compilar y proporcionar descripciones detalladas de cualquier vulnerabilidad que se descubra. Al realizar una

auditoría de seguridad integral, podemos evaluar las áreas de fortaleza, debilidad, amenazas potenciales y riesgos de la empresa en relación con la seguridad de Internet. Tomar medidas para mitigar y erradicar estos problemas es crucial para proteger a la empresa contra posibles ciberataques. Invertir en ciberseguridad es el medio más eficaz de autoprotección (Toledo, 2019).

2.3.1 Seguridad de datos.

La seguridad de los datos es un aspecto esencial para salvaguardar su valiosa infraestructura de TI. Implica implementar un conjunto integral de medidas y protocolos de ciberseguridad para garantizar la protección de su información crítica. Al emplear una variedad de controles, aplicaciones y técnicas, la seguridad de los datos identifica de manera efectiva la importancia de diferentes conjuntos de datos y aplica las medidas de seguridad más adecuadas. Este enfoque proactivo de la seguridad de los datos permite a las organizaciones del sector público y privado evaluar amenazas potenciales y mitigar los riesgos asociados con el almacenamiento y manejo de datos. Al reconocer la importancia de la seguridad de los datos, es imperativo que todas las organizaciones prioricen su implementación.

La principal responsabilidad de las empresas reside en salvaguardar los datos de sus usuarios y clientes, tanto desde el punto de vista jurídico como moral, para evitar accesos no autorizados. Además, existe el riesgo potencial de dañar la reputación debido a una infracción o piratería. Descuidar la importancia de la seguridad de los datos puede provocar un daño irreparable a la reputación. Tendrás que gastar tiempo y dinero evaluando y reparando el daño, además de determinar qué procesos de negocio han fallado y qué necesita mejorarse (Rosenthal, 2018).

Tipos de seguridad de datos:

- Controles de acceso.

Para salvaguardar los sistemas y datos críticos, se implementan varias medidas para mantener la seguridad de los datos. Estas medidas abarcan la restricción del acceso tanto físico como digital. Esto implica hacer cumplir el acceso de entrada

obligatorio para todas las computadoras y dispositivos, así como permitir la entrada a espacios físicos exclusivamente para personas autorizadas.

- Autenticación.

Al igual que los controles de acceso, la autenticación de usuarios se ocupa de verificar con precisión la identidad de las personas antes de otorgarles acceso a los datos. Este proceso comúnmente implica el uso de varios métodos, como contraseñas, números PIN, tokens de seguridad, tarjetas magnéticas o datos biométricos para confirmar la identidad del usuario.

- Copias de recuperación y de seguridad.

Para asegurar la adecuada seguridad de sus datos, es esencial contar con un plan completo que permita el acceso seguro a la información en situaciones de vulnerabilidad, desastres o fallos del sistema. En caso de necesitar recuperar datos, es crucial disponer de copias de seguridad almacenadas en diferentes formatos, como en un disco físico, en la nube o en una red loca.

- Borrado de datos.

Para eliminar adecuadamente los datos se utiliza un software especializado que sobrescriba completamente la información almacenada en cualquier dispositivo, superando la seguridad que ofrecen los métodos estándar de eliminación de datos que simplemente verifican la irrecuperabilidad de los datos.

- Enmascaramiento de datos.

Mediante el uso de software, se emplea una técnica de ocultación en la que se utilizan letras, números y caracteres proxy para ocultar los datos.

Los detalles cruciales, como el acceso no autorizado, quedan efectivamente ocultos mediante este proceso. Los datos se restablecen a su estado original únicamente tras su recepción por parte del usuario autorizado.

- Resistencia de datos.

Garantizar una protección integral de los datos implica la capacidad de sus sistemas para resistir o recuperarse de posibles fallos. Al incorporar resiliencia tanto en su hardware como en su software, puede estar seguro de que la seguridad no se verá comprometida incluso ante cortes de energía o calamidades naturales.

- Cifrado.

El proceso de cifrado implica la utilización de un algoritmo informático para transformar caracteres de texto en una estructura ininteligible mediante el empleo de claves de cifrado. El acceso a la información cifrada y su descifrado está limitado a usuarios autorizados que posean las claves adecuadas. El cifrado se puede implementar en diversas formas de datos, incluidos archivos, bases de datos y comunicaciones por correo electrónico.

2.3.2 Integridad del mensaje.

Se refiere al proceso de garantizar que un mensaje no ha sido alterado de ninguna manera durante su transmisión, a menos que el receptor previamente lo haya verificado y esté al tanto de cualquier cambio que haya sufrido. Esto significa que no hay modificaciones que no sean conocidas por el remitente original (IBM, 2020.)

2.3.3 Autenticación.

Dentro del ámbito de los sistemas informáticos, la autenticación denota la garantía y validación de la identidad de un individuo. Antes de cualquier intento por parte de un usuario de recuperar información alojada dentro de una red, existe un requisito previo para comprobar su identidad y autorización para acceder a los datos. Al establecer una conexión a la red, el usuario debe proporcionar credenciales de inicio de sesión único, como un nombre de usuario y contraseña, como medida de precaución destinada a proteger la red contra una posible infiltración de piratas informáticos.

Para salvaguardar los recursos de la red, es fundamental implementar medidas de autenticación que restrinjan el acceso únicamente a usuarios y dispositivos autorizados (Stallings, 2017).

2.3.4 Control de acceso.

La implementación de medidas de control de acceso se extiende más allá de los sistemas digitales e incluye la restricción de la entrada a campus, edificios, salas y centros de datos. Este componente crucial de la seguridad de la información, la seguridad de los datos y la seguridad de la red sirve para mitigar las amenazas potenciales que plantean las personas no autorizadas que obtienen acceso físico o digital a sistemas sensibles.

Según Stallings (2017) Para salvaguardar los recursos de la red, es fundamental implementar medidas de control de acceso que restrinjan el acceso únicamente a usuarios y dispositivos autorizados.

2.4 Ciberataques

Según Stallings (2017), en los ciberataques se emplean diversas técnicas y herramientas tecnológicas, que son acciones deliberadas destinadas a causar daño, destrucción o manipulación de sistemas y datos informáticos. Estos ataques pueden manifestarse como virus, malware, phishing y otras formas de actividad maliciosa. Los objetivos de estos ataques pueden incluir el robo de datos confidenciales, la interrupción de servicios o la extracción de fondos de un individuo o de una organización. Los ciberataques siguen siendo un peligro constante para las empresas, por lo que es fundamental anticiparse y adoptar medidas proactivas para protegerse contra ellos.

2.4.1 Aplicaciones maliciosas habituales en ciberataques.

El acto de un ciberataque implica un esfuerzo deliberado y perjudicial realizado por un individuo o colectivo para infiltrarse en el sistema de información de otra entidad. Normalmente, el objetivo del atacante es obtener un determinado beneficio mediante la interrupción o manipulación de la red del objetivo (Cisco, 2020).

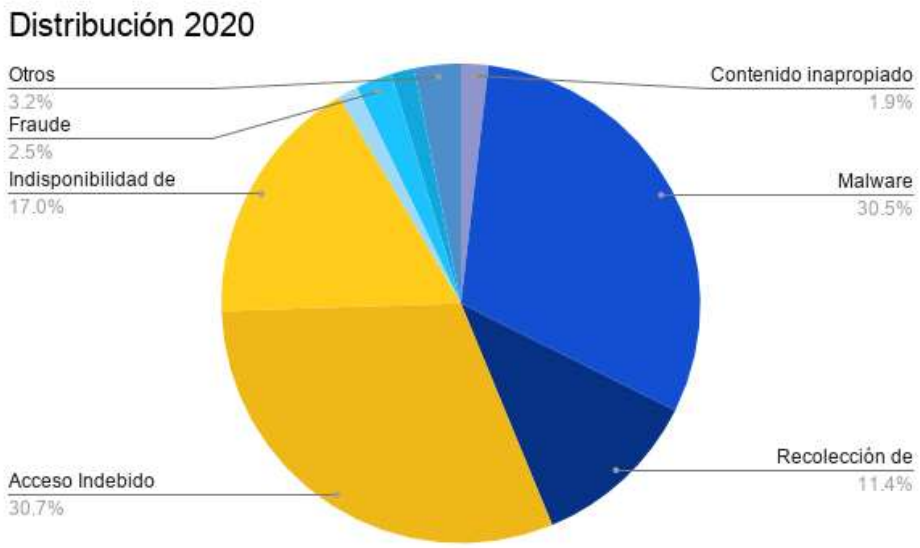
2.4.2 Malware.

El malware, un término amplio que abarca varios programas o códigos diseñados para dañar sistemas y dispositivos, demuestra un comportamiento intrusivo y hostil, con el objetivo de infiltrarse, dañar o incapacitar computadoras, sistemas de TI, redes, tabletas y dispositivos móviles, estableciendo a menudo un control parcial sobre sus operaciones. Este código malévolo opera de manera similar a una enfermedad contagiosa, alterando la funcionalidad normal (Malwarebytes, 2018).

El crecimiento de "Malware" experimentó un aumento constante en porcentaje, mientras que vulnerabilidades como "Acceso inadecuado" y "Recopilación de información" experimentaron una tendencia al alza”.

La figura 3 describe las proporciones relativas de los incidentes de seguridad (Gub, 2020).

Figura 3. Estadísticas de ataques por malware



Nota: Adaptado de las estadísticas sobre incidentes de seguridad informática (Gub, 2020)

2.4.2.1 Siete formas en las que se pueden infectar tus dispositivos con malware. Comprender las estrategias empleadas por los ciberdelincuentes para infiltrar códigos maliciosos en sus dispositivos es fundamental, ya que permite implementar medidas preventivas. En consecuencia, profundizamos en el examen de las técnicas y tácticas predominantes utilizadas por estos individuos nefastos para engañar a los usuarios desprevenidos de Internet para que descarguen software dañino que pone en peligro sus datos y su seguridad general (Owaida, 2021).

- Correos de spam y phishing.

Los correos electrónicos de phishing tienen como objetivo principal adquirir datos confidenciales, y otra información personal, haciéndose pasar por organizaciones acreditadas. Además de esto, estos correos electrónicos pueden contener archivos adjuntos o hipervínculos que pueden exponer su dispositivo a malware. Por lo tanto, es fundamental tener precaución al leer los correos electrónicos, prestando atención a indicadores como errores

tipográficos, demandas urgentes, solicitudes de datos personales y mensajes provenientes de dominios dudosos.

- Sitios web fraudulentos.

Los ciberdelincuentes utilizan el engaño para hacer que las víctimas descarguen aplicaciones maliciosas, creando sitios web fraudulentos que se parecen a los de marcas conocidas o organizaciones legítimas. Normalmente, estos sitios web engañosos poseen un dominio parecido al auténtico, aunque con una ligera variación en una letra o símbolo, y están asociados con malware que tiene como objetivo incitar a la víctima a hacer clic en enlaces que facilitan la descarga de código malicioso en su dispositivo.

- Memorias USB.

Si bien los dispositivos de almacenamiento externo se utilizan ampliamente para el almacenamiento y la transferencia de archivos, es importante ser consciente de los riesgos asociados. Los ciberdelincuentes emplean con frecuencia la estrategia de distribuir memorias USB infectadas con el pretexto de perderlas, engañando a personas desprevenidas para que las conecten a sus ordenadores. Tras la conexión y el acceso, estos dispositivos pueden introducir malware dañino, como registradores de pulsaciones de teclas o ransomware.

Además, si no eres cuidadoso al usar tu memoria USB y la conectas a cualquier equipo desconocido, tu computadora también puede infectarse a través de contaminación cruzada. Es fundamental utilizar una solución de seguridad que permita escanear unidades externas conectadas a sus dispositivos y notificarle rápidamente sobre cualquier contenido potencialmente sospechoso.

- Intercambio de archivos P2P y torrents.

Las redes P2P y los torrents han servido como plataforma tanto para descargas ilícitas de software, juegos y archivos multimedia, como para la difusión de programas de código abierto o

música de artistas. Sin embargo, estas redes también suelen ser explotadas por delincuentes que inyectan código dañino en estos archivos compartidos. En una investigación reciente, los investigadores de ESET descubrieron la utilización del protocolo BitTorrent y la red Tor por parte de ciberdelincuentes para distribuir KryptoCibule, un software malicioso diseñado para robar criptomonedas.

Para mitigar los peligros potenciales de verse comprometido, es recomendable utilizar un servicio VPN confiable para salvaguardar su actividad en línea cifrando sus datos y protegiéndolos del acceso no autorizado. Además, es fundamental mantener un software de seguridad actualizado que ofrezca una protección integral contra diversas amenazas, como el malware que puede residir en los archivos que intenta descargar a través de Torrent.

- Software Comprometido.

Los delincuentes también pueden utilizar los ataques a la cadena de distribución, aunque son poco frecuentes, para comprometer el software legítimo. El caso del software CCleaner sirve como ejemplo, donde los ciberdelincuentes estratégicamente incorporaron malware dentro de la propia aplicación, propagándolo de manera efectiva a usuarios desprevenidos al descargarlo.

Cuando se trata de descargar software, la precaución es clave, independientemente de cuánta confianza tenga en él. Es fundamental combinar esta precaución con el uso de una solución de seguridad confiable, la actualización constante de las aplicaciones y la instalación de los parches de seguridad que las acompañan. Estos parches están diseñados para abordar cualquier vulnerabilidad de seguridad o error encontrado en las aplicaciones afectadas.

- Adware.

Ciertos sitios web bombardean a los usuarios con anuncios que aparecen incesantemente cada vez que hacen clic en cualquier parte de la página web o visitan sitios específicos. Si bien estos anuncios sirven principalmente para generar ingresos para el sitio web, también pueden albergar software malicioso. Al hacer clic sin darse cuenta en estos anuncios o programas publicitarios, los usuarios pueden descargar programas dañinos en sus dispositivos sin saberlo. Algunos anuncios emplean estrategias engañosas, engañando a los usuarios haciéndoles creer que sus dispositivos han sido comprometidos y que la única manera de resolver el problema es comprando la solución de seguridad anunciada. Sin embargo, estas afirmaciones casi siempre son falsas.

Con el fin de evadir el adware, es recomendable emplear un bloqueador de anuncios confiable en su navegador para evitar que los anuncios se manifiesten en el sitio web que está navegando actualmente.

- Falsas aplicaciones.

En esta recopilación de amenazas se incluye el problema de las aplicaciones móviles falsificadas. Estas aplicaciones engañosas se hacen pasar por auténticas y engañan a los usuarios para que las instalen en sus dispositivos con la intención de comprometer su seguridad. Sin embargo, en lugar de ofrecer los servicios anunciados, estas aplicaciones infectan dispositivos con una variedad de software malicioso, incluido ransomware, spyware y registradores de pulsaciones de teclas.

Para proteger sus dispositivos contra el riesgo de descargar aplicaciones dañinas, es aconsejable optar por aplicaciones desarrolladas por creadores acreditados que posean un historial comprobado y hayan recibido comentarios favorables de otros usuarios. Además, asegurarse de que sus dispositivos se actualicen

y parcheen periódicamente proporcionará una capa adicional de defensa contra posibles amenazas que pueden aprovechar las vulnerabilidades encontradas en versiones obsoletas de las aplicaciones (Owaida, 2021).

2.4.3 Virus.

Un virus informático es una forma de software malicioso que tiene como objetivo propagarse y duplicarse pasando de una computadora a otra. Al igual que un virus biológico, depende de un programa o archivo anfitrión para sobrevivir y difundirse. Al adjuntarse a un programa, archivo o documento, el virus tiene el potencial de provocar consecuencias perjudiciales e imprevistas, como deterioro del software del sistema o corrupción de datos.

Hasta que se ejecute el programa infectado, el virus permanecerá inactivo, esperando su momento. Una vez activado, llevará a cabo su programación, propagándose potencialmente a otros ordenadores dentro de la misma red. Sus capacidades incluyen robar contraseñas y datos, registrar pulsaciones de teclas, corromper archivos, enviar correos electrónicos masivos e incluso asumir el control de la máquina comprometida, entre otras acciones maliciosas. Las consecuencias de un virus informático pueden variar desde inconvenientes menores hasta una pérdida catastrófica de datos y funcionalidad del sistema.

El código malicioso, conocido como virus informático, tiene la capacidad de infiltrarse en su computadora al conectarse a archivos preexistentes. Al igual que sus contrapartes biológicas, estos virus emplean tácticas para propagar e infectar diversas ubicaciones. Sin embargo, es importante señalar que el término "virus" a menudo se utiliza incorrectamente para abarcar todo tipo de amenazas. Con el tiempo, esta terminología se está desvaneciendo gradualmente, dando paso al término más preciso "malware", tal como se muestra en la figura 4 (Eset, s/f)

Figura 4. Malware más comunes

Nota. Adaptado de *Tipos de malware comunes*

2.4.4 Gusano informático.

Es un programa de software malévolo tiene la capacidad de autorreplicarse en computadoras y redes, evadiendo la detección. La rápida diseminación de las infecciones se produce debido a la capacidad de cada virus o gusano de reproducirse. Existen multitud de virus y gusanos informáticos, cada uno de ellos capaz de causar daños importantes. Pueden corromper o eliminar datos, robar información o incluso tomar el control de la computadora infectada. Es importante tomar medidas para proteger tu computadora y red de estas amenazas utilizando software antivirus y manteniendo actualizados los sistemas (Kaspersky, 2021).

2.4.5 Adware

acrónimo de "software con publicidad", Este software en particular funciona mostrando anuncios no deseados o dañinos en la computadora o dispositivo del usuario. El adware puede venir en forma de anuncios emergentes, banners o anuncios en el texto y a menudo se incluye con otro software e instalado sin el conocimiento del usuario. El adware también puede rastrear los hábitos de navegación y la información personal de un usuario y compartirla con terceros para la publicidad dirigida.

El adware es considerado una forma de código malicioso y puede causar una serie de problemas para los usuarios, como ralentizar el rendimiento de su computadora, mostrar anuncios no deseados e incluso comprometer su información personal, también puede utilizarse para instalar otros tipos de malware en la computadora de un usuario.

De manera similar, Stallings (2017) menciona que el adware se identifica como un tipo de software malicioso que muestra anuncios intrusivos y tiene la capacidad de monitorear las actividades de navegación de los usuarios.

2.4.6 Spyware

El Spyware es una forma de software malicioso que opera de manera encubierta, recopilando información personal de un usuario sin su conocimiento o permiso. El spyware puede instalarse en una computadora a través de descargas de software, correos electrónicos o sitios web infectados. Tras la instalación del Spyware tiene la capacidad de recopilar datos personales confidenciales, incluidas contraseñas, detalles de tarjetas de crédito e información bancaria, además de monitorear los patrones de navegación y las preferencias del usuario.

De manera similar, Stallings (2017) menciona que el spyware es un tipo de software malicioso que recopila datos personales y monitorea el comportamiento en línea de los usuarios, como se menciona en el texto.

2.4.7 Troyano

El caballo de Troya, o caballo de Troya informático, es una forma de malware que se camufla como un programa válido o inofensivo para infiltrarse en la computadora o dispositivo móvil de un objetivo y ejecutar una variedad de actividades maliciosas (Muñoz, 2021).

2.4.7.1 En un equipo infectado que puede hacer un troyano. Los atacantes emplean troyanos para una multitud de intenciones nefastas, que incluyen, entre otras, establecer puntos de acceso no autorizados, tomar el control del dispositivo de la víctima, robar datos de la computadora comprometida, transmitir dichos datos al atacante y descargar y ejecutar software malicioso complementario en la computadora. sistema de la víctima. Estas acciones, entre otras, ejemplifican la amplia gama de actividades que pueden realizar los troyanos. Los troyanos se distinguen por su gran dependencia de técnicas de ingeniería social, que dependen de la simulación de archivos legítimos y dependen de la ejecución del usuario*.* (Muñoz, 2021)

2.4.7.2 Principales características de los troyanos. Capacidad de contactarse con sus servidores de Comando & Control (C&C).- Estos tienen la capacidad de ampliar su funcionalidad descargando nuevos componentes desde sus servidores de control y mando. Por ejemplo, un Troyano básico puede comenzar con funcionalidad de registro de teclas, pero una vez en la computadora, puede descargar otros componentes que le permiten robar información específica, como credenciales bancarias, contraseñas y documentos. La extensión de estas capacidades adicionales puede depender del interés del atacante en la computadora infectada, pero a menudo es un proceso automatizado. La eficiencia de la distribución de las campañas de phishing determina la cantidad de dispositivos que pueden infectarse, desde cientos hasta miles, razón por la cual los troyanos pueden propagarse con tanta eficacia (Muñoz, 2021)

- **Extensibilidad de sus funciones:** Los Troyanos tienen la capacidad de ampliar su funcionalidad mediante la descarga de nuevos componentes desde sus servidores de control y mando. Por ejemplo, un Troyano básico puede comenzar con la funcionalidad de registro de teclas, pero una vez instalado en la computadora, puede descargar otros componentes que le permiten robar información específica, como credenciales bancarias, contraseñas y documentos. La extensión de estas capacidades adicionales puede depender del interés del atacante en la computadora infectada, pero a menudo es un proceso automatizado. La

razón detrás de esto es que las campañas de phishing que involucran troyanos tienen el potencial de infectar una cantidad significativa de dispositivos, desde cientos hasta incluso miles, dependiendo de la eficiencia con la que se distribuyan. (Muñoz, 2021)

- **Descargar otros programas maliciosos:**

Cuando un ordenador ha sido infiltrado con éxito por un troyano, algunos pueden aprovechar esta oportunidad para descargar otros tipos de malware. Además, algunos actores maliciosos también pueden permitir que otros ciberdelincuentes accedan a los sistemas que han sido comprometidos por un troyano, esencialmente alquilando el sistema comprometido por el troyano como un servicio para otros. (Muñoz, 2021)

- **Actualización**

Según Muñoz (2021) Algunos tienen la función de actualizarse a sí mismos y sus componentes.

2.4.8 Phishing.

El acto de phishing, un ataque cibernético, utiliza tácticas de ingeniería social para adquirir datos confidenciales y monetarios de personas desprevenidas. Normalmente, estos ataques están dirigidos a una audiencia amplia y pueden enviarse a través de correo electrónico, mensajes de texto o WhatsApp. Para engañar a las víctimas, los atacantes suelen emplear logotipos reconocibles y marcas de renombre, dando la ilusión de legitimidad. Los ataques de phishing pueden ser muy complejos e incorporan tácticas de manipulación emocional para crear una sensación de urgencia y obligar a las víctimas a revelar información. Además, los atacantes pueden crear sitios web falsificados para engañar a las personas para que revelen sus credenciales de inicio de sesión (Vázquez et al., 2022).

Para evitar ser víctima de estos ataques, es importante tomar ciertas precauciones, incluido mantener un saludable escepticismo hacia los correos electrónicos o mensajes de remitentes desconocidos, abstenerse de hacer clic en enlaces o descargar archivos de fuentes no confiables y asegurarse de que el software y los sistemas se actualicen periódicamente. para salvaguardar la información personal y financiera (Briceño, 2023).

- Spear Phishing. Es un tipo de ataque altamente preciso e individualizado, se centra en señalar a una persona específica o a un pequeño grupo de personas en lugar de lanzar una amplia red para llegar a una gran audiencia. Los delincuentes investigan y recopilan meticulosamente detalles específicos sobre su objetivo, incluido su nombre, ocupación, intereses y preferencias. Armados con esta información, elaboran mensajes o correos electrónicos que parecen provenir de fuentes confiables. Su objetivo es engañar a la víctima para que divulgue información confidencial o financiera, o instalar subrepticiamente malware en su dispositivo. El Spear phishing supera al tradicional en términos de efectividad, ya que aprovecha la personalización y resulta más difícil de identificar. (García, 2020)
- Vishing.- Esta forma de phishing se desvía del enfoque tradicional de correo electrónico o mensajes de texto al utilizar llamadas telefónicas. El objetivo principal de este método es engañar al objetivo para que divulgue datos confidenciales, incluidos detalles de tarjetas de crédito, contraseñas o información bancaria. Para lograr este objetivo se emplea la manipulación emocional y la creación de un sentido de urgencia o necesidad. En algunos casos, los estafadores pueden utilizar software de falsificación de identidad que hace que el número telefónico mostrado en la llamada sea el mismo que el de una organización legítima, como un banco o una empresa de seguridad informática, para aumentar la confianza de la víctima. (García, 2020)

- Smishing.- Los mensajes de texto se han convertido en una nueva vía para las estafas de phishing, reemplazando a los correos electrónicos tradicionales. Estas estafas se basan en tácticas de manipulación emocional para ganarse la confianza de las víctimas y extraer datos confidenciales, como contraseñas o detalles

financieros. Los atacantes crean mensajes de texto que parecen genuinos, incitando a las personas a hacer clic en enlaces dañinos o divulgar información personal. Para protegerse, es fundamental actuar con cautela y abstenerse de compartir datos confidenciales en respuesta a mensajes de texto no solicitados.

Tipos de smishing incluyen:

1. Phishing por mensaje de texto: Se envía mensajes de texto que parecen ser de un remitente confiable, como una institución financiera o una empresa, para engañar a las personas a proporcionar información confidencial.

2. Smishing de seguridad: El acto de hacerse pasar por una institución de seguridad, como una empresa de seguridad en línea o una entidad gubernamental, para adquirir información confidencial tiene su origen en preocupaciones por la seguridad.

3. Smishing de análisis de datos: Se envía un mensaje de texto que solicita la descarga de una aplicación o software para analizar los datos de un dispositivo, que en realidad es un malware que infecta el dispositivo y roba información.

4. Smishing de donación: Se hace pasar por una organización benéfica o una campaña de caridad para obtener donaciones.

5. Smishing de sorteo: Se hace pasar por una empresa o una organización que ofrece un sorteo o un premio para obtener información confidencial o financiamiento, tal como se muestra en la figura 5 (Rudra, 2022)

Figura 5. Robo de información

Nota. Adaptado de *Qué es el phishing, cómo funciona y cómo protegerte,* (Infospyware, 2021)

2.4.9 Ransomware.

Existe una forma de software malicioso que cifra los archivos que pertenecen a sus víctimas, haciéndolos inaccesibles hasta que se paga un rescate a cambio de la clave de descifrado. Las consecuencias de este tipo de ataques pueden ser catastróficas tanto para las personas como para las empresas, ya que los archivos cifrados suelen contener información confidencial y valiosa. Este tipo de malware se distribuye comúnmente a través de correos electrónicos de phishing o explotando vulnerabilidades en el software, y puede adoptar diferentes disfraces, incluidos enlaces, archivos adjuntos o software maliciosos. Algunos de los ataques de ransomware más notables que se han informado incluyen WannaCry, Petya y Locky. (Proofpoint, 2020).

2.5 Incursión de ataques informáticos en Ecuador.

Entre las naciones latinoamericanas más afectadas por el cibercrimen, Ecuador se ha sumado a las filas de Argentina, Brasil, Colombia, México y Perú. El último Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones revela que Ecuador ocupa la posición 119 entre 182 países en términos de susceptibilidad a ataques cibernéticos. Numerosos ataques cibernéticos importantes han tenido como objetivo a Ecuador, incluido un ataque al Banco Pichincha, el banco privado más grande del país. Para reforzar sus medidas de ciberseguridad, Ecuador ha implementado una política integral de ciberseguridad que involucra activamente a diversas partes interesadas, incluidos el gobierno, las empresas privadas, las instituciones académicas y la sociedad civil. Desde 2017, Ecuador ha establecido un Comité de Ciberseguridad dedicado a proteger contra ataques informáticos (Solano, 2022).

Para las pequeñas y medianas empresas (PYME), el costo de implementar un sistema integral de ciberseguridad para proteger sus bases de datos y la información de sus clientes puede representar una carga financiera significativa. No obstante, no tomar medidas y enfrentar un ciberataque podría tener graves consecuencias, incluyendo la quiebra de la empresa o demandas. La transformación digital y la pandemia han llevado a un aumento en la industria del cibercrimen, que es un negocio multimillonario (Cyberwar, 2022).

El informe anual de Kaspersky muestra un aumento del 75% en los ataques informáticos en Ecuador, con un promedio de 89 ataques por minuto. Los expertos afirman que estos ataques afectan no solo a las grandes empresas y bancos, sino también a las pymes. Entre los cinco tipos de malware más comunes utilizados por los hackers están los virus, troyanos, gusanos, spyware en Ecuador, se registraron más de 51 mil casos de cryptominers, alrededor de 140 mil detecciones de exploits, cerca de seis mil detecciones y casi ocho mil detecciones de spyware. En Ecuador, el ransomware ha demostrado ser la forma más destructiva de software malicioso, causando daños significativos a las empresas públicas y privadas.

Además, en 2020, el país ocupó el sexto lugar en América Latina para detecciones de malware, detrás de Brasil, México, Argentina, Colombia y Perú (Cyberwar, 2022).

2.5.1 Hackers lanzan ofensiva global.

El país sufrió un ataque cibernético masivo, entre el jueves y la mañana del lunes 15 de abril de 2019. Los hackers lanzaron un asombroso 40 millones de ataques a sitios web gubernamentales, con el objetivo de abrumarlos con una cantidad excesiva de datos, una táctica conocida como un ataque de denegación de servicio. A pesar de este ataque, los sitios web lograron resistir el asalto, con solo interrupciones intermitentes en su funcionalidad, según lo confirmado por el viceministro de tecnologías de información y comunicación. Afortunadamente, no se robó información, y los servidores permanecieron ilesos, aunque los sitios web de dos oficinas de alcaldes fueron víctimas de la piratería. Sin embargo, la Escuela de la Función Judicial no tuvo tanta suerte, pues la organización Usuarios Digitales reportó una brecha en su base de datos que resultó en robo de información, tal como se muestra en la figura 6 (Ortíz, 2019).

Figura 6. Ataques informáticos a Ecuador

Nota. Hackers atacaron al país luego de que arrestaron a Julian Assange en el 2019 (Ortíz, 2019)

2.5.2 Criminales informáticos incursionan al banco privado en Ecuador.

Uno de los bancos más grandes de Ecuador, Banco Pichincha, sufrió recientemente un ciberataque que provocó interrupciones en sus operaciones e inutilizó varios cajeros automáticos. Para contener el ataque y evitar daños mayores, el banco tomó la medida de precaución de cerrar una parte de su red. Se cree que el ciberataque al Banco Pichincha se inició a través de correos electrónicos no solicitados que contenían archivos adjuntos maliciosos que inyectaron Cobalt Strike en el sistema del banco. Esta no es la primera vez que Banco Pichincha es víctima de un ciberataque. En un incidente anterior, los ciberdelincuentes conocidos como 'Hotarus Corp' se atribuyeron la responsabilidad, pero el banco refutó sus afirmaciones y atribuyó la infracción a un proveedor comprometido, tal como se muestra en la figura 7 (Lawrence, 2021).

Figura 7.Venta de datos informáticos robados del Banco

Nota. Elaboración propia del Autor.

2.5.3 Ransomware afecta a una empresa de Telecomunicaciones

En julio de 2021, la Corporación Nacional de Telecomunicaciones (CNT) de Ecuador experimentó un ciberataque que resultó en interrupciones en sus operaciones comerciales, portal de pagos y servicio al cliente. Aunque CNT aseguró que los datos corporativos y de los clientes permanecían

seguros y no se veían afectados, el grupo de ransomware RansomEXX afirmó que habían obtenido y compartido con éxito 190 GB de datos, proporcionando capturas de pantalla de documentos seleccionados en una página de fuga de datos oculta. El ataque se originó a partir de la adquisición de credenciales por parte de la pandilla, que utilizaron para infiltrarse en servidores expuestos a Internet a través del servicio abierto RDP. Posteriormente, se propagaron de forma encubierta por la red mientras robaban archivos no cifrados con fines de extorsión. Una vez que la contraseña de administrador se vio comprometida, se implementó el malware, lo que provocó el cifrado de todos los dispositivos (Ávila, 2023).

La ocurrencia de este ataque sirve como un conmovedor recordatorio de la máxima importancia de la ciberseguridad y del imperativo de salvaguardar la información y la infraestructura vitales contra posibles amenazas. Corresponde a las empresas y organizaciones tomar medidas proactivas para fortalecer sus defensas, como implementar protocolos de contraseña sólidos y mantener diligentemente actualizados sus sistemas y software. Además, es crucial establecer medidas de contingencia para mitigar las repercusiones de tales ataques y restaurar rápidamente los sistemas y datos comprometido, tal como se muestra en la figura 8.

Figura 8.Portal de la deepweb

Nota: Elaboración propia del autor.

2.5.3.1 Ataques DDos. El aumento de los ciberataques y las filtraciones de datos durante la pandemia de COVID-19 puede atribuirse a redes vulnerables y sistemas de teletrabajo. En consecuencia, ha habido un mayor enfoque en las regulaciones de ciberseguridad y la aprensión con respecto a la propiedad de los datos y la responsabilidad después de una violación. Un problema persistente en la seguridad de la información es la aparición de ataques distribuidos de denegación de servicio (DDoS).

El impacto de estos ataques se extiende más allá de la comunicación corporativa en Internet y afecta el ancho de banda, la latencia y el flujo de datos. Estos ataques se ejecutan inundando uno o más servidores con numerosas solicitudes, utilizando malware especializado. El objetivo de un ataque DDoS es interrumpir los servicios de conectividad a Internet y puede estar impulsado por diversas motivaciones, incluidos agravios personales o corporativos, extorsión o chantaje, espionaje, competencia desleal o agendas políticas y militares. Un ejemplo notable de esto ocurrió en 2016, cuando los sistemas de nombres de dominio de empresas destacadas como Twitter, PayPal y Spotify fueron atacados, lo que provocó horas de interrupción del servicio para cientos de miles de usuarios y pérdidas financieras significativas. La proliferación de dispositivos IoT inseguros y mal configurados contribuye a la creciente frecuencia de estos ataques. (Márquez, 2019)

2.5.3.2 Perdida de datos. En una tendencia alarmante, los ciberdelincuentes están recurriendo al robo de datos de empresas de todos los tamaños, con el objetivo de extorsionar ofreciendo la recuperación de la información comprometida. Los datos serán eliminados si la corporación se niega a pagar, los ataques de malware costaron a muchas empresas una cantidad significativa de dinero en 2019.

Por ejemplo, Everis, Cadena SER o Prosegur se vieron afectadas por el ciberataque Wanna Cry, que inutilizó todos sus sistemas e impidió trabajar a su personal durante dos días.

Otro ejemplo es el del Instituto Municipal de Empleo y Desarrollo Empresarial de Zaragoza que vivió recientemente una situación en la que un software malicioso se tomó el control de sus servidores, perjudicando la

productividad de sus empleados. Para recuperar el acceso a sus datos, el ciberdelincuente exigió un pago. Sin embargo, es fundamental tener en cuenta que se desaconseja pagar a estas personas. No hay garantía de que realmente restaurarán la información y, al cumplir con sus demandas, solo sirve para incentivarlos a continuar con sus actividades ilícitas (Sardanyés, 2022).

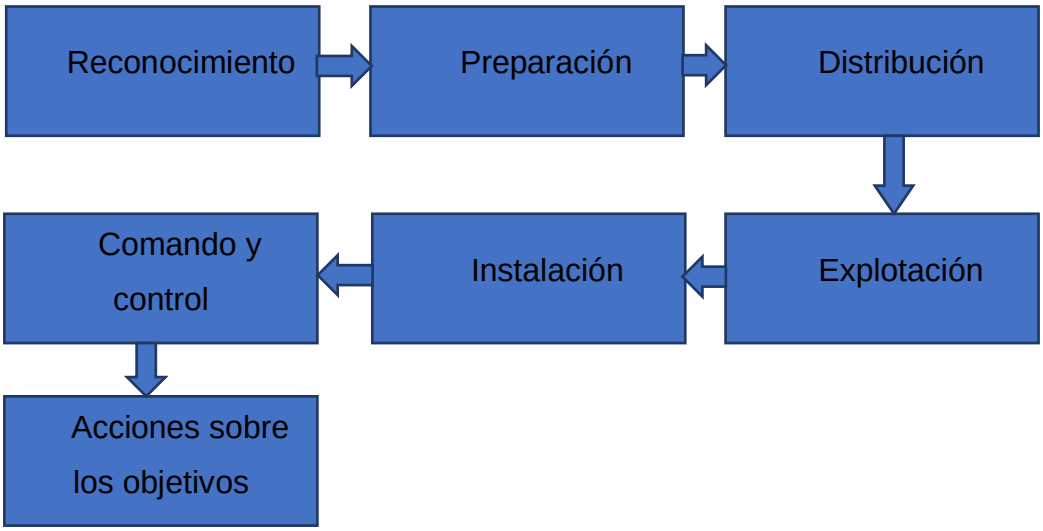
2.5.3.3 Afectación a la reputación. Cuando se pierden los datos, tiene el efecto de disminuir la confianza y crear una percepción negativa de una empresa, organización o individuo. Esta pérdida de confianza puede ocurrir debido a varios factores, incluida la revelación de que la empresa no implementó suficientes medidas de seguridad para proteger los datos de los clientes o el uso malicioso de información confidencial filtrada. Las repercusiones del daño a la reputación son sustanciales y afectan la imagen de marca, la lealtad del cliente y, en última instancia, las ganancias y el valor general de la empresa.

A veces los delincuentes cibernéticos pueden obtener información porque las personas que ingresan a un enlace de un correo electrónico, estos correos electrónicos de phishing son cada vez más realistas y parecen provenir de empresas y organizaciones confiables. Si la persona ingresa al, el delincuente cibernético puede acceder a la información. Una persona relato recibir un correo de este tipo, pero al no confiar en él, lo abrió en su trabajo al día siguiente y así, enteras organizaciones, incluyendo compañías de seguros, son vulneradas. Esto también puede poner en peligro la información de los clientes. Por lo tanto, es importante que las empresas concienticen a sus empleados sobre los peligros cibernéticos y los signos de alerta para evitar dañar su reputación, causar angustia a los clientes y ahorrar dinero (ya que los delincuentes cibernéticos a menudo encriptan archivos y las empresas deben pagar para recuperarlos). Todo por un solo clic en un enlace (Friss, 2018).

2.6 Fases de ciberataques.

Los ciberataques están aumentando en frecuencia, complejidad y sofisticación, lo que representa un desafío constante para los equipos de seguridad cibernética. La capacidad de estos equipos para identificar proactivamente áreas de vulnerabilidad en sus operaciones, antes de que los hackers tengan la oportunidad de explotarlas. Los ataques no buscan robar datos para obtener beneficios económicos, sino interrumpir servicios. En muchos casos, los atacantes optan por no apuntar directamente a sus principales objetivos; en cambio, explotan las vulnerabilidades de proveedores menos seguros que están conectados a estos objetivos. Si bien los detalles específicos de los ciberataques pueden diferir de un caso a otro, hay siete etapas distintas que se pueden discernir en el proceso, tal como se muestra en la figura 9.

Figura 9. Fases de un ciberataque



Nota: Elaboración propia de autor.

2.6.1 Primera fase: Reconocimiento.

El objetivo de los atacantes es identificar un objetivo susceptible e idear estrategias para aprovecharlo. El objetivo inicial podría ser cualquier individuo dentro de la organización, ya que los atacantes solo necesitan un único punto de entrada para comenzar sus actividades. Los correos electrónicos de

phishing sirven como método frecuente para difundir malware durante esta etapa. En esta fase, los atacantes estudian meticulosamente al personal clave de la empresa, sus conexiones comerciales y cualquier información de acceso público sobre la organización objetivo. Cuanto más tiempo inviertan los piratas informáticos en recopilar información sobre el personal y los sistemas de la empresa, mayor será la probabilidad de lograr el éxito en su esfuerzo de piratería.

2.6.2 Segunda fase: Preparación.

Al aprovechar los datos preexistentes, el atacante elabora estrategias para infiltrarse en la red de su víctima prevista. Esto puede implicar la elaboración de correos electrónicos de phishing personalizados que imiten las comunicaciones de proveedores conocidos o conocidos profesionales. El objetivo principal del atacante durante esta fase es adquirir los medios necesarios para capitalizar eficazmente cualquier debilidad que pueda encontrar cuando finalmente acceda a la red del objetivo.

2.6.3 Tercera fase: Distribución.

Durante la fase de entrega, los atacantes recurren a diversas tácticas, como enviar correos electrónicos de phishing y crear páginas web falsificadas, mientras esperan pacientemente recibir información crucial. En los casos en que el correo electrónico de phishing incluye un archivo adjunto de malware, el atacante espera el momento oportuno hasta que alguien lo abre sin saberlo, lo que permite que el malware establezca una conexión con el pirata informático.

2.6.4 Cuarta fase: Explotación.

Durante la fase de detonación, el atacante obtiene control sobre la computadora infectada y su red asociada. Esto se logra aprovechando vulnerabilidades conocidas que ya se han solucionado con parches de seguridad, como las que se encuentran en escritorios remotos. Para evitar este tipo de ataques, es fundamental mantener soluciones de seguridad actualizadas y actualizar periódicamente todos los sistemas, incluido el software de seguridad.

2.6.5 Quinta fase: Instalación.

La víctima se ve comprometida mediante la instalación de software malicioso, aunque hay casos en los que no es necesaria la instalación, como en casos de robo de credenciales o fraude de CEO. Para frustrar los ataques durante esta etapa, es crucial priorizar la educación y la concientización sobre ciberseguridad, además de implementar salvaguardias técnicas como el monitoreo del sistema. Esto se puede lograr a través de una infraestructura interna o contando con la asistencia de servicios de seguridad administrados o personal subcontratado.

2.6.6 Sexta fase: Comando y control.

Una vez que el atacante ha llegado a esta etapa, posee autoridad total sobre el sistema de la víctima y puede ejecutar operaciones malévolas a través de un servidor centralizado denominado Comando y Control (C&C). Estas operaciones abarcan la adquisición de información de inicio de sesión, la captura de imágenes de pantalla, la recuperación de archivos confidenciales, la instalación de software adicional y la adquisición de conocimientos sobre la configuración de red del usuario, entre otras actividades.

2.6.7 Séptima fase: Acciones sobre los objetivos.

Durante esta etapa final, el atacante adquiere la información y se esfuerza por extender su actividad maliciosa a objetivos adicionales. Como resultado, la cadena de muerte opera de manera cíclica en lugar de lineal, ya que cada fase se repite para infectar a más víctimas. Por lo tanto, para frustrar los objetivos del ataque, es imperativa una dedicación firme a la ciberseguridad.

Al garantizar que sus sistemas y equipos se actualicen periódicamente, implementar soluciones de seguridad adecuadas, monitorear la actividad de comunicación y brindar capacitación en ciberseguridad a los empleados, una organización puede mejorar en gran medida su capacidad para identificar y abordar incidentes de seguridad, impidiendo así los esfuerzos de posibles adversarios y salvaguardando sus sistemas e información del peligro. (Incibe, 2020)

2.7 Mecanismos de ciberseguridad.

2.7.1 Criptografía.

La encriptación implica la transformación de un texto plano a un formato ilegible llamado texto cifrado, a través de un proceso conocido como encriptación.

Sucede la siguiente manera:

- El remitente toma el mensaje original en texto plano y lo convierte en un texto cifrado ilegible a través del proceso llamado encriptación.
- El mensaje ilegible, conocido como texto cifrado, se envía al destinatario.
- El destinatario toma el texto cifrado recibido y utilizando un proceso de descifrado, lo convierte de nuevo a su formato de texto plano original. Este paso también se conoce como decodificación.

La conversión de un mensaje sufre una serie de operaciones matemáticas que alteran su apariencia durante la transmisión, pero no afectan al contenido.

Al emplear métodos criptográficos, se puede salvaguardar la privacidad y proteger los mensajes del acceso no autorizado, ya que los mensajes cifrados se vuelven incomprensibles. La utilización de un algoritmo universal, combinada con la selección de una clave específica, constituye la base de estas técnicas.

Hay dos clases de algoritmos:

Dentro del ámbito de las técnicas criptográficas, existen dos categorías distintas: simétricas y asimétricas. El primero requiere la utilización de una clave compartida, lo que exige que ambas partes posean la misma clave secreta. La Figura 10 proporciona una representación visual de estos algoritmos. Por el contrario, los algoritmos asimétricos emplean claves separadas para el cifrado y descifrado, donde una clave permanece

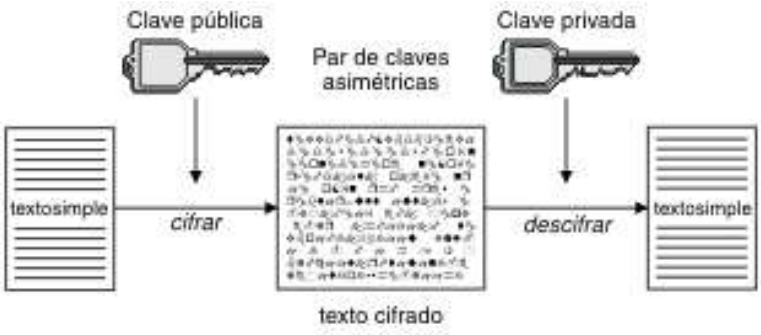
confidencial y la otra es de acceso público. Estos algoritmos son ilustrados en la figura 11 y también son conocidos como criptografía de clave pública.

Para garantizar la seguridad, es fundamental salvaguardar y mantener el secreto tanto de la clave secreta compartida como de la clave privada, mientras que los algoritmos de cifrado y descifrado empleados pueden revelarse abiertamente, tal como se muestra en la figura 10 (IBM, 2022)

Figura 10. Criptografía de clave simétrica

Nota. Adaptado de *Cryptography* de IBM, 2021, Página web de investigación.

Figura 11. Cifrado de claves Asimétricas.



Nota. Adaptado de *Cryptography is the process t*, de IBM, 2021, Página web de investigación.

La figura 10 demuestra el cifrado del texto plano utilizando la clave pública del destinatario, seguido del descifrado con la clave privada correspondiente. Es importante tener en cuenta que sólo el receptor previsto posee la clave privada necesaria para descifrar el texto cifrado. En cuanto los

algoritmos asimétricos, los mensajes tienen la capacidad de cifrarse utilizando claves públicas o privadas, pero solo pueden ser descifrados con la clave opuesta.

La clave privada es la única que debe ser mantenida en secreto, mientras que la clave pública puede ser compartida abiertamente. Aunque estos algoritmos son más lentos en comparación con los simétricos, tienen la ventaja de no tener problemas relacionados con la distribución de claves. (IBM, 2022)

2.7.2 Firewall.

Este dispositivo de seguridad de la red, ya que monitorea de manera efectiva todo el tráfico dentro de una red, determinando si se permite o restringe el tráfico específico en función de un conjunto predeterminado de normas de seguridad.

Durante más de 25 años, los firewalls han servido como salvaguardia inicial en la seguridad de la red. Crean una partición entre redes internas confiables y reguladas y redes externas que no son confiables, como Internet.

2.7.3 Firewall proxy.

Al actuar como intermediario entre dos redes, un firewall proxy sirve como un tipo inicial de dispositivo de firewall. Su función principal es establecer una conexión entre redes para un objetivo específico. Además de esto, ofrece funcionalidades complementarias como protección y almacenamiento temporal de datos al obstruir las conexiones externas directas. No obstante, es importante tener en cuenta que esto podría tener un impacto en el rendimiento y la gama de aplicaciones compatibles.

2.7.4 Firewall de inspección activa.

Un firewall tradicional, comúnmente conocido como firewall de inspección activa, regula el flujo de tráfico otorgando o denegando el acceso en función de factores como el estado, el puerto y el protocolo. Proporciona una vista integral de toda la actividad que ocurre durante la duración de una conexión. Las determinaciones de filtrado se realizan de acuerdo con las reglas establecidas por el administrador, teniendo en cuenta también el contexto.

2.7.5 Firewall de próxima generación (NGFW)

La mayoría de las organizaciones están adoptando firewalls de última generación con el propósito de neutralizar amenazas contemporáneas, tales como ataques en la capa de aplicación y malware avanzado.

Según lo definido por (Gartner, s/f) un firewall de próxima generación debe incluir las siguientes características:

- Capacidades estándar de firewall, como inspección activa.
- Prevención de intrusiones integrada.
- Control y conciencia de aplicaciones para ver y bloquear aplicaciones de riesgo.
- Actualizaciones para incluir fuentes de información futuras.

2.7.7 NGFW centrado en amenazas.

Estos firewalls no solo poseen toda la gama de funciones que se encuentran en un NGFW tradicional, sino que también ofrecen capacidades avanzadas para detectar y abordar amenazas. Al utilizar un NGFW centrado en amenazas, tiene la capacidad de realizar las siguientes tareas.

2.7.8 Función Hash.

La seguridad de un sistema depende en gran medida de la función Hash, que transforma datos regulares en un valor consistente de longitud predeterminada. Cuando se ingresa en esta función, el resultado es un "valor hash", generalmente representado como un número en formato hexadecimal. Las computadoras interpretan los valores en forma binaria, por lo que el valor Hash también se procesa en binario. La generación de un valor Hash, denominado "Hashing", sirve para garantizar la integridad de los datos al detectar posibles modificaciones, manipulaciones o corrupción.

Independientemente de la cantidad de veces que se ejecute el algoritmo Hash en los datos, siempre producirá el mismo resultado siempre que los datos sean los mismos. (Ionos, 2020)

¿Cómo ayuda la función hash a las funciones de búsqueda?

- Examinando grandes cantidades de datos puede consumir muchos recursos, especialmente cuando se busca un término específico dentro de una tabla que contiene numerosos campos, como nombre, apellido y dirección postal. Esta tarea puede llevar mucho tiempo y ser costosa, especialmente en el contexto de una gran ciudad. Sin embargo, existe una solución para agilizar este proceso: la utilización de un valor hash. A cada entrada de la tabla se le asigna un valor hash único, que se recalcula y se compara con los valores hash existentes al realizar una búsqueda. Este enfoque demuestra ser más eficiente en comparación con la búsqueda en todos los campos dentro de la tabla de datos. (Ionos, 2020)

2.8 Seguridad de la Información

La organización de los datos de manera significativa es lo que define la información. Las empresas han reconocido el valor de la información y el daño potencial que puede causar si se maneja mal, lo que las ha llevado a priorizar su protección. La seguridad de la información tiene como objetivo implementar salvaguardas tanto técnicas como humanas, así como establecer procedimientos y protocolos para garantizar la seguridad de la información. Este enfoque se alinea con los tres principios básicos de la seguridad informática, comúnmente conocidos como la tríada CID tal como se muestra en la figura 12.

Figura 12. Principios de la Seguridad informática

2.8.1 Integridad

Refiere a la constancia de la información, respaldando que esta es total y precisa. Algunos mecanismos que garantizan la integridad de los datos incluyen:

- Permisos de archivos.
- Control de acceso de usuarios.

2.8.2 Confidencialidad

El objetivo es asegurar que solo los usuarios autorizados puedan acceder a la información y modificarla. Algunas estrategias para garantizar la privacidad abarcan:

- El uso de cifrado y encriptación de datos
- La implementación de sistemas de identificación de usuarios
- La administración de contraseñas seguras
- La implementación de controles de autenticación.

2.8.3 Disponibilidad

Para mantener una accesibilidad constante para los usuarios autorizados, es fundamental priorizar la disponibilidad de la información. Para lograr esto, es imperativo tomar medidas exhaustivas Para lograr esto, es importante llevar a cabo:

- Mantenimientos preventivos
- Reparar el hardware
- Actualizar el software
- Asegúrese de que haya suficiente conectividad disponible

2.9 Ciber riesgos

Según Cano (2019) El creciente volumen de datos generados por nuevas conexiones e interfaces ha llevado a una convergencia de tecnología entre los mundos físico y lógico, lo que a su vez constituye la causa fundamental de los riesgos cibernéticos. Estos riesgos son diferentes a los tradicionales riesgos tecnológicos y requieren un enfoque interdisciplinario y sistemático para ser comprendidos y manejados adecuadamente en un escenario global. A la luz de estas circunstancias, las organizaciones deben adoptar un nuevo paradigma de gestión para abordar eficazmente los desafíos actuales.

Para lograr una comprensión más profunda de este tipo de riesgos, es fundamental establecer definiciones claras de los distintos componentes que los constituyen, (Dion, 2020) define los siguientes conceptos fundamentales y sus categorías:

2.9.1 Activo

Los activos abarcan elementos tanto tangibles como intangibles que tienen importancia en la organización

2.9.2 Vulnerabilidad

Las vulnerabilidades se originan de deficiencias internas que provienen de cuestiones relacionadas con el diseño, la documentación, la implementación, el código de software o el mantenimiento preventivo del sistema. Estas deficiencias pueden consistir en fallos en el sistema que lo exponen a posibles ataques.

2.9.3 Amenaza

Las amenazas son factores externos que no podemos controlar, pero podemos gestionar y reducir su impacto mediante medidas adecuadas.

2.9.4 Tipos de Amenaza

- **Amenaza adversaria:**

Según Dion (2020), las personas o entidades que intentan infiltrarse e interrumpir su red o negocio pueden clasificarse como las amenazas más críticas.

Amenaza accidental:

Los incidentes de seguridad se producen cuando se comete un error que amenaza la seguridad del sistema. Estos eventos pueden prevenirse al establecer y comunicar de manera efectiva los procedimientos operativos.

- **Amenaza Estructural:**

Los incidentes relacionados con la disponibilidad surgen cuando se producen fallos en los equipos, el software o los controles físicos.

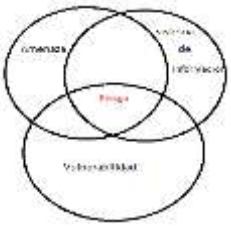
- **Amenaza Ambiental:**

Los eventos naturales pueden desencadenar situaciones que afecten a la disponibilidad. Estas contingencias pueden ser abordadas a través de la implementación de sistemas altamente disponibles. (Dion, 2020)

2.9.5 Riesgo

E-SPIN (2019) dice que un riesgo depende de la presencia tanto de vulnerabilidad como de amenaza, ya que sin estos factores no hay posibilidad de que una amenaza se materialice, tal como se muestra en la figura 13.

Figura 13. Componentes de un riesgo



Nota: Elaboración propia del autor.

2.9.6 Gestión de Riesgos.

Para alinearse con su misión y visión, es crucial que cualquier empresa incluya la minimización de riesgos como uno de sus objetivos al seleccionar un proceso apropiado para sus diversas funciones operativas.

Según (Dion, 2020) el riesgo se puede:

- **Aceptar:**

En los casos en que el nivel sea lo suficientemente bajo como para hacer innecesarias las contramedidas, o si ya se han implementado contramedidas adecuadas (Dion, 2020)

- **Transferir:**

En caso de que la organización carezca de los medios económicos para aceptar, evitar o reducir el riesgo, tiene la opción de transferirlo a una compañía de seguros (Dion, 2020)

- **Mitigar:**

Reducir el nivel de riesgos a un nivel aceptable mediante la implementación de medidas adicionales de control de riesgos (Dion, 2020)

- **Evitar:**

Para mitigar el alto riesgo involucrado, se altera la configuración o el diseño del sistema para prevenir las posibles consecuencias asociadas a una vulnerabilidad específica, impactando así sus aspectos operativos (Dion, 2020).

2.9.7 Tipos de Riesgo.

Según Dion (20020) dentro de una organización, existen cinco categorías distintas que definen diferentes tipos de riesgos:

- **Riesgo Estratégico:**

La consecuencia de trabajar en una industria particular en un momento dado se manifiesta al formar colaboraciones estratégicas en el ámbito empresarial.

- **Riesgo de Cumplimiento:**

Surge a raíz de la falta de cumplimiento de las leyes y regulaciones gubernamentales.

- **Riesgo financiero:**

Está relacionado con aspectos financieros y presupuestarios, generalmente asociados a cuestiones monetarias.

- **Riesgo Operacional:**

Se origina debido a fallos internos en los procesos, en las personas o en los sistemas internos de la organización.

- **Riesgo Reputacional:**

Implica la posibilidad de que la imagen y la confianza en una empresa o comunidad se vean afectadas negativamente debido a problemas con los productos, litigios legales o una mala publicidad. La reputación es un activo que se construye con esfuerzo a lo largo del tiempo, pero puede perderse en un corto período. (Dion, 2020)

CAPÍTULO 3
INSTALACIÓN DE HERRAMIENTAS ADICIONALES

3.1 Kali Linux

Es un proyecto iniciado en 2012 que convierte el venerable proyecto BackTrack Linux, donde Offensive Security se administraba manualmente, en un verdadero derivado de Debian con todas las mejoras necesarias de infraestructura y paquetes. Comenzó cuando decidí reemplazarlo con Kali Linux es conocido por su calidad, estabilidad y amplia disponibilidad de software, por lo que se decidió construirlo en la distribución Debian. (Reydes, 2019) Kali Linux utiliza un sistema operativo diseñado específicamente para ejecutar diversas funciones de seguridad, que incluyen, entre otras, análisis de red, ataques a redes inalámbricas, análisis forense y otras tareas de seguridad esenciales.

Kali tiene instaladas alrededor de 600 herramientas de prueba de penetración, incluidas todo tipo de aplicaciones. Sí, siempre nos enfocamos en problemas informáticos, vulnerabilidades y hacks. Como tal, Kali no es una distribución destinada al uso diario por parte del usuario promedio. Debido a que se enfoca en temas de seguridad informática, generalmente tiene un nicho en empresas de seguridad y profesionales de la programación (incluidos los piratas informáticos) (Jesús, 2022).

Eso no significa que las personas con poco conocimiento no puedan instalar y usar Kali. Sin embargo, comprender las herramientas y cómo usarlas correctamente lleva tiempo. Les dejo brevemente la lista de pros que suelen preferir Kali Linux (Jesús, 2022).

- Administradores de seguridad y red;
- CISO
- Indagación de seguridad
- Ingeniero forense
- Hacker de sombrero blanco y negro
- Experto en informática o aficionado.

3.1.2 Herramientas en Kali Linux y funciones.

Kali Linux incluye una amplia gama de herramientas diseñadas para fines de seguridad y pruebas de penetración. A continuación se enumeran algunas de las herramientas esenciales que se pueden encontrar dentro del marco de Kali Linux:

Nmap: permite exploración de redes empleada para cartografiar redes y detectar dispositivos conectados.

Metasploit: un marco de explotación utilizado para probar la seguridad de sistemas y aplicaciones.

Wireshark: red que facilita la captura y examen del tráfico en una red.

Aircrack-ng: un conjunto de herramientas utilizadas para crackear claves de Wi-Fi.

Burp Suite: una colección de herramientas de seguridad web que abarca un proxy de intercepción, un escáner de aplicaciones web y otras funcionalidades.

Las herramientas expuestas anteriormente pueden ser utilizadas para realizar tareas de seguridad informática como la búsqueda de vulnerabilidades en redes y sistemas, la prueba de penetración y la protección de la información confidencial (Kali, 2023).

3.1.3 Razones por las cuales se debería usar Kali Linux.

En el pasado, se consideraba que el sistema operativo Linux era más adecuado exclusivamente para servidores y no era ampliamente utilizado en computadoras personales. Con el tiempo, ha experimentado una evolución y mejoras significativas. En la actualidad, Linux se ha vuelto fácil de instalar y puede desempeñar un papel similar al de cualquier otro sistema operativo.

Ahora examinemos algunas razones por las cuales sería recomendable utilizarlo.

- Menor riesgo. - Linux es un sistema operativo de código abierto, lo cual implica que la comunidad de desarrolladores puede ver y modificar el código fuente además de no depender de ninguna empresa en caso de que se requiera soporte esto puede continuar por largo tiempo ya que cualquiera puede contribuir por la inmensa popularidad (Hernández, 2021).
- Linux sin costo. - Se trata de un sistema operativo que se encuentra totalmente libre de cargos y al alcance de cualquier individuo. Debido a su naturaleza de código abierto, ha desplazado a UNIX como la elección predominante para servidores web. Tanto pequeñas empresas como equipos de trabajo lo emplean con regularidad. Además, es factible experimentar con diversas distribuciones de Linux sin ningún costo y cambiar a otra si la primera no satisface sus necesidades (Noel, 2022).
- Seguridad. - Es reconocido por su mayor nivel de seguridad y fiabilidad en comparación con otros sistemas operativos. Dado que un extenso grupo de desarrolladores lleva a cabo revisiones continuas en el código, los sistemas Linux experimentan menos problemas de seguridad. Por lo tanto, no se requiere la instalación de software antivirus para proteger su computadora de amenazas como malware y virus. Gracias a su naturaleza de código abierto, es posible examinar y verificar si existen vulnerabilidades en el sistema (Zavala, 2020).
- Sin Spyware. - Asimismo, en Linux, los mecanismos de seguimiento no resultan intrusivos ni incluyen datos personales o confidenciales. La recopilación de datos se lleva a cabo con la finalidad de mejorar la experiencia del usuario y resolver cuestiones técnicas. Los desarrolladores de Linux reconocen la importancia de salvaguardar la privacidad y se esfuerzan por ser transparentes en

cuanto a su política de recolección de datos. Esta transparencia brinda a los usuarios la confianza de que el sistema operativo utiliza su información de manera adecuada y les permite comprender cómo se emplea (Medina, 2022).

3.2 Herramientas utilizadas en Kali Linux.

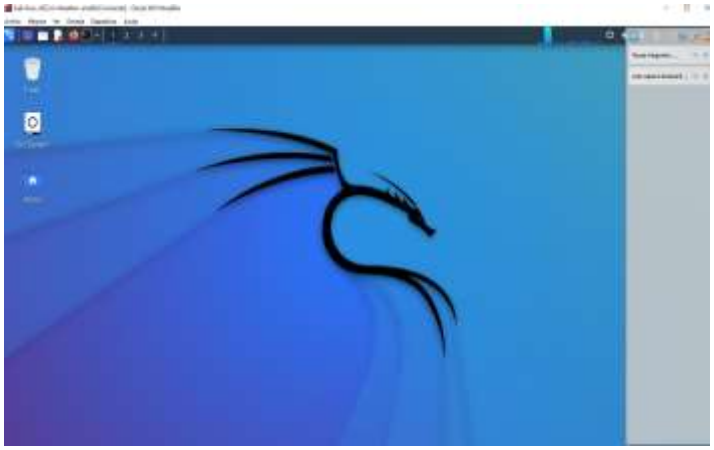
Figura 14. Iniciando Kali Linux desde una VM.

Nota. Elaboración propia de autor.

Figura 15. Ingreso del user y el pass.

Nota. Elaboración propia de autor

Figura 16. Entorno de Escritorio del Kali Linux



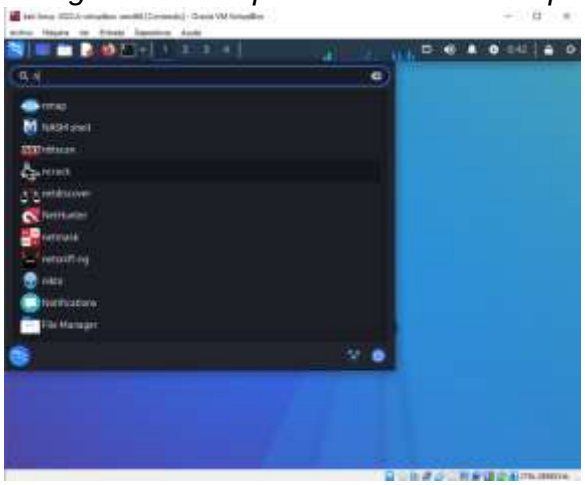
Nota. Elaboración propia de autor.

Visualizaremos algunas herramientas, pero en este caso usaremos las más comunes.

3.2.1 Nmap.

Es una herramienta de código abierto empleada para examinar redes y llevar a cabo auditorías de seguridad. Utiliza paquetes de protocolo IP para identificar qué dispositivos están presentes en una red, los servicios que ofrecen, el sistema operativo que utilizan y otros datos relevantes. Muchos administradores de redes también encuentran que Nmap es valioso para sus tareas diarias. La salida generada por Nmap es un registro de los objetivos analizados, acompañado de detalles adicionales sobre cada uno, como una "tabla de puertos de interés" que muestra el número de puerto, el protocolo, el nombre común del servicio y su estado. Además de la tabla de puertos, Nmap puede proporcionar información suplementaria, incluyendo el nombre DNS, el sistema operativo, el tipo de dispositivo y la dirección MAC (Nmap, 2023).

Figura 17.Nmap en la barra de búsqueda



3.3 Instalación de Nessus en Kali Linux

Después de configurar el entorno de trabajo, la instalación de Nessus se llevará a cabo descargando el software desde el sitio web oficial de Tenable y optaremos por la versión gratuita 'Essentials', con la limitación de escanear solo 16 direcciones IP este proceso implica registrarse en el sitio web y esperar un código de activación que llegará al correo, que será necesario durante la instalación.

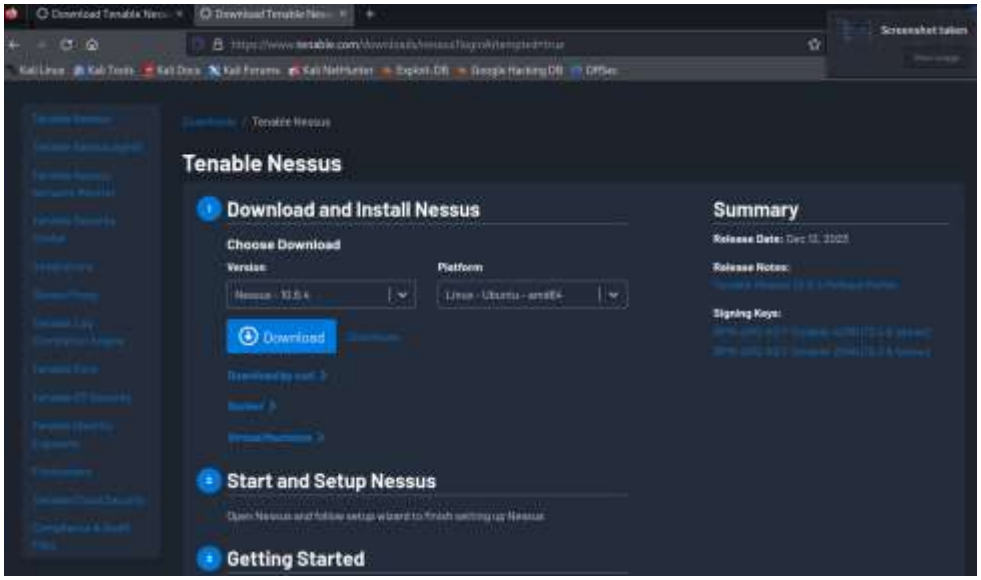
Abrimos nuestro sistema Kali Linux para luego ingresar a la web para buscar el recurso adecuado para nuestro sistema.

Figura 18.Inicio sistema Kali

Nota. Elaboración propia de autor.

Luego entramos a la pagina web para poder bajar el archivo correspondiente ya que la misma detecta automáticamente cuál es el sistema que tienes y que versión puedes instalar en este caso vemos que el sistema operativo es Linux, tal como se muestra en la figura 19.

Figura 19.Pagina web Tenable Nessus



Nota. Elaboración propia de autor.

Verificamos la carpeta donde lo bajamos el instalador y luego desde el terminal de Kali Linux empezamos a instalarlo, tal como se muestra en la figura 20.

Figura 20.Instalando Nessus desde Kali.

Nota. Elaboración propia de autor.

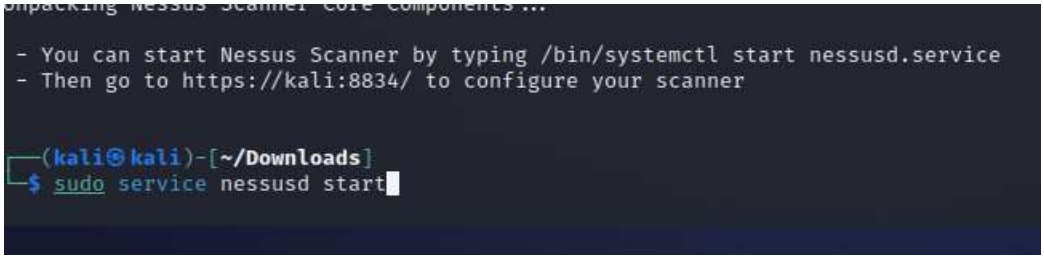
Vemos que luego que después de haber instalado hay que inicializar el servicio, tal como se muestra en la figura 21.

Figura 21.Verificando la instalación del Nessus.

Nota. Elaboración propia de autor.

Inicializamos el servicio de Nessus con “sudo service nessusd start” para luego entrar a configurar, tal como se muestra en la figura 22.

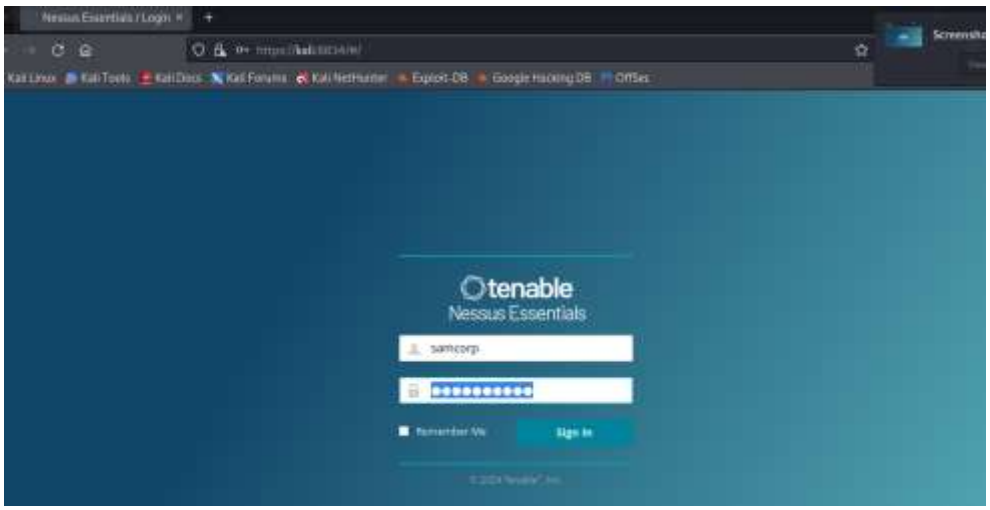
Figura 22.Activamos el servicio de Nessus



Nota. Elaboración propia de autor

Entramos a una página del explorador web e ingresamos el https://kali:8834 para poder inicializar y configurar el Nessus, con nuestro usuario y contraseña, tal como se muestra en la figura 23.

Figura 23.Ingreso del usuario para configurar el Nessus.



Nota. Elaboración propia de autor.

3.3.1 Documentación e instalación de las herramientas usadas.

En esta sección, analizaremos las herramientas externas utilizadas para explotar vulnerabilidades.

La inicial herramienta que emplearemos es Mimikatz, la cual fue creada en el año 2011 por Benjamin Delpy con la intención original de ser una utilidad para detectar debilidades en los protocolos de ataque de Windows. No obstante, con el tiempo, esta aplicación se transformó en una herramienta de ataque con un alto potencial de eficacia contra sistemas Windows.

Mimikatz nos posibilitó la adquisición de todas las contraseñas robustas de un sistema, además de los hashes de las contraseñas almacenados en la

memoria. Aprovechó la funcionalidad de inicio de sesión único de Windows para sustraer las contraseñas almacenadas.

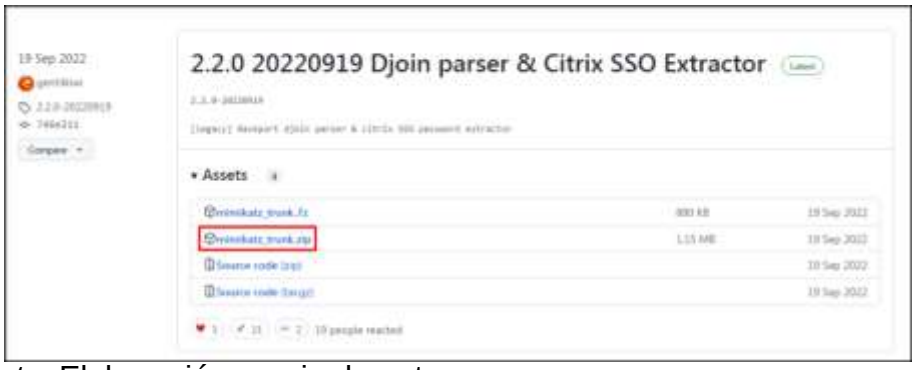
De manera predeterminada, Windows solía utilizar WDigest para almacenar en la memoria todas las contraseñas de usuario del sistema de forma cifrada, incluyendo la clave secreta necesaria para descifrarlas. Fue en este punto donde Mimikatz intervino para obtener estas contraseñas.

En la actualidad, Windows ha desactivado la función de WDigest de manera predefinida, pero aún permanece integrada en los sistemas operativos de Microsoft. Esto representa una potencial amenaza, ya que un atacante que tenga acceso al sistema podría reactivarla y utilizar Mimikatz para recuperar todas las contraseñas.

Este software es de código abierto y puede descargarse del siguiente repositorio de GitHub: https://github.com/gentilkiwi/mimikatz/releases

Una vez dentro descargamos el archivo 'mimikatz_trunk.zip', tal como se muestra en la figura 24.

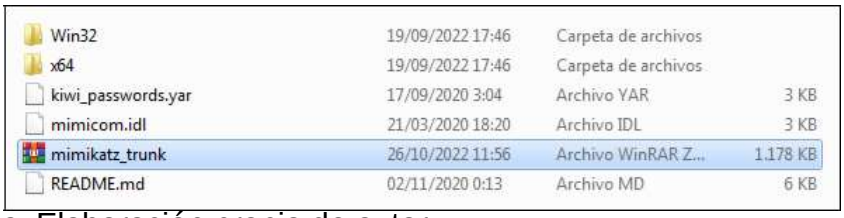
Figura 24.Descarga de Mimikatz



Nota. Elaboración propia de autor.

Luego de terminar la descarga descomprimimos el .zip, tal como se muestra en la figura 25.

Figura 25.Descomprensión del archivo mimikatz_trunk .rar



Nota. Elaboración propia de autor.

3.3.2 Metasploit: Herramienta de Penetración y Desarrollo Exploits

Metasploit constituye una plataforma robusta para realizar pruebas de desarrollo y penetración de exploits que proporciona a los profesionales de la seguridad cibernética una suite integral para descubrir vulnerabilidades y evaluar la seguridad de sistemas informáticos.

Inicialmente creado por H.D. Moore, Metasploit ha evolucionado para establecerse como un referente en la industria para llevar a cabo pruebas de penetración.

Esta plataforma ofrece un extenso conjunto de herramientas, exploits, payloads y módulos que permiten a los profesionales simular ataques cibernéticos en entornos controlados, con el objetivo de identificar y corregir vulnerabilidades antes de que los actores maliciosos las exploten, su capacidad para automatizar y agilizar el proceso de prueba de penetración lo ha convertido en una herramienta esencial para expertos en seguridad y investigadores, tal como se muestra en la figura 26 (metasploit, 2023).

Figura 26.Metasploit ya instalado en las nuevas versiones de Kali.

Nota. Elaboración propia de autor

CAPÍTULO 4

DETECCIÓN, EXPLOTACIÓN Y MITIGACIÓN

4.1 Descripción Experimental.

En esta sección, detallaremos la implementación práctica del proyecto, comenzando con la identificación de los distintos hosts en la red. Después, procederemos a analizar las vulnerabilidades presentes en cada equipo y, una vez identificadas, las aprovecharemos utilizando Metasploit y Mimikatz. Por último, realizaremos la aplicación de parches en los sistemas

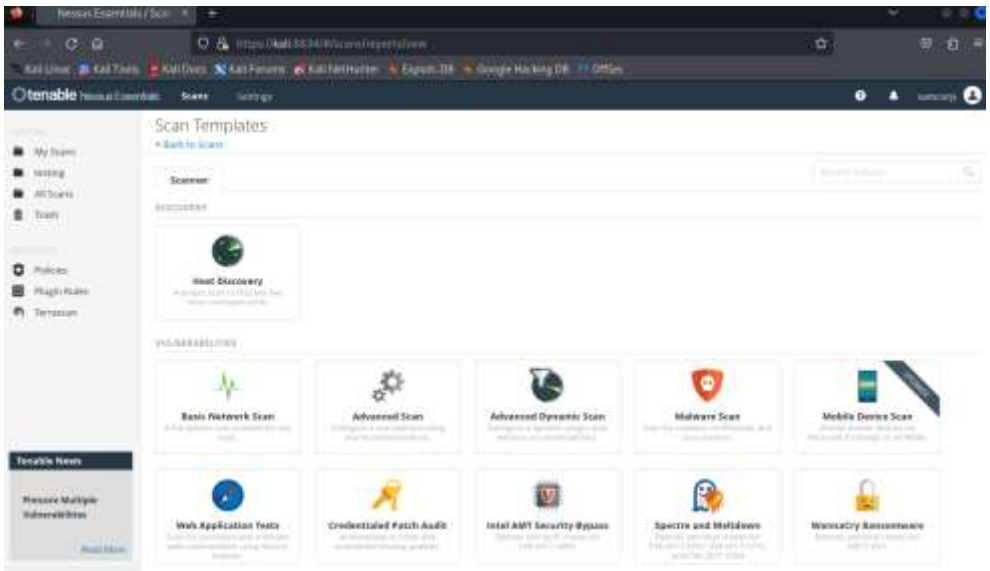
4.1.1 Escaneo de la red – Detección.

Comenzaremos por acceder a Nessus, para ello, abriremos el navegador Google Chrome y escribiremos la siguiente dirección URL (https://localhost:8834). Una vez dentro, procederemos a generar un nuevo escaneo con el objetivo de identificar los dispositivos conectados a nuestra red. Para esto, hacemos clic en la opción que indica 'New Scan'.

Ilustración 1.– Creación de escaneo

Llegamos a la pantalla donde están todas las opciones y escogemos la primera que es “Host Discovery”.

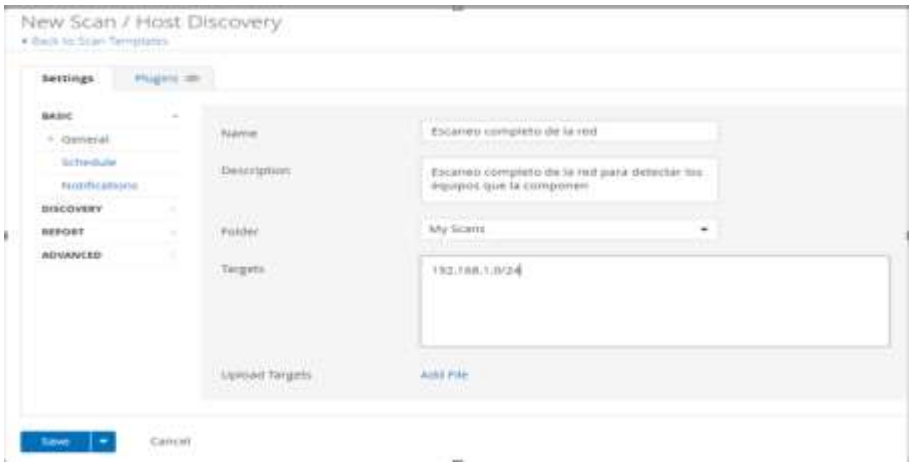
Ilustración 2. – Selección de escaneo



Dentro de la sección de escaneo, se nos pedirá que rellenemos varios campos. Daremos un nombre y una descripción al escaneo, además de suministrar la dirección IP de la red que queremos analizar. Para abarcar toda la red, especificamos la IP con la terminación '/24', indicando así que, de los

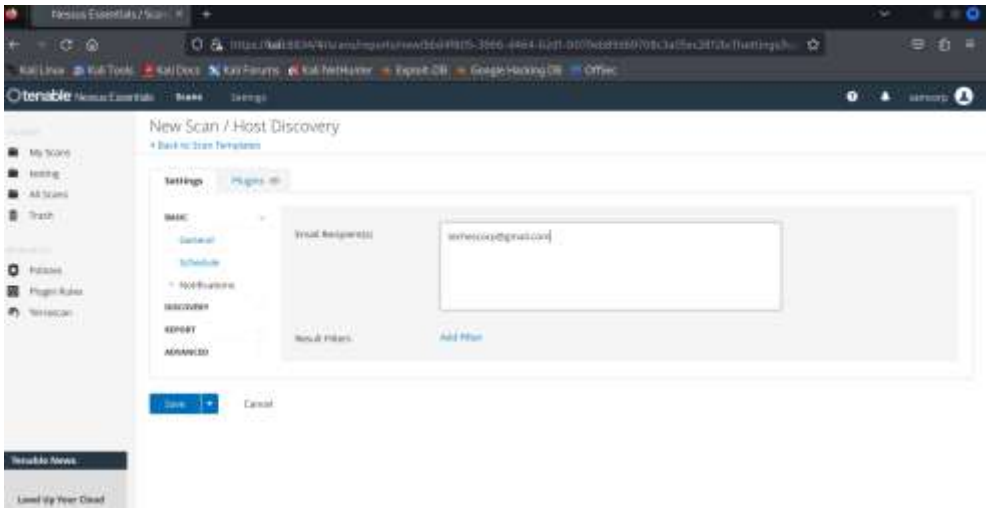
32 bits que conforman la dirección, los primeros 24 corresponden a la red. En este caso, la red se identifica como 192.168.1.0/24.

Ilustración 3. – Configuración general



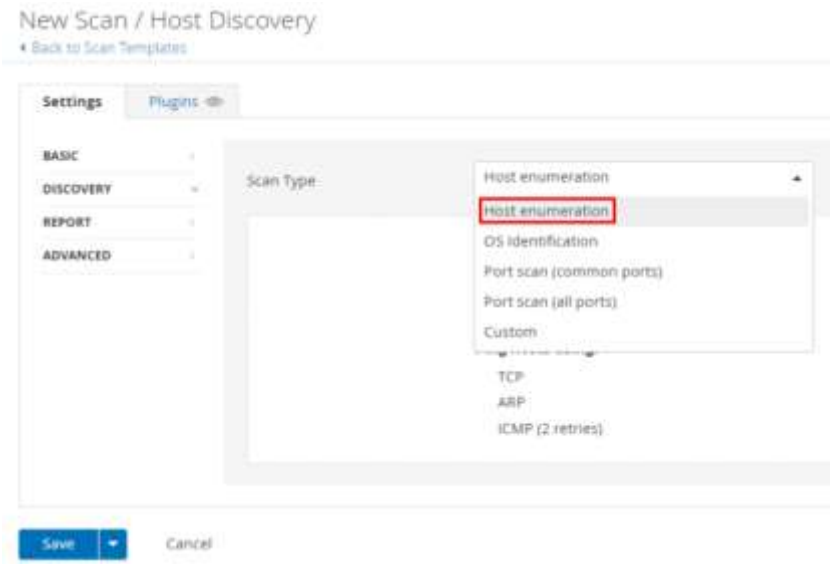
El siguiente apartado que debemos completar es el de notificaciones, en este campo ingresaremos la dirección de correo electrónico a la cual se enviarán los resultados de los análisis..

Ilustración 4.– Introducción de correo



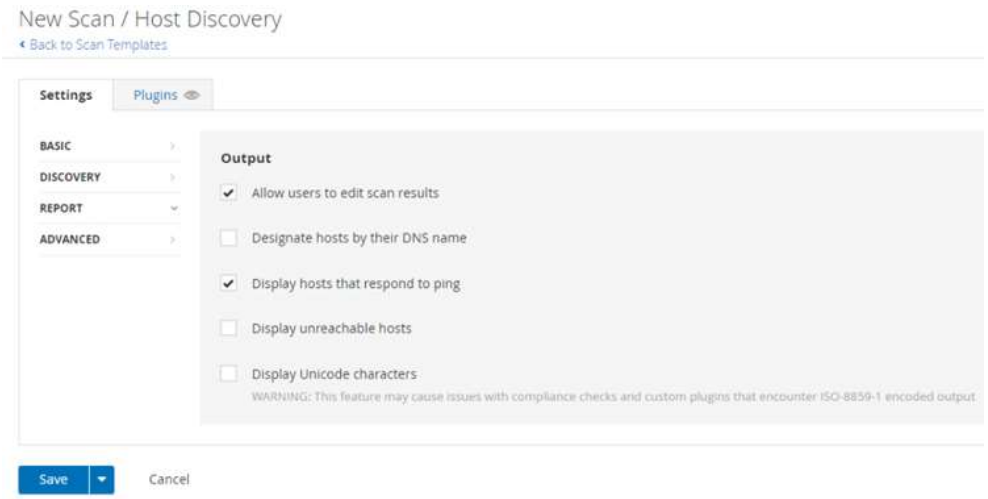
Después de completar los campos en la sección "Basic", avanzamos a la siguiente sección denominada "Discovery". Aquí elegiremos el tipo de escaneo que deseamos realizar. En esta ocasión, optamos por una detección de hosts básica y marcamos la opción "Host enumeration".

Ilustración 5. – Tipo de escaneo: Host enumeration – Host discovery



En la sección siguiente titulada 'Report', mantendremos las configuraciones predeterminadas proporcionadas por Nessus para este escaneo. Estas configuraciones permiten que cualquier usuario de Nessus pueda adaptar los resultados del escaneo a sus necesidades y ver todos los dispositivos que respondan al ping.

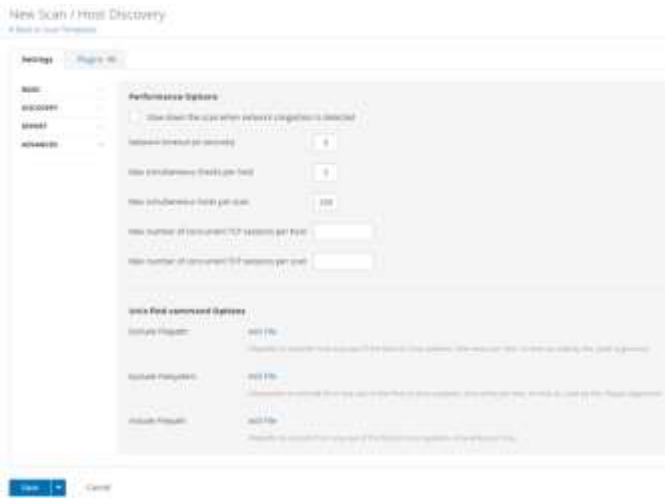
Ilustración 6.– Parámetros de configuración



En la sección "Advanced" elegimos el período de espera que Nessus permite para recibir una respuesta al ping de un host, la cantidad máxima de verificaciones que se realizarán por host para validar la información y el

número máximo de hosts que se analizarán simultáneamente en cada escaneo.

Ilustración 7. – Parámetros de configuración avanzados



Luego de tener configurado todos los parámetros del escaneo damos en "save" y ejecutamos yendo a la pestañada de "My scan" y le das al botón play.

Ilustración 8. – Ejecución del escaneo

Cuando presionamos el botón play, podemos observar cómo comienza la ejecución

Ilustración 9. – Progreso del escaneo

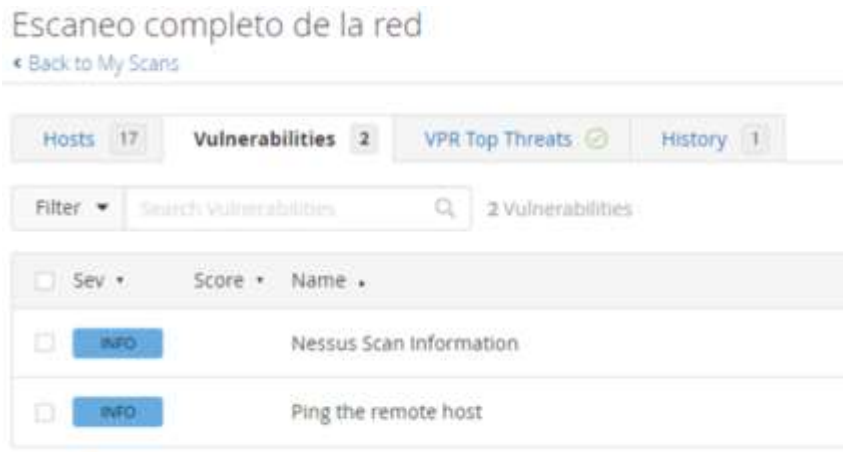
Una vez que el escaneo ha concluido, podemos acceder a él para revisar toda la información recopilada. En la pestaña 'Hosts', en el lado derecho, encontramos datos como el estado del escaneo, la fecha de inicio y

finalización, así como su duración. En la esquina inferior derecha, observamos un círculo que representa las vulnerabilidades y muestra el porcentaje de cada tipo; en este caso, solo se presentan vulnerabilidades informativas, dado que este tipo de escaneo se limita a enviar pings. En el lado izquierdo, se enumeran todas las direcciones IP de los dispositivos detectados en nuestra red, junto con los puertos abiertos asociados a cada uno.

Ilustración 10.– Resultados del escaneo

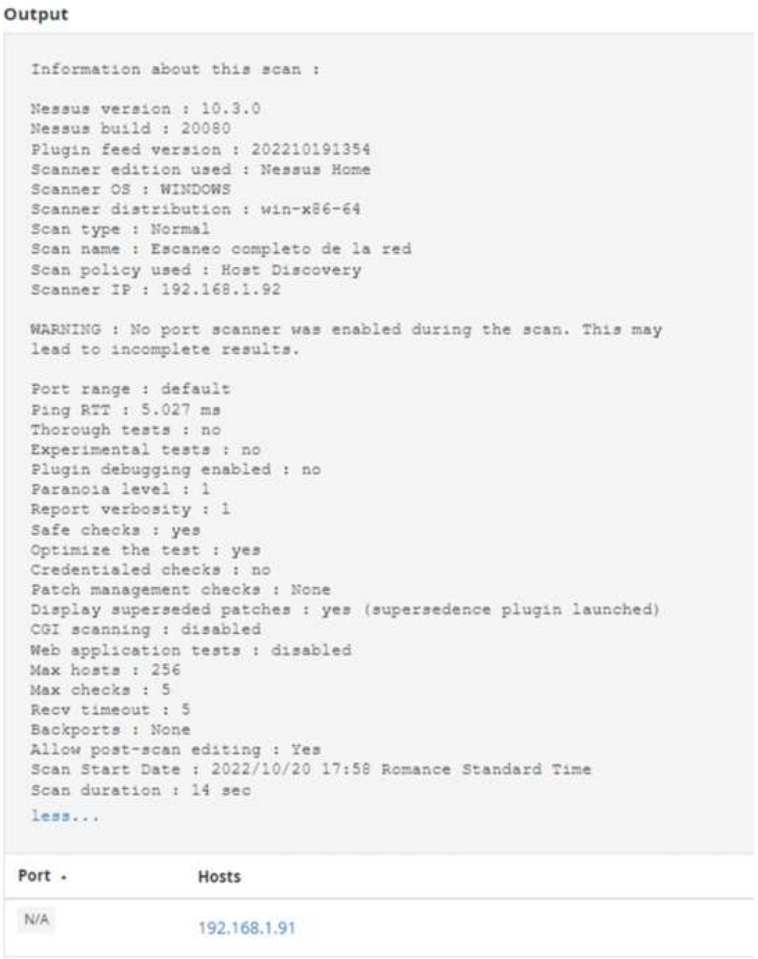
En la pestaña "Vulnerabilidades", visualizamos un resumen completo de todas las vulnerabilidades detectadas, si bien en esta ocasión se presentarán únicamente dos de tipo informativo.

Ilustración 11. – Pestaña vulnerabilidades



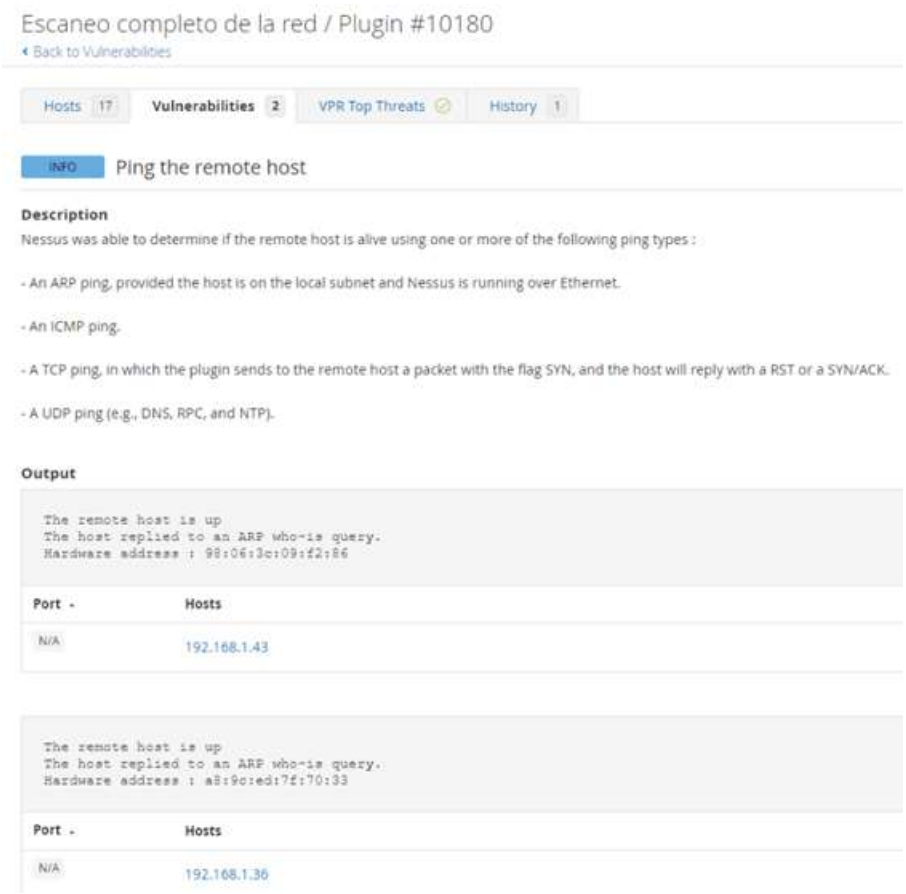
Cuando ingresamos a la primera vulnerabilidad de tipo informativo, podemos ver la dirección IP del dispositivo al que se hace referencia en la información, así como todos los ajustes de configuración que se aplicaron durante la configuración del escaneo.

Ilustración 12.– Información del escaneo



En la segunda vulnerabilidad de tipo informativo, se presenta una descripción acerca de los tipos de pings que fueron enviados para identificar los dispositivos, junto con los que respondieron a estos pings. Asimismo, se proporciona información acerca del hardware del equipo.

Ilustración 13. – Información de los pings y los equipos

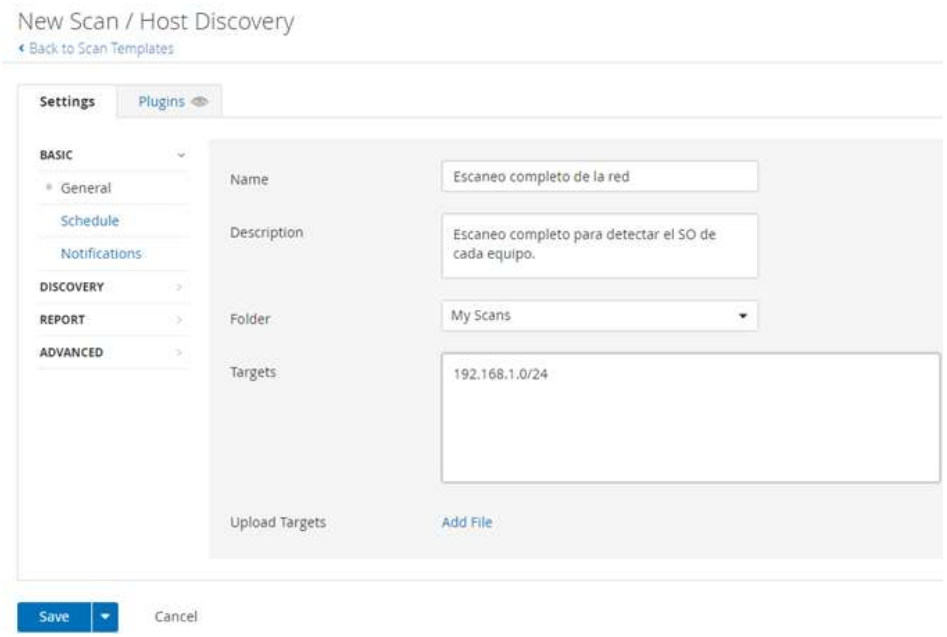


En la pestaña de "VPR Top Threats", se encuentra el "vulnerability priority rating" (índice de prioridad de vulnerabilidades), el cual, en este escenario, no se presenta.

Ilustración 14.– VPR

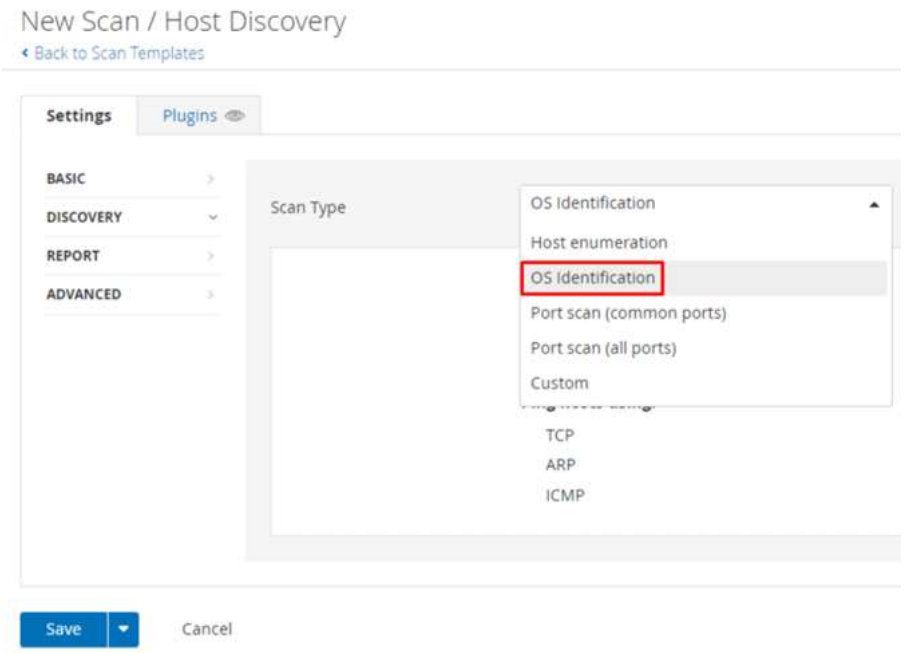
Después de completar el escaneo previo utilizando "Host enumeration", es necesario realizar otro escaneo, pero esta vez cambiando la opción a "OS identification" para identificar las direcciones IP correspondientes a ordenadores. Se repiten los mismos procedimientos, ajustando los parámetros y proporcionando un nuevo nombre junto con la dirección IP de la red.

Ilustración 15. – Configuración general – Host 2



En la sección de "Discovery" ahora seleccionamos el tipo "OS identification" para permitir que Nessus identifique cuáles de las direcciones IP detectadas corresponden a ordenadores.

Ilustración 16.– Tipo de escaneo: OS identification

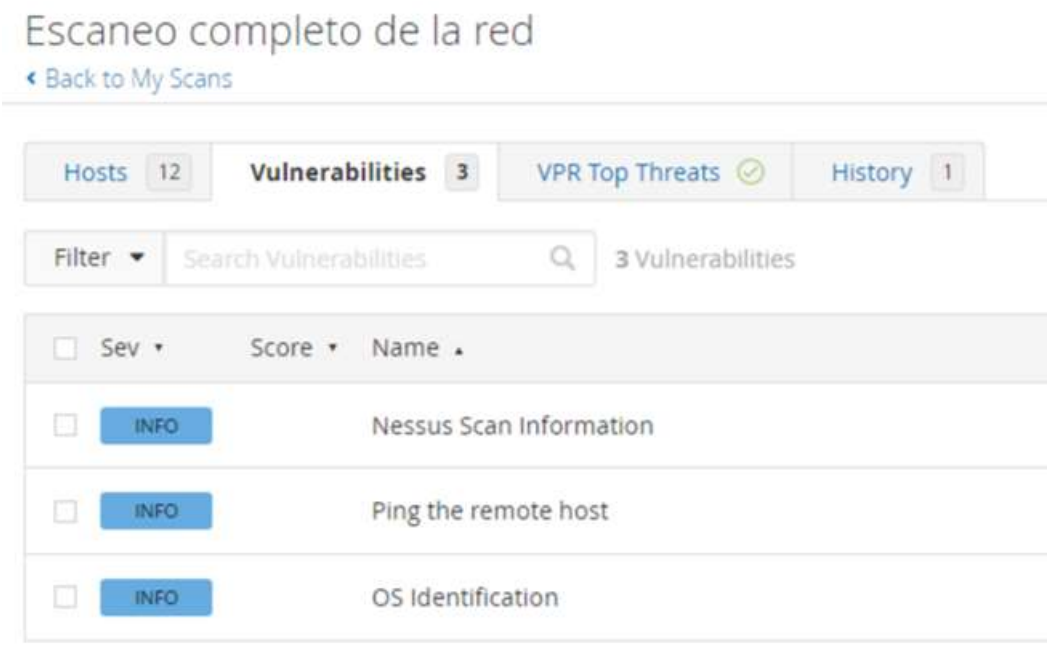


A continuación, mantenemos la misma configuración que se utilizó en el escaneo anterior y procedemos a ejecutarlo. Después de que el escaneo finaliza, accedemos a los resultados, donde podemos observar las direcciones IP conectadas a nuestra red, así como los puertos abiertos en cada sistema, entre otros detalles.

Ilustración 17. – Resultados del escaneo 2

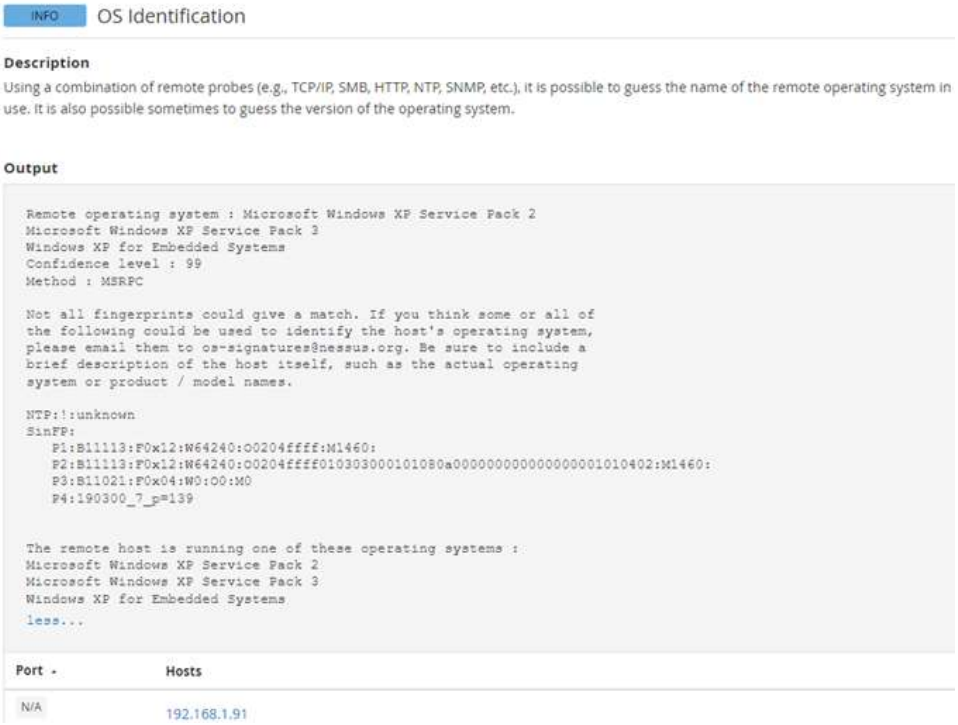
Ahora en la pestaña de "Vulnerabilities" observamos una nueva, "OS" identification.

Ilustración 18. – Vulnerabilidad – OS identification



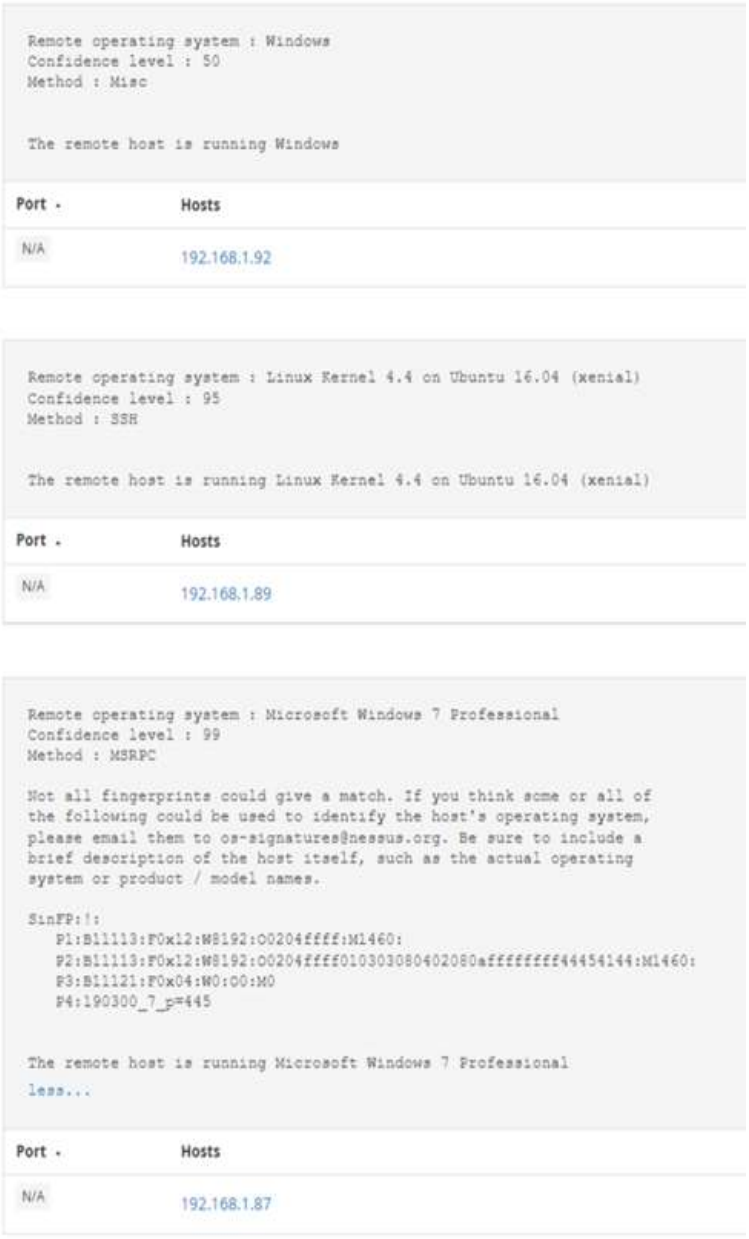
En la nueva vulnerabilidad, encontramos detalles acerca del sistema operativo que está instalado en los dispositivos, junto con su dirección IP. Además, se incluye una breve descripción que explica los métodos utilizados por Nessus para determinar cuál sistema operativo se trata

Ilustración 19.– información sobre Windows P – Host Discovery 2



Además de la información sobre el sistema operativo y su versión, en el caso de Windows, también podemos visualizar otros detalles, como la versión del kernel instalado, con esto ya habríamos detectado que tenemos equipos con Windows distintas versiones.

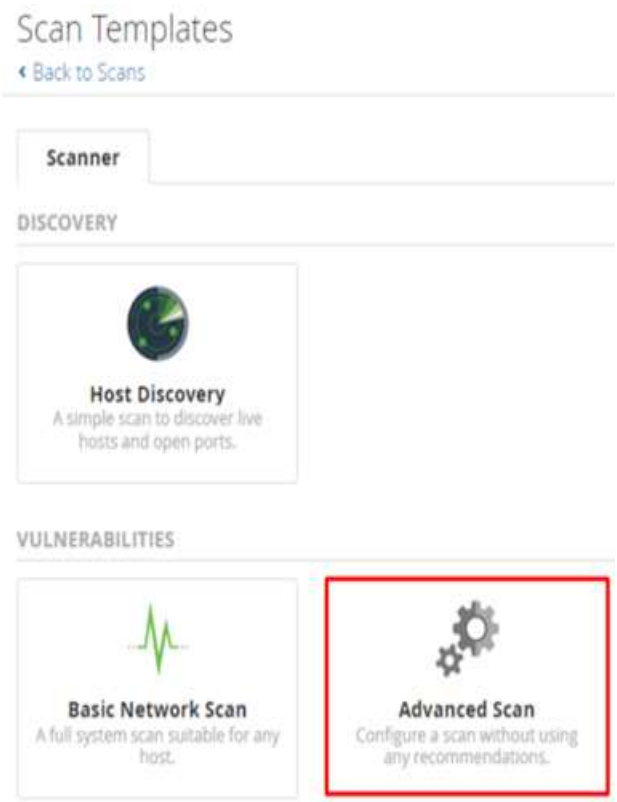
Ilustración 20. – Información sobre los sistemas detectados.



4.2 Búsqueda de vulnerabilidades – Escaneo de la red.

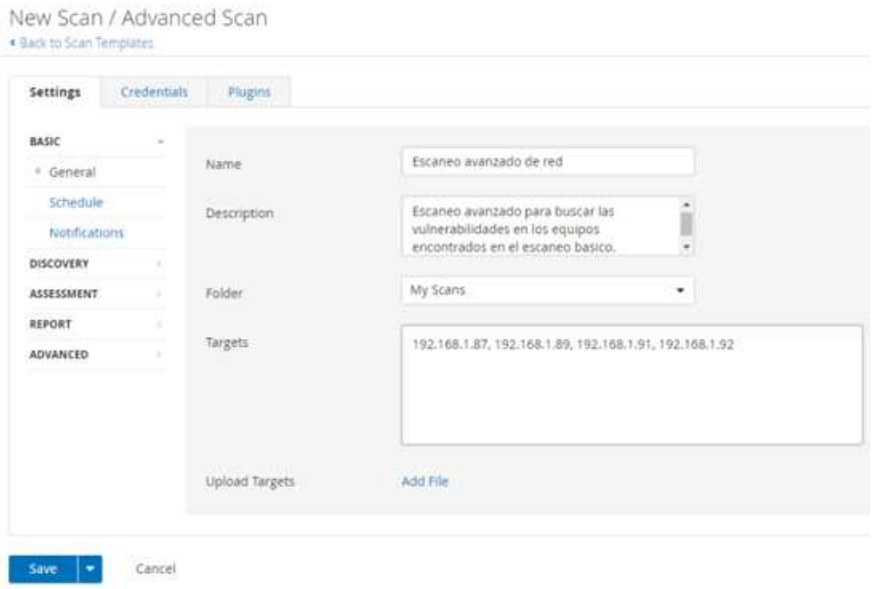
Después de identificar las 4 direcciones IP que pertenecen a los ordenadores, procederemos a realizar otro escaneo denominado "Advanced Scan" con el objetivo de detectar todas las vulnerabilidades presentes en cada uno de estos equipos. Para llevar a cabo este proceso, creamos un nuevo escaneo y seleccionamos la opción "Advanced Scan".

Ilustración 21. – Advanced Scan



Ingresamos un nombre al escaneo que vamos a realizar para poder identificarlo, además de proporcionar las 4 direcciones IP que identificamos en el escaneo previo.

Ilustración 22– Configuración general - Advanced Scan

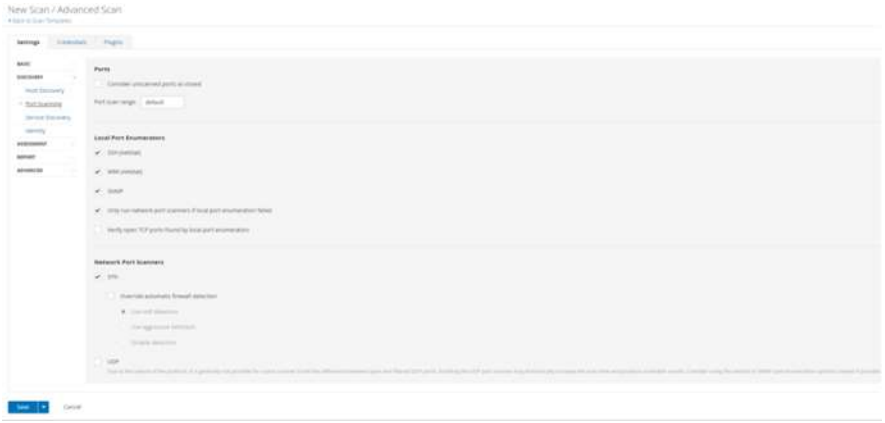


En este tipo de escaneo, tenemos la capacidad de ajustar los parámetros relacionados con el tipo de ping que deseamos emplear..

Ilustración 23. – Host Discovery - Advanced Scan

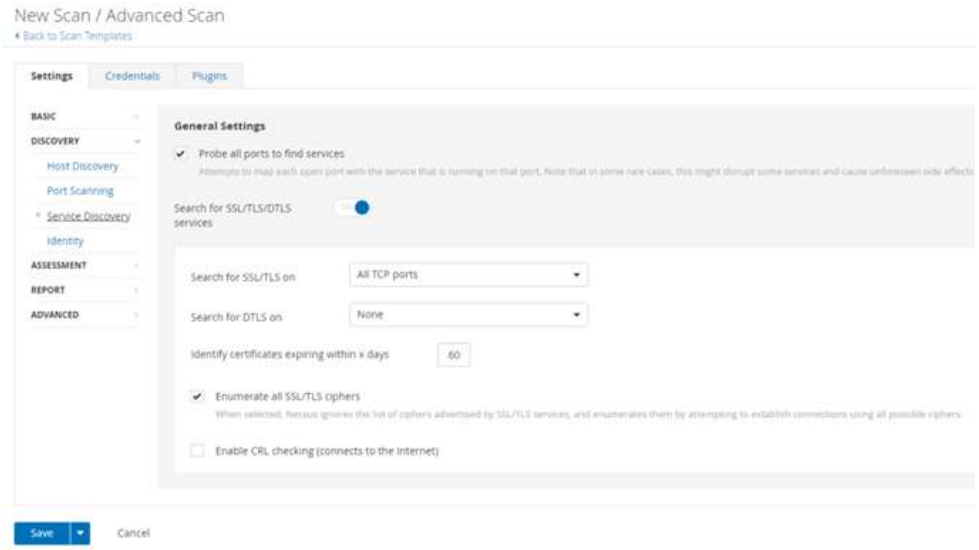
En la opción de "Port Scanning" ajustaremos todos los parámetros relacionados con la detección de puertos.

Ilustración 24. – Port Scanning - Advanced Scan



En la parte de ‘Service Discover”, activaremos diversas opciones para permitir que el analizador de Nessus identifique qué servicio está utilizando cada puerto activo. También especificaremos qué tipo de tecnología preferimos que utilice para escanear los puertos.

Ilustración 25.– Service Discovery - Advanced Scan



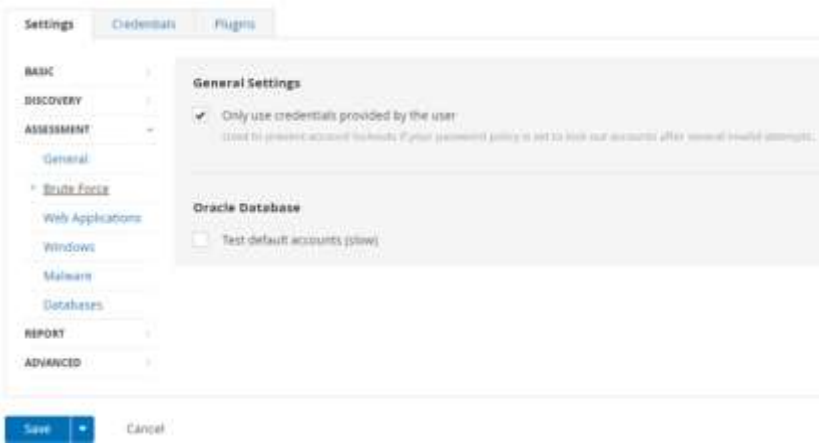
La próxima es ‘Identity’, pero no la habilitaremos porque está diseñada para redes con un active directory implementado, en la sección ‘Assessment’

que sigue, hay opciones para ajustar ciertos parámetros para un escaneo más detallado, pero también la dejaremos inactiva, además, existe la posibilidad de ajustar el tiempo de demora para la comprobación del software antivirus. Por último, encontramos la sección SMTP, que puede emplearse para realizar pruebas de envío de (spam).

Ilustración 26. – Assessment - Advanced Scan

En la sección ‘Brute Force’, seleccionaremos la opción que indica que proporcionaremos la contraseña del equipo y que no se intentará descifrarla.

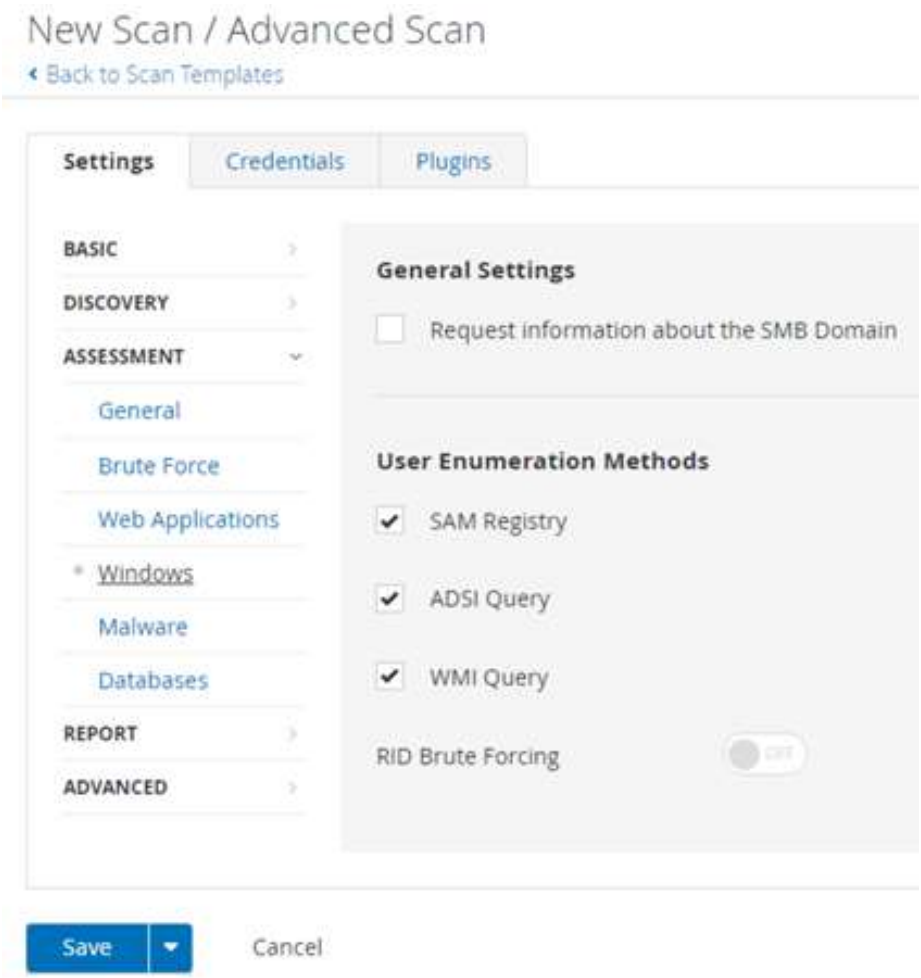
Ilustración 27. – Brute force - Advanced Scan



No habilitaremos la categoría 'Aplicaciones web', dado que no tenemos ninguna aplicación web que requiera ser sometida a un escaneo. En la sección 'Windows', solo activaremos las diferentes técnicas de enumeración de hosts

proporcionadas por Nessus, mientras que dejaremos desactivadas las demás opciones. Estas últimas opciones se utilizan para consultar a los usuarios del dominio en lugar de a los usuarios locales y para enumerar a los usuarios mediante fuerza bruta utilizando el identificador RID.

Ilustración 28– Windows - Advanced Scan



La sección 'Malware' se utiliza para instruir al sistema a buscar virus específicos que puedan estar presentes en archivos cifrados en la computadora, utilizando diversas tecnologías de cifrado como MD5/SHA1/SHA256. En este caso, la mantendremos desactivada.

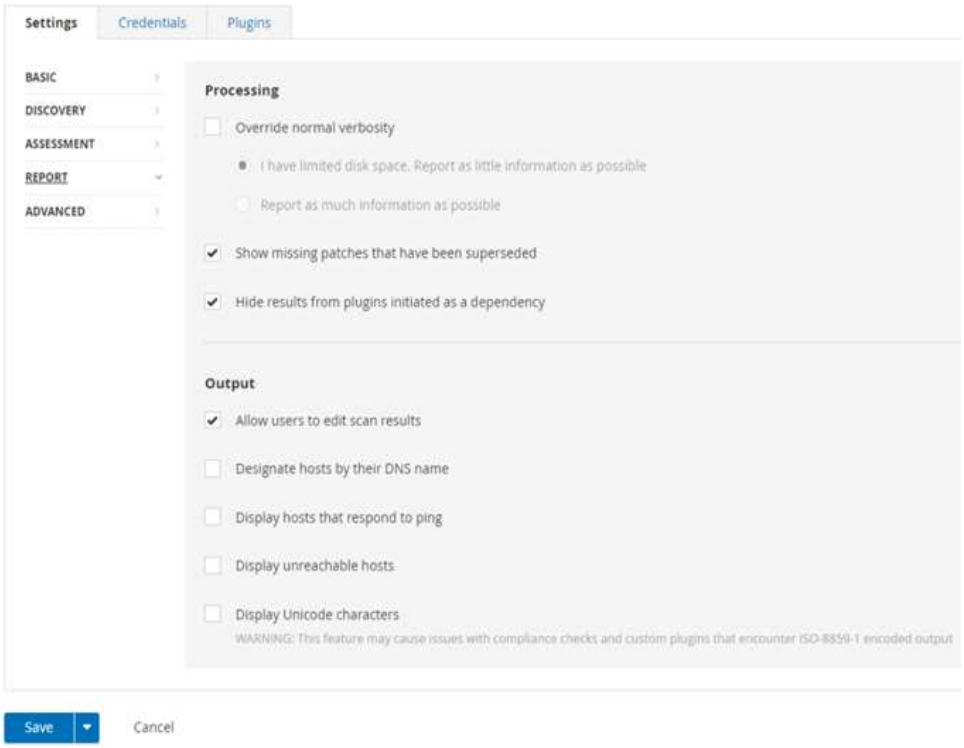
La sección 'Databases' se emplea para indicar al escáner de Nessus que intente autenticarse utilizando un nombre de usuario y contraseña

proporcionados al escáner en una base de datos conocida en la red. Mantendremos esta sección desactivada.

En la sección 'Reporte', activaremos las opciones que nos permitirán visualizar los parches que han sido reemplazados y ocultar los resultados de los complementos iniciados como dependencias. Además, mantendremos seleccionada la opción predeterminada, que permite que cualquier usuario con acceso a Nessus pueda editar los resultados del escaneo.

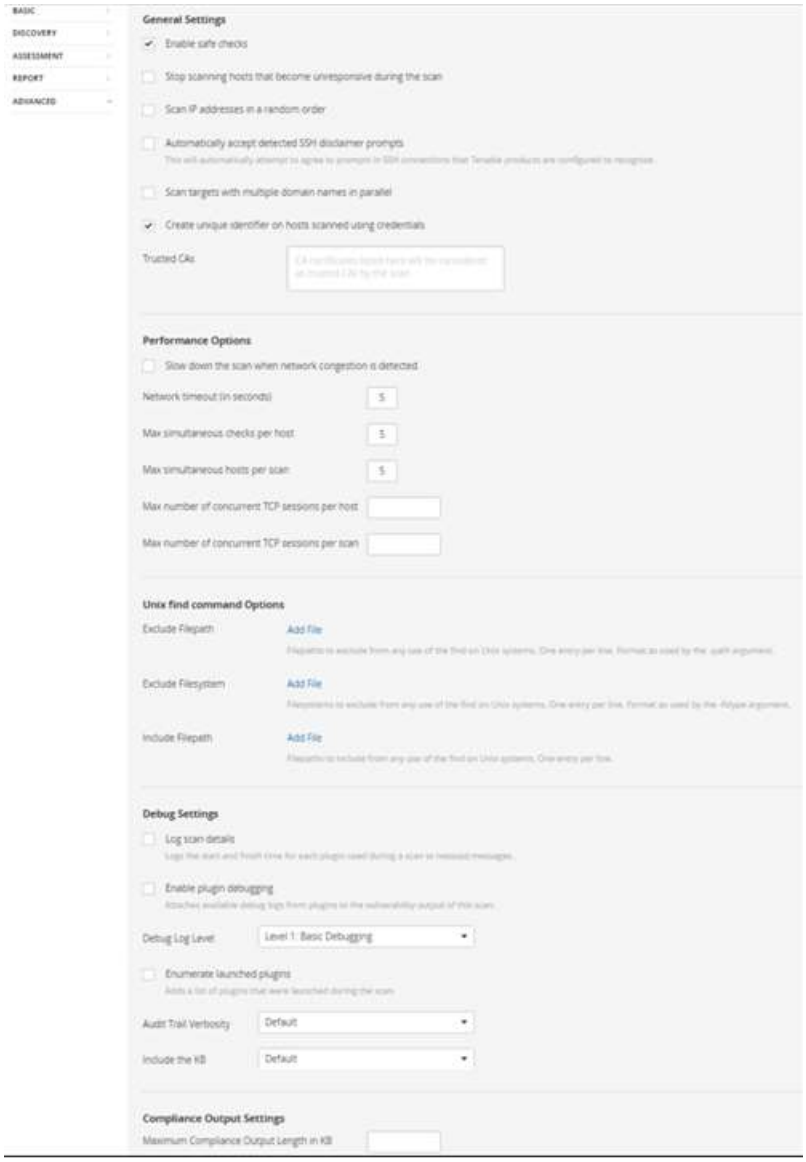
.

Ilustración 29.– Report - Advanced Scan



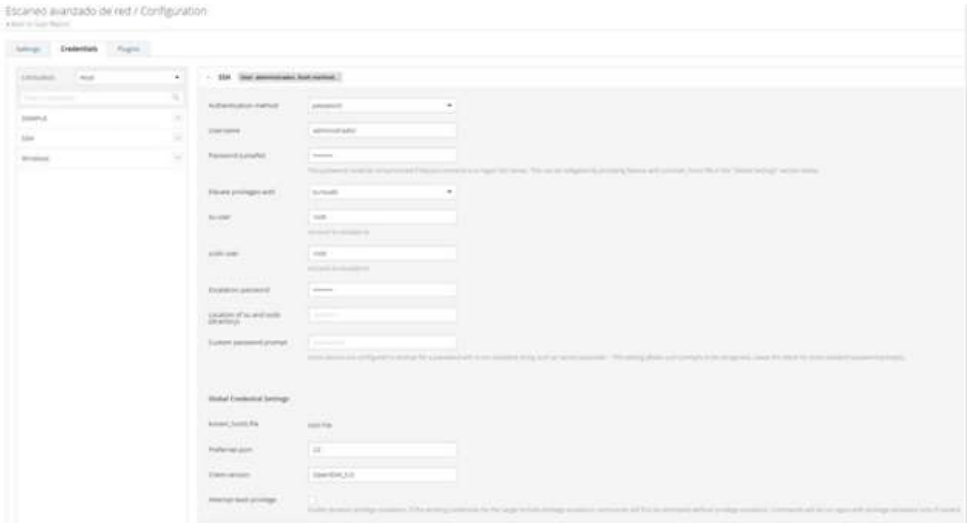
Dentro de la sección "Advanced", perfeccionaremos aún más la configuración del escaneo al habilitar las opciones de escaneo seguro y la generación de un identificador único para cada host. También definiremos el tiempo de espera de la red, el número de escaneos por host y la cantidad máxima de escaneos simultáneos por host.

Ilustración 30. – Advanced - Advanced Scan



Después, nos dirigimos a la pestaña "Credenciales", donde ingresamos tanto el nombre de usuario como la contraseña de cada equipo. Esto se debe a que el escaneo se vuelve más exhaustivo al contar con estos datos. Además, en ausencia de esta información, podríamos verse obligados a llevar a cabo un ataque de fuerza bruta, que incluye una lista de nombres de usuario comunes y sus contraseñas correspondientes.

*Ilustración 31. – Credential Windows - Advanced Sca*n



A continuación, en la sección de "Complementos," seleccionaremos la opción de incluir todos los complementos en el escaneo, con el fin de que analice todos los parámetros en cada equipo.

Ilustración 32. – Plugins - Advanced Scan

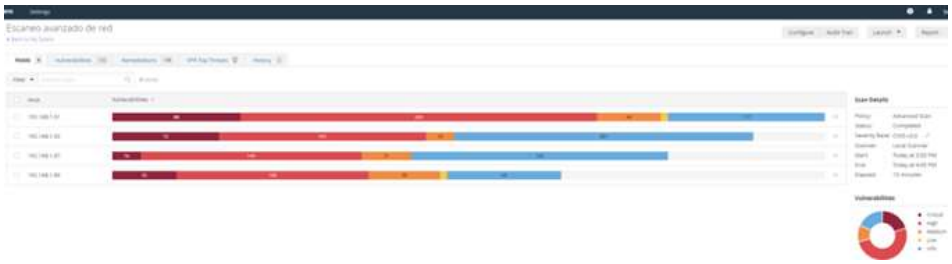
Después de haber concluido la configuración de todos los parámetros en cada sección del escaneo "Advanced Scan", procedemos ejecutarlo haciendo clic en el botón de play. Este tipo de escaneo tiene un período de ejecución prolongado, por lo que se requiere paciencia durante el proceso. Es aconsejable evitar sobrecargar la red con otros dispositivos mientras se lleva a cabo el escaneo, ya que podría generar falsos positivos debido a los paquetes no deseados.

Ilustración 33. – *Progreso del escaneo - Advanced Scan*

Una vez completado el escaneo, lo primero que se observa son barras horizontales que muestran la cantidad de vulnerabilidades de cada tipo en cada equipo, junto con la dirección IP de cada equipo visible en el lado izquierdo. En el lado derecho, se pueden consultar los detalles del escaneo, como el tipo de escaneo realizado, su estado (que se puede seguir en tiempo real mientras se analizan los diferentes equipos), el CVSS (Sistema de Puntuación de Vulnerabilidades Comunes) que proporciona una puntuación y permite estimar el impacto de las vulnerabilidades, el escáner, la fecha y hora de inicio del escaneo, la fecha y hora de finalización del escaneo, así como su duración.

Justo debajo de esta información, se encuentra un gráfico circular que representa las vulnerabilidades. En este gráfico, se muestran distintos niveles de gravedad de las vulnerabilidades, que abarcan desde menor hasta mayor, como Informativa, Baja, Media, Alta y Crítica. Por último, también se presenta el porcentaje de cada nivel de gravedad en el escaneo realizado.

Ilustración 34. – *Visualización de resultados - Advanced Scan*

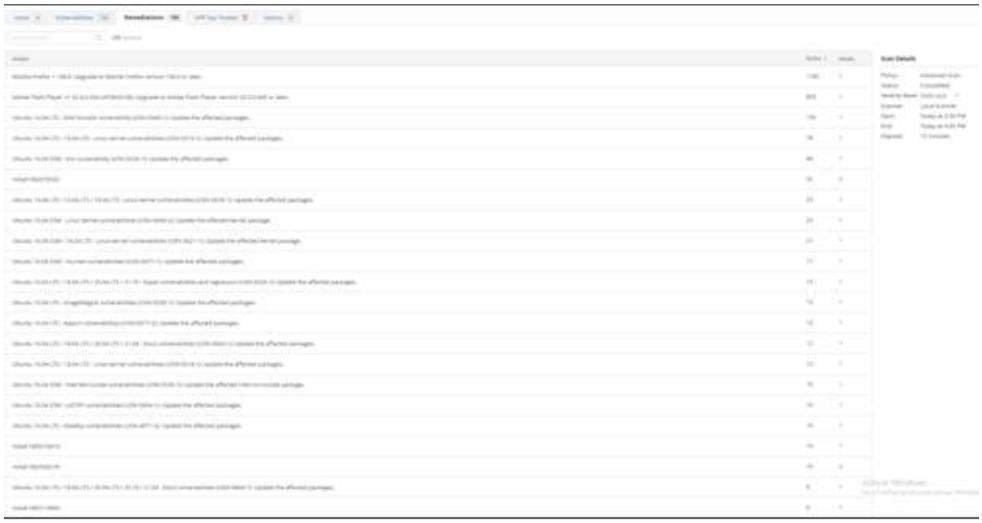


En la pestaña de "vulnerabilities", se encuentra un resumen consolidado de todas las vulnerabilidades organizadas en orden descendente de gravedad en todos los equipos escaneados. Si accedemos a cada una de estas vulnerabilidades, podemos obtener información detallada sobre ellas y cómo abordar su solución.

Ilustración 35. – *Pestaña Vulnerabilities - Advanced Scan*

En la pestaña "Remediations", se encuentran todas las posibles acciones que debemos tomar para gestionar la corrección de las vulnerabilidades en cada uno de los equipos.

Ilustración 36. Pestaña Remediations - Advanced Scan

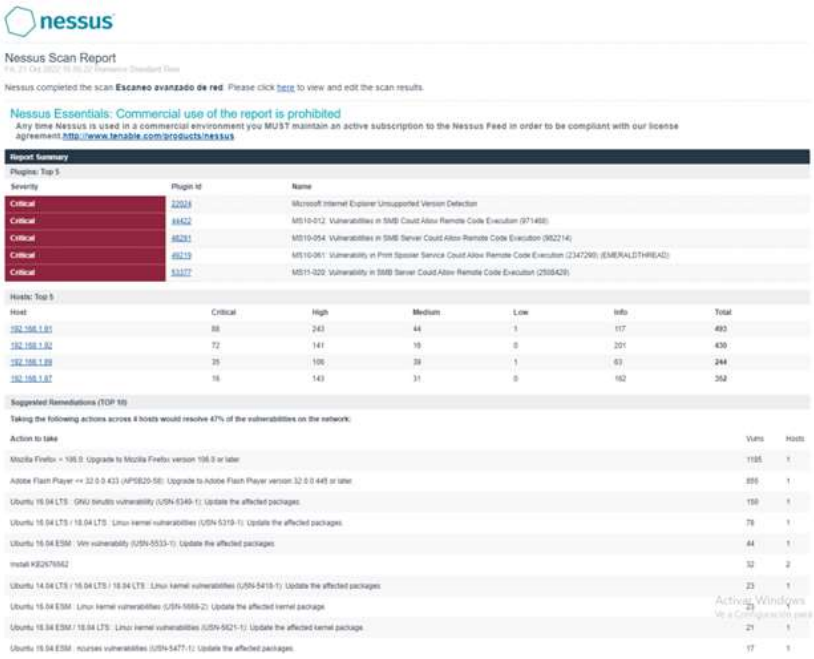


En la sección "VPR Top Threats", se muestra la clasificación de las vulnerabilidades según el sistema patentado de "Clasificación de Prioridad de Vulnerabilidades" (VPR) de Tenable. Cada vulnerabilidad incluye una guía que ayuda a evaluar el riesgo para nuestro sistema.

Ilustración 37. – Pestaña VPR - Advanced Scan

Dentro del correo electrónico, encontramos un resumen informativo del resultado del escaneo. En este resumen, se detalla el número de vulnerabilidades de cada tipo y el total por equipo. Además, se incluye un listado de las acciones que deben ser implementadas para mitigar las vulnerabilidades.

Ilustración 38. – informe al correo - Advanced Scan



4.3 Explotación de vulnerabilidades y análisis.

En esta parte analizaremos los resultados que se obtuvo anteriormente y explotaremos varias vulnerabilidades.

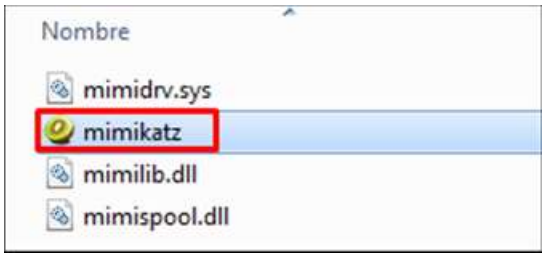
4.3.1 Mimikatz.

Uno de los principales problemas relacionados con Windows es tener habilitada la función WDigest para el almacenamiento de contraseñas, ya que esta guarda en todo momento una copia en texto plano de las contraseñas de los usuarios que están en el sistema. Aquí es donde se presenta la vulnerabilidad en el sistema. Luego de llevar a cabo el escaneo en un equipo con Windows 7, identificamos esta vulnerabilidad y dentro de la misma podemos acceder a información detallada sobre ella, así como un enlace a la página de Tenable con información adicional.

Ilustración 39. – WDigest

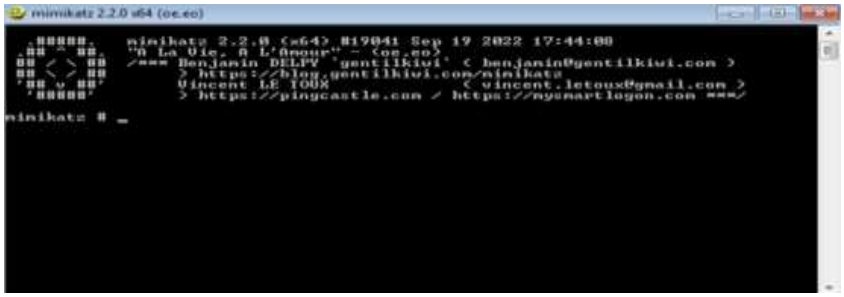
Después de confirmar la presencia de esta vulnerabilidad en el sistema, podemos proceder a utilizar Mimikatz para extraer las contraseñas de todos los usuarios que han sido creados en el equipo..

IIlustración 40.– mimikatz.exe



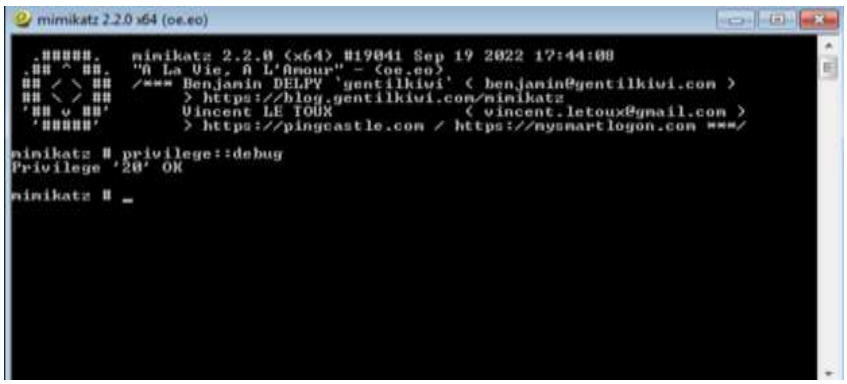
Luego de ejecutar el .exe se nos abre la terminal del exploit

Ilustración 41. – Terminal mimikatz



En este paso, enviamos el comando "privilege:debug" para verificar los privilegios disponibles en la terminal. Cuando recibimos la respuesta "Privilege "20" OK", confirma que hemos obtenido el control de la terminal y podemos continuar con la secuencia de comandos.

Ilustración 42. – comando privilege::debug



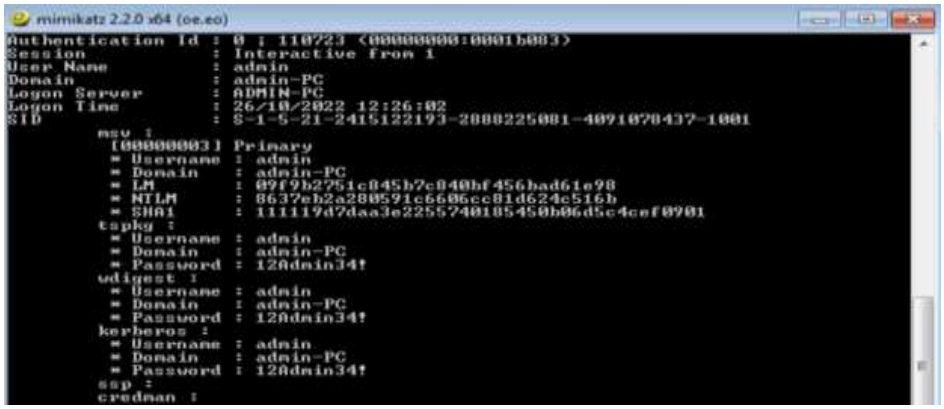
Enviamos el comando "sekurlsa:logonpasswords" con el fin de visualizar toda la información almacenada en la memoria, lo que incluye las contraseñas de todos los usuarios..

Ilustración 43. – comando sekurlsa::logonpasswords

Como resultado, se muestran las siguientes dos imágenes en las cuales podemos encontrar todos los detalles acerca de los usuarios registrados en el sistema, así como la información del equipo. Observamos que el equipo con Windows 7 tiene tres usuarios. El primero es el Administrador con la contraseña ‘admin’, el segundo es Juan con la contraseña ‘Juan1234’, ¡y el tercero es admin con la contraseña ‘12Admin34!'..

Ilustración 44. – información obtenida con Mimikatz

Ilustración 45. – información obtenida con Mimikatz



Al revisar los usuarios registrados en el equipo, podemos verificar de manera efectiva que existen tres usuarios y que cada uno de ellos está protegido con una contraseña.

Ilustración 46. – usuarios de W7

Así, con la asistencia de Nessus, hemos descubierto una vulnerabilidad en el sistema de Windows 7. Utilizando la información proporcionada, hemos confirmado la posibilidad de explotarla mediante Mimikatz, y al emplear esta herramienta, logramos aprovechar la vulnerabilidad y acceder a los nombres y contraseñas de todos los usuarios registrados en el equipo.

4.3.2 Reverse

El segundo problema fundamental se relaciona con la falta de actualizaciones en los equipos, lo cual crea una vulnerabilidad significativa en el sistema. En muchos casos, la ausencia de actualizaciones y de medidas de seguridad en los equipos resulta en que numerosos exploits o archivos maliciosos no sean detectados una vez que se descargan en el equipo. En nuestro caso, al revisar los resultados del escaneo de vulnerabilidades en el equipo con Windows 10, hemos identificado que presenta varias vulnerabilidades debido a la falta de actualizaciones de seguridad.

Ilustración 47. – Vulnerabilidades W10

Aprovecharemos estas vulnerabilidades para realizar un ataque de reversión en la máquina objetivo utilizando Metasploit. Para ello, configuraremos un oyente y crearemos un archivo malicioso que enviaremos a la máquina Windows 10, la cual actuará como cliente y se conectará a

nuestro oyente. De esta manera, obtendremos una shell interactiva que nos permitirá explorar la máquina objetivo y ejecutar código como atacantes.

Una gran ventaja de llevar a cabo un ataque de reversión es que Metasploit se ejecuta completamente en la memoria y no escribe ningún dato en el disco. Además, no crea nuevos procesos, sino que se inyecta en procesos comprometidos, desde donde toma el control de otros procesos en ejecución.

El primer paso consiste en ejecutar el siguiente comando para generar un archivo ejecutable llamado "Update.exe", el cual enviaremos a la víctima con el fin de obtener acceso completo al sistema y controlar la máquina.

Ilustración 48. – Generación de ejecutable

Una vez lanzado el comando, habremos creado el archivo malicioso que enviaremos al equipo víctima.

Ilustración 49. – Ejecutable

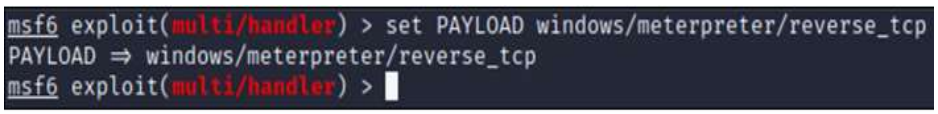
Nuestro siguiente paso implica abrir una consola de Metasploit. Para ello, ejecutaremos el comando 'msfconsole' en una terminal de Kali. Una vez

que la consola esté activa, introduciremos el siguiente comando para establecer el controlador de explotación que vamos a utilizar.

Ilustración 50. – Controlador de explotación

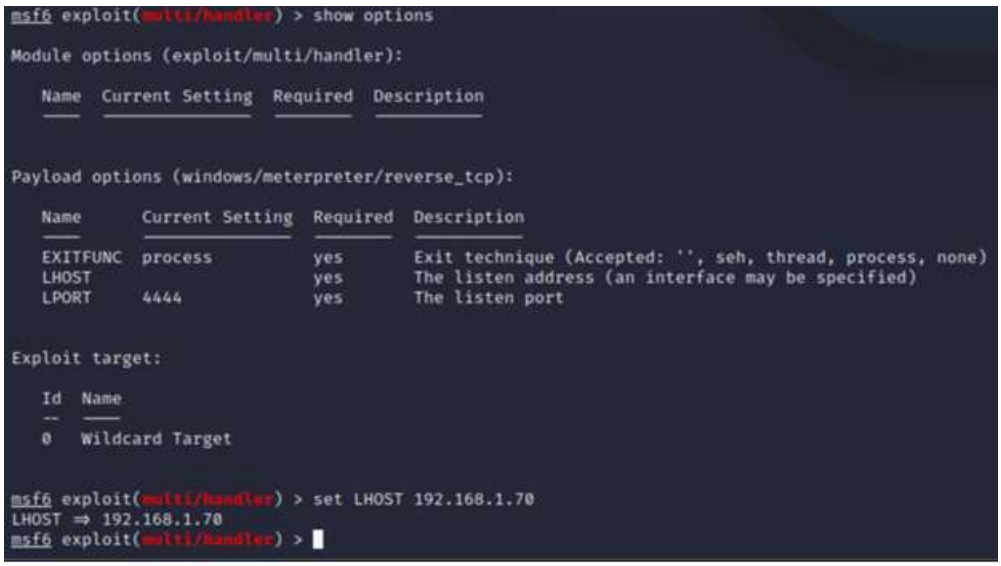
Después de haber configurado el controlador de explotación, continuaremos especificando el tipo de conexión que utilizaremos desde la máquina víctima hacia la máquina del atacante. Con este comando, nos aseguraremos de mantener una comunicación constante entre ambas máquinas en todo momento.

Ilustración 51. – Payload



Exponemos las opciones de meterpreter para verificar que únicamente debemos ingresar la dirección IP del equipo atacante. Establecemos la dirección del servidor atacante.

Ilustración 52. – Establecimiento de la IP del equipo atacante

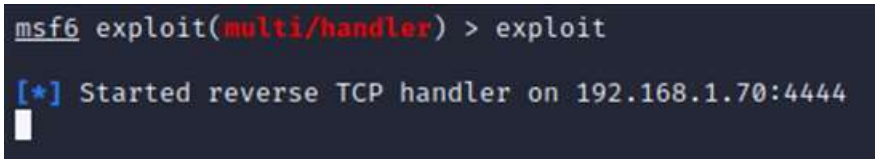


Luego se confirma que se ha establecido la IP del equipo atacante.

Ilustración 53. – Corroborar la correcta configuración

A continuación, ingresamos el siguiente comando para poner la máquina atacante en modo de escucha, esperando a que la máquina víctima ejecute el archivo creado.

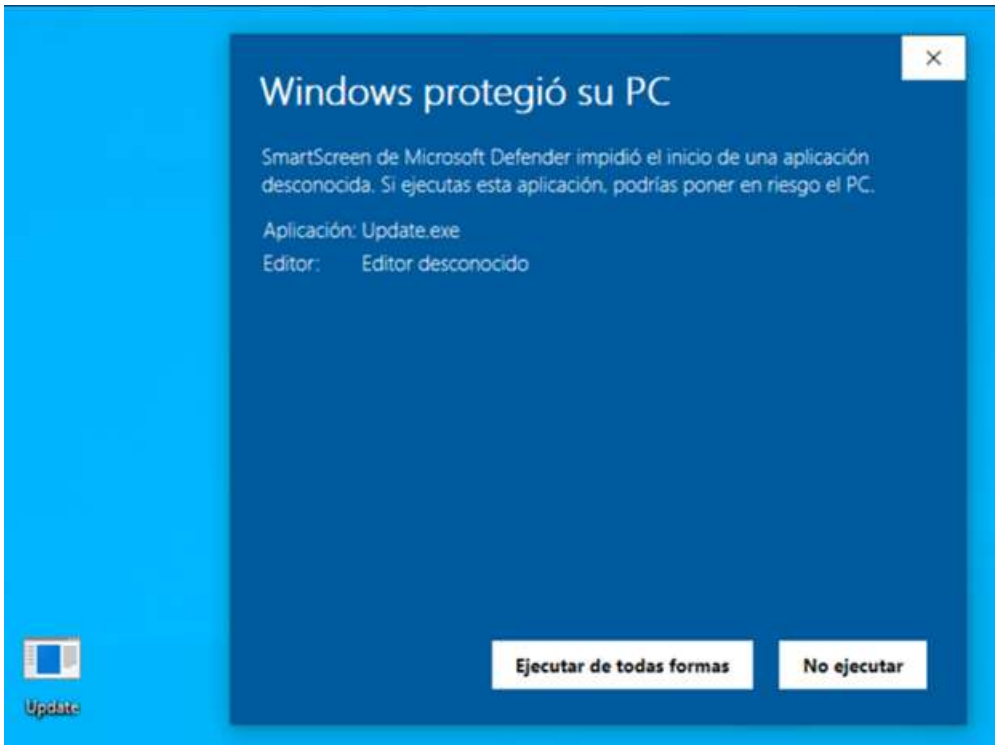
Ilustración 54. – Maquina atacante en escucha



Una vez concluido este procedimiento, habremos finalizado la creación y configuración de nuestro archivo malicioso. Luego, a través de la ingeniería social o tomando el control de otro equipo en la red mediante un ataque informático, enviaremos el archivo a la víctima para que lo ejecute.

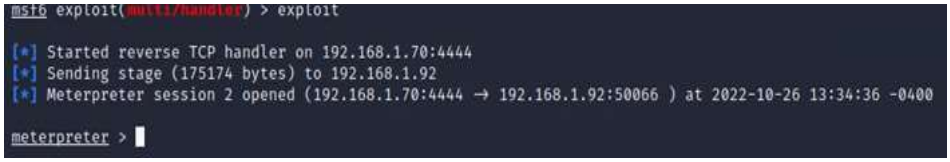
Como se puede apreciar, el archivo se descarga correctamente en el equipo y, al ejecutarlo, solo muestra un mensaje indicando que la procedencia del archivo es desconocida. Sin embargo, el sistema no lo bloquea ni lo identifica como un virus, lo que nos permite avanzar en el proceso.

Ilustración 55. – Ejecución del archivo malicioso



Después de que el archivo haya sido ejecutado en la máquina víctima, regresamos a la máquina atacante. Como se puede observar en la imagen siguiente, la máquina atacante ha iniciado exitosamente el proceso de reverse shell, lo que nos permite obtener una terminal shell de Windows desde la máquina Kali.

Ilustración 56. – Inicio de reverse

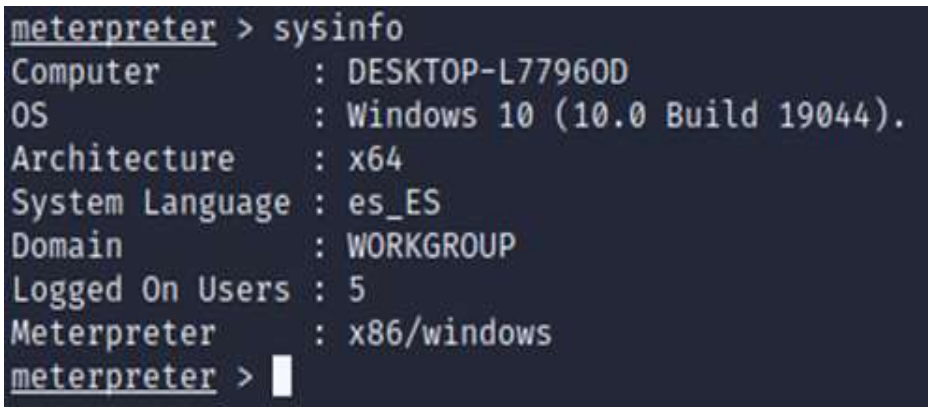


Ahora, al utilizar el comando "help", podemos visualizar una lista de todos los comandos disponibles para controlar la máquina víctima. Esta lista incluye una variedad de comandos de distintas categorías, como comandos genéricos para el manejo de Windows, manipulación de archivos, redes, sistemas, interfaces, cámaras web, audio, elevación de privilegios, bases de datos de contraseñas almacenadas y comandos relacionados con el timestomp.

Con esta amplia variedad de comandos y acceso a una terminal con privilegios de administrador, habremos logrado obtener el control total del equipo.

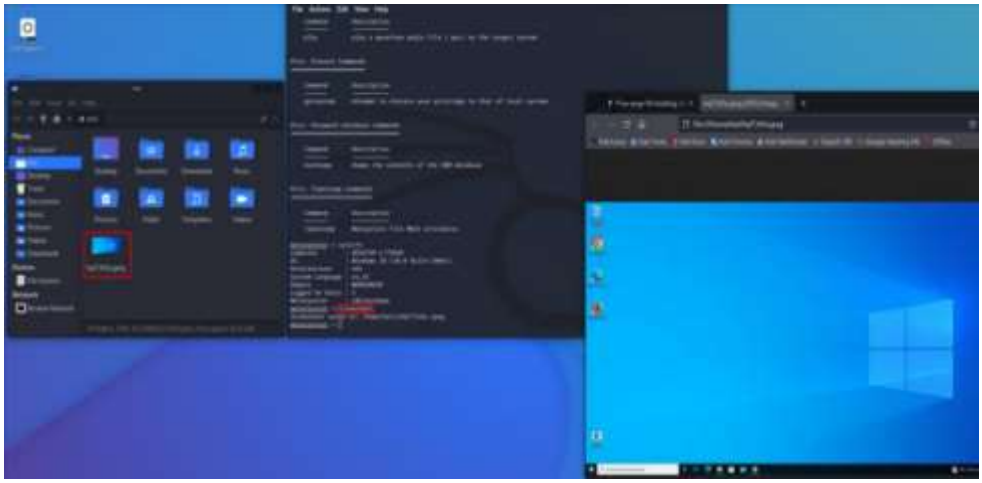
.

Ilustración 57. – comando sysinfo



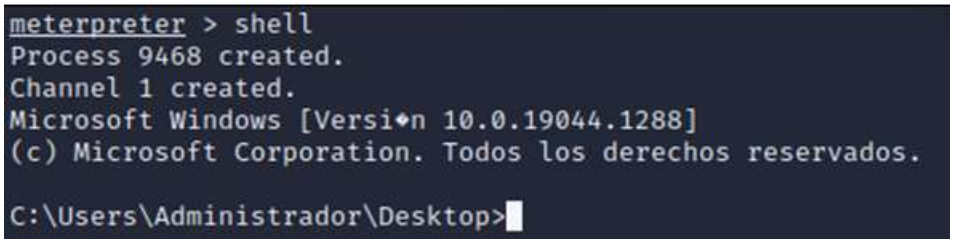
Un comando adicional que se puede emplear es "screenshot", que nos permite capturar la pantalla de la víctima y transferirla a nuestra máquina

Ilustración 58. – comando screenshot



Otro comando que se exploró es el que permite abrir una terminal de comandos (cmd) desde la máquina atacante, como se puede observar con el comando "shell". Esto nos proporciona acceso directo con el usuario administrador y control total con todos los privilegios.

Ilustración 59. – comando Shell



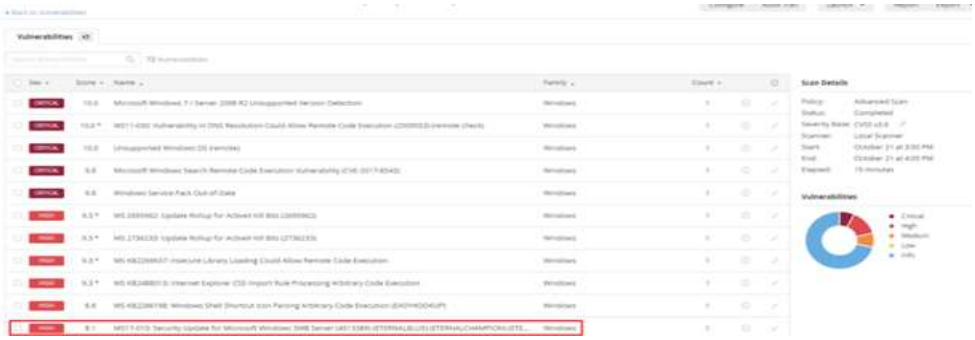
De este modo, hemos identificado varias vulnerabilidades en el sistema de Windows 10 utilizando Nessus. A través de la información recopilada, hemos comprobado que la falta de actualizaciones de seguridad en el sistema impide la detección de posibles ataques a través de archivos maliciosos. Además, al realizar un ataque de reversión mediante Metasploit, hemos logrado obtener un control total sobre el equipo.

4.3.3 EternalBlue

Como señalamos en el ataque anterior, una de las principales preocupaciones está relacionada con la falta de actualizaciones de seguridad. En esta sección, abordaremos los desafíos que surgen de la ausencia de actualizaciones de seguridad y el uso de un sistema operativo sin soporte.

Al utilizar Nessus y llevar a cabo un escaneo en un sistema con Windows 7 como sistema operativo, hemos identificado una vulnerabilidad conocida que podría ser objeto de explotación.

Ilustración 60. – Vulnerabilidad CVE-2017-0144



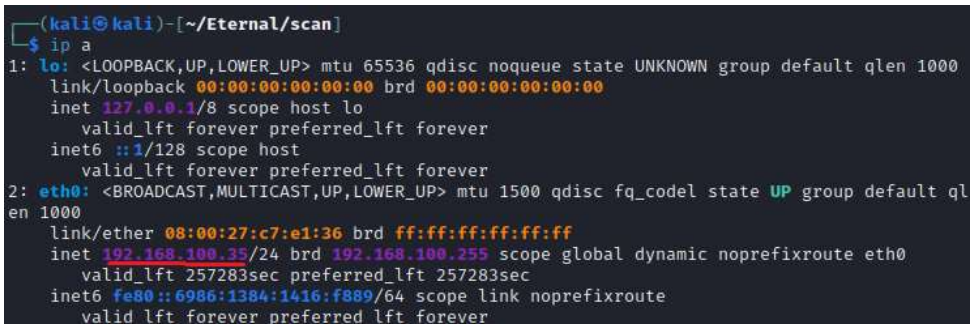
De acuerdo con la información presentada en la imagen adjunta, se puede notar que esta vulnerabilidad posee un nivel de riesgo significativo y es susceptible de ser aprovechada mediante Metasploit. Además, tanto la descripción como los enlaces proporcionados indican que esta vulnerabilidad en el sistema permite que un atacante cibernético ejecute de forma remota código malicioso en la computadora de la víctima sin ser detectado.

Ilustración 61. – Información de la vulnerabilidad CVE-2017-0144

Esta vulnerabilidad, en conjunto con su exploit, se hizo ampliamente reconocida debido a la facilidad con la que puede ser aprovechada y a la falta de correcciones disponibles en el sistema. En un momento posterior, Microsoft emitió una actualización de seguridad, denominada MS17-010, pero esta actualización solo estuvo disponible para determinadas versiones de Windows 7.

Reviso cual es mi ip con el comando ip a.

Ilustración 62. – Información de la ip para atacar



Luego hago un escaneo de la red para verificar cual es la ip para atacar a la máquina y ver cúal está dentro del segmento con mi ip , con el comando

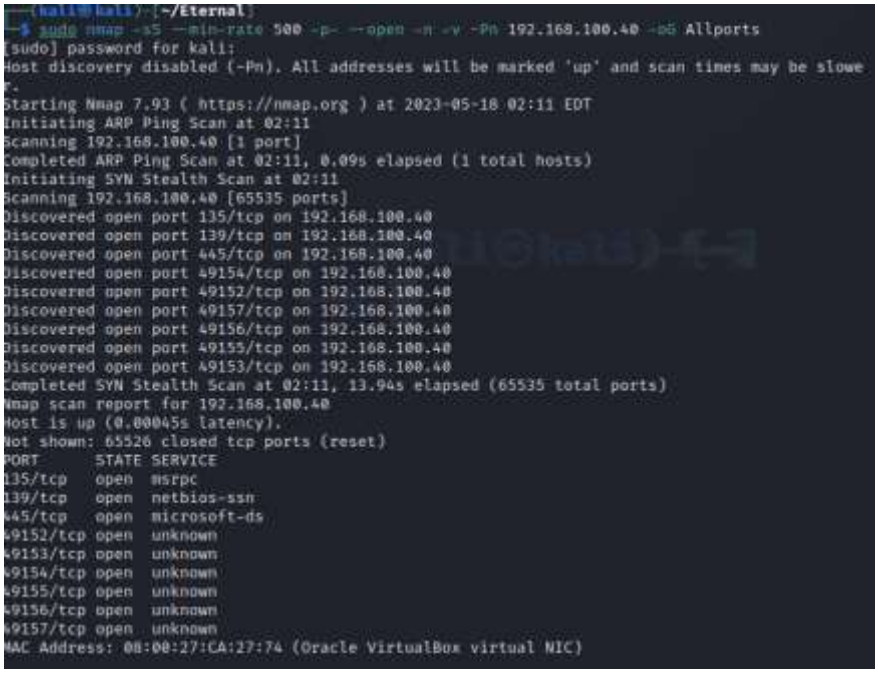
Sudo arp -scan -l

Ilustración 63. – Ip identificada para el ataque

Hago un escaneo de los puertos sobre la dirección ip objetivo y que me lo de en archivo tambien, adicional que trate a los puertos todos online y abiertos, tambien que sea grepeable con los siguietes comandos:

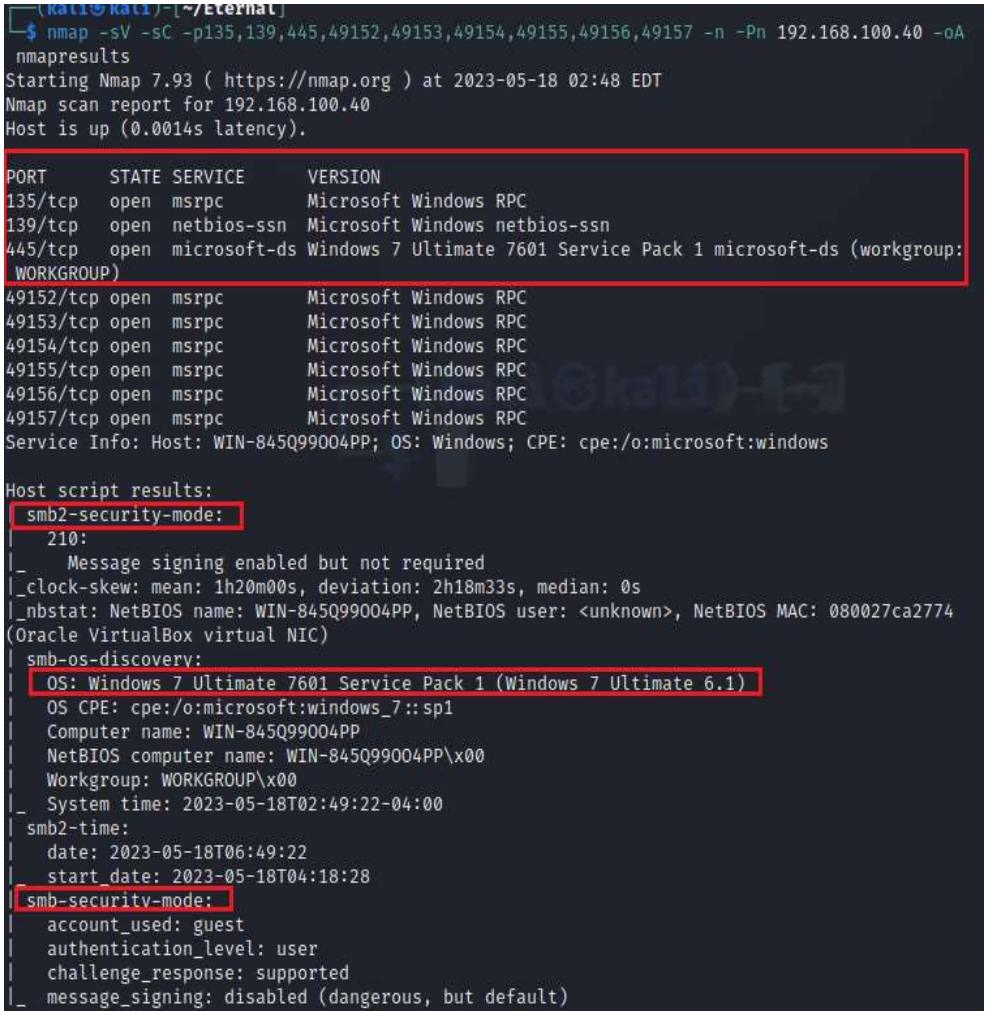
$ sudo nmap -sS --min-rate 500 -p- --open -n -v -Pn 192.168.100.40 -oG Allports

Ilustración 64. – Información de puertos abiertos



Como vemos en la figura anterior vemos que los puertos 135, 139, 145 están abiertos y con servicios podemos ver que mas se puede ver si tienen alguna versión adicional o algo con el siguiente comando: nmap -sv -sc -p 135, 139.

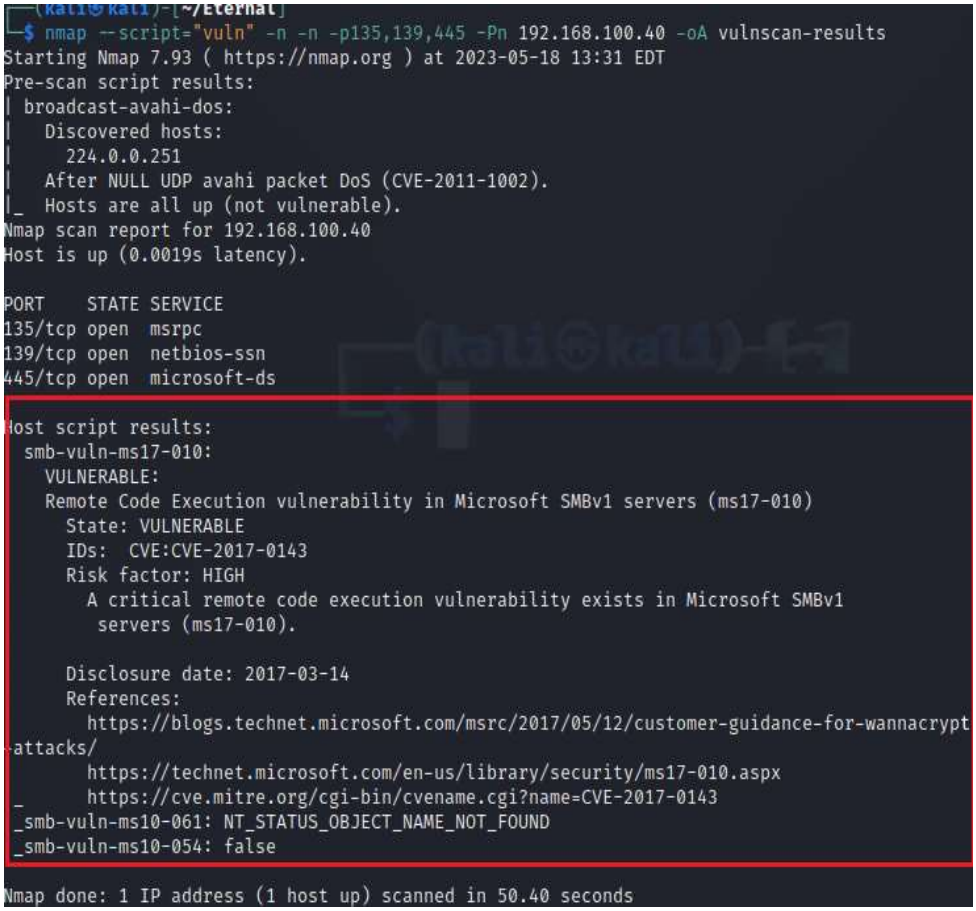
Ilustración 65. – Identificación del puerto para atacar



Buscamos alguna vulnerabilidad escaneando con nmap con los scripts de default de kali con Vuln a los puertos abiertos que descubrimos anteriormente con versiones, en la cual encontramos una vulnerabilidad de servidor SMB con escalada de privilegios, con el CVE-2017-0143. usamos el siguiente codigo:

nmap --script="vuln" -n -n -p135,139,445 -Pn 192.168.100.40 -oA vulnscan-results

Ilustración 66. – Información de la ip vulnerable

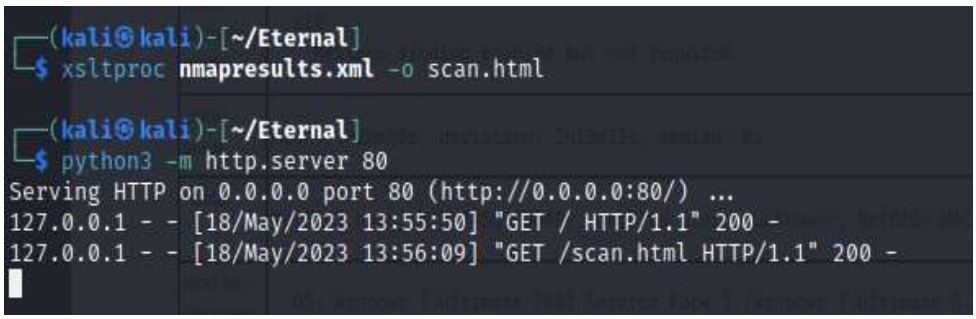


Leemos con comandos de: xsltproc nmapresults.xml -o scan.html para leerlo de mejor manera alzamos un servidor con python3 -m http. server 80.

xsltproc nmapresults.xml -o scan.html

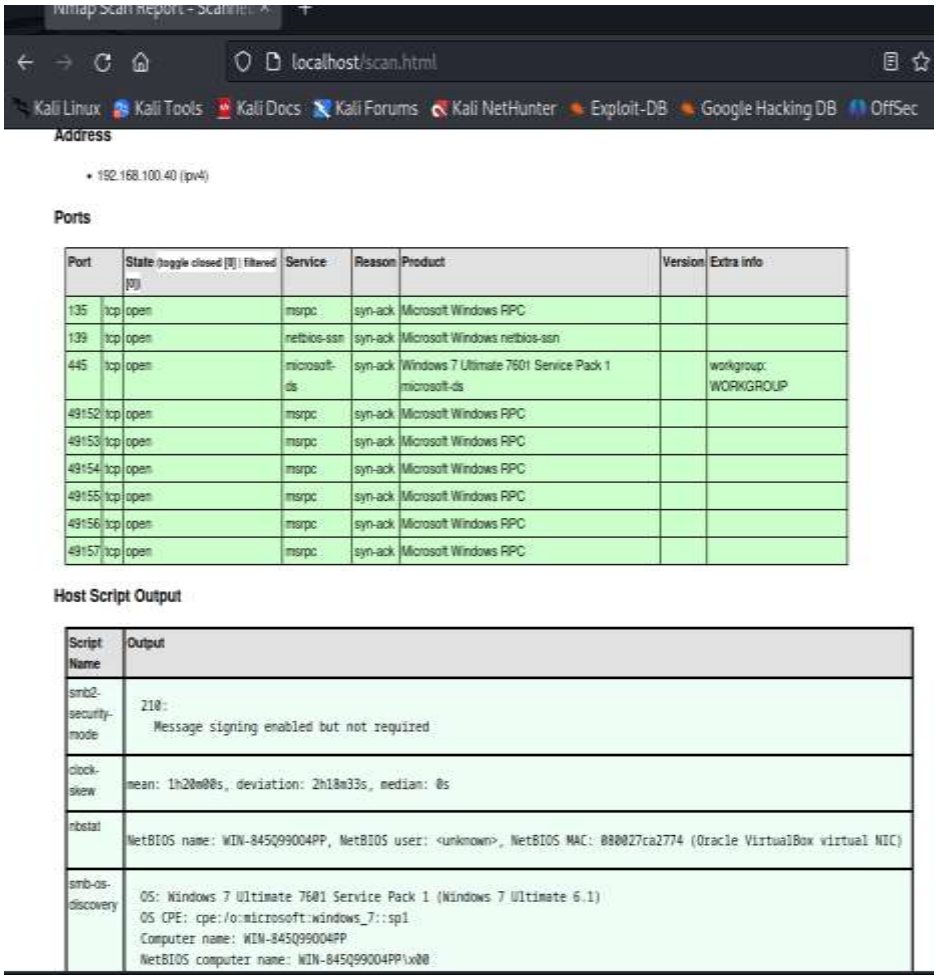
python3 -m http. Server 80

Ilustración 67. – Creación de un servidor con Python 3 en Kali



Podemos observar de mejor manera leyendo la imagen del escaneo y la clase de la vulnerabilidad.

Ilustración 68. – Reporte de la Ip para atacar

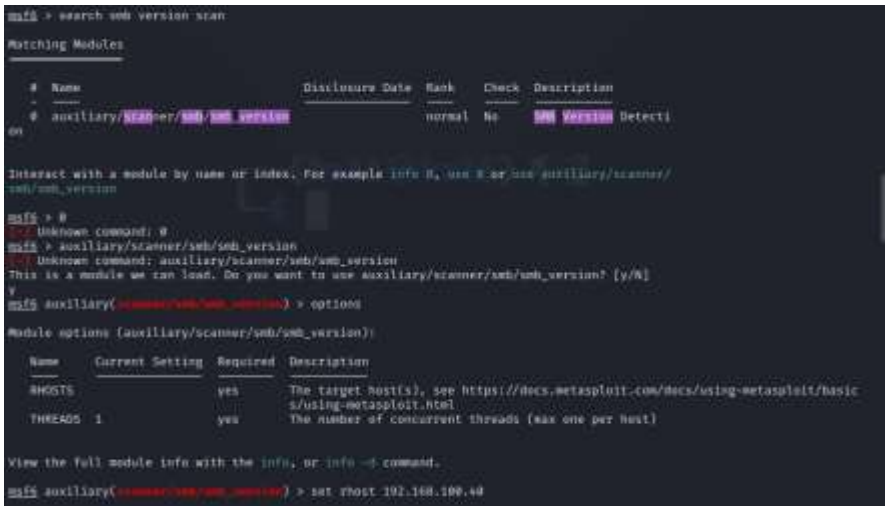


Usamos el msfconsole para poder buscar alguna vulnerabilidad referente al servidor que se presentó ante.

Ilustración 69. – metasploit

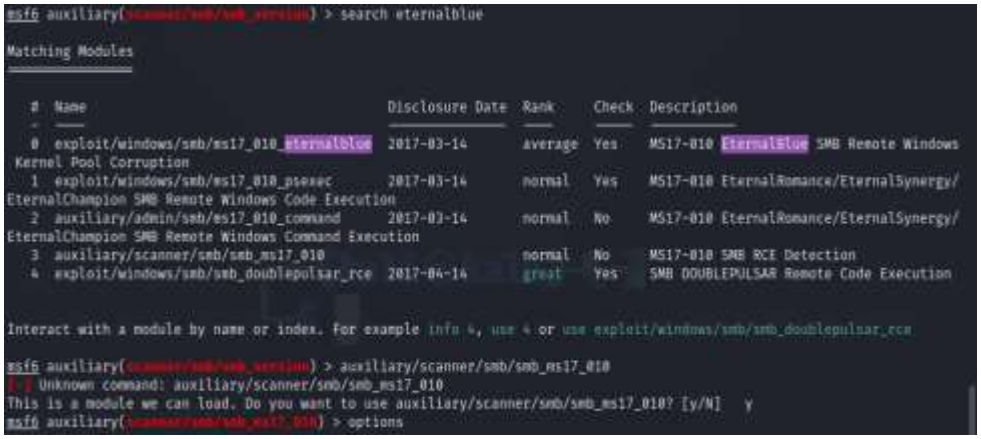
Usamos y configuramos el host y el remote luego de entrar al msfconsole

Ilustración 70. – Versión de la falla de samba



Luego escribimos para atacar al eternal blue que fue lo que nos comunicó la vulnerabilidad

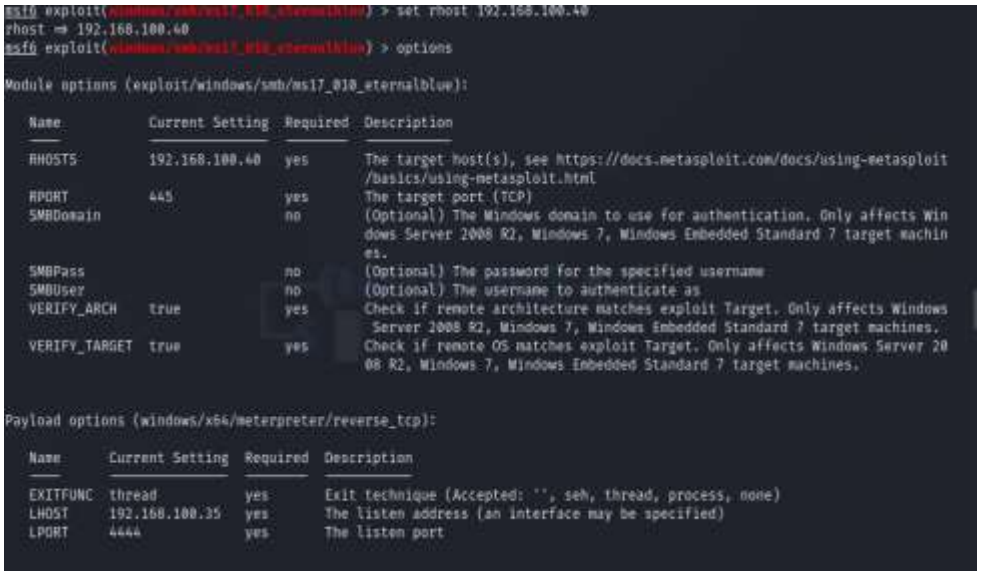
Ilustración 71.– Información de eternalblue de smb remote Windows.



.

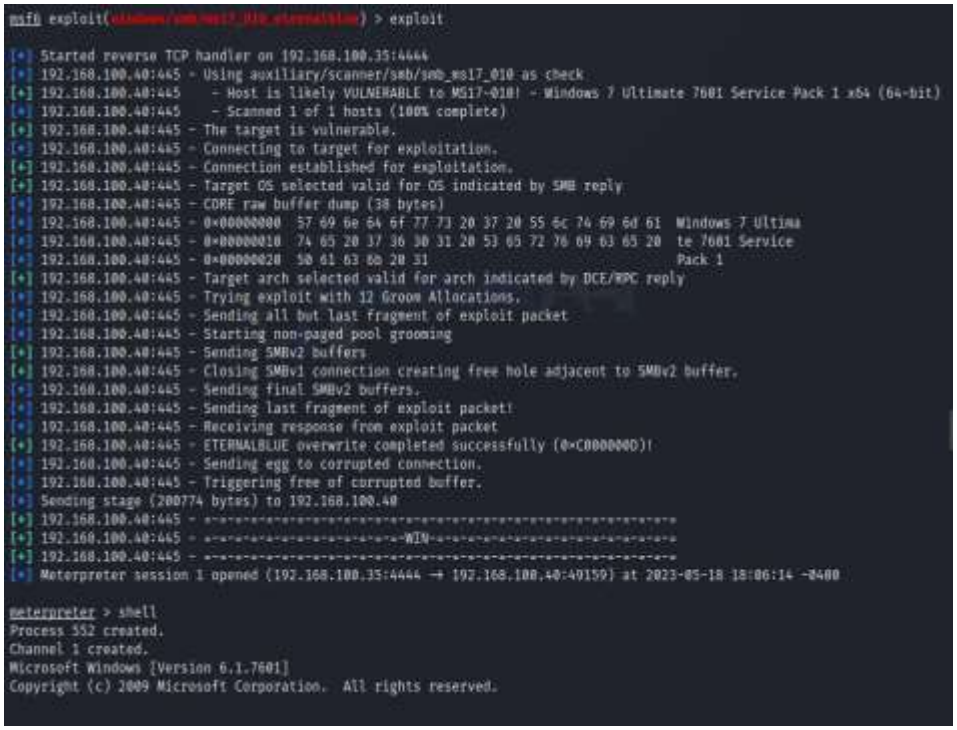
Verificamos que este bien configurado el local host y remote host con la respectiva ip.

Ilustración 72. – configuración de la ip atacante y la ip victima



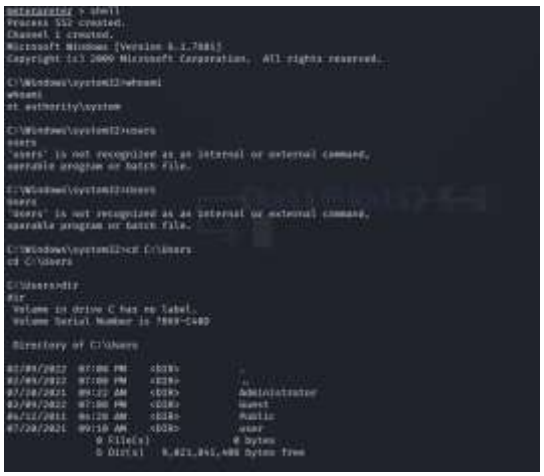
Escribimos exploit y verificamos que ya fue vulnerado el sistema y pudimos ingresar, luego podemos usar la Shell para encontrar las banderas escondidas en los directorios de la máquina

Ilustración 73. – exploit



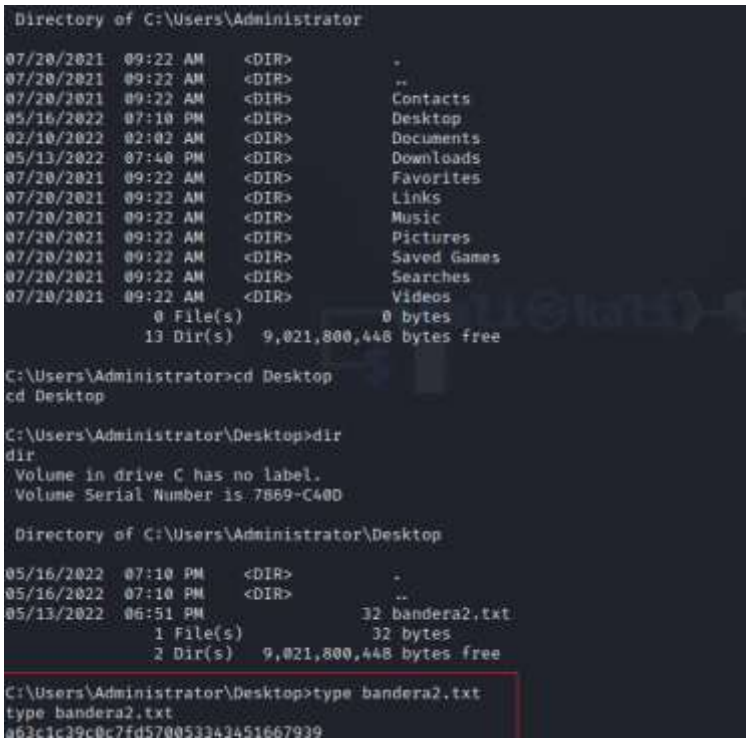
Luego que entramos en la Shell de la máquina podemos ver en que directorio estamos con whoami, para después buscar las banderas.

Ilustración 74. – whoami



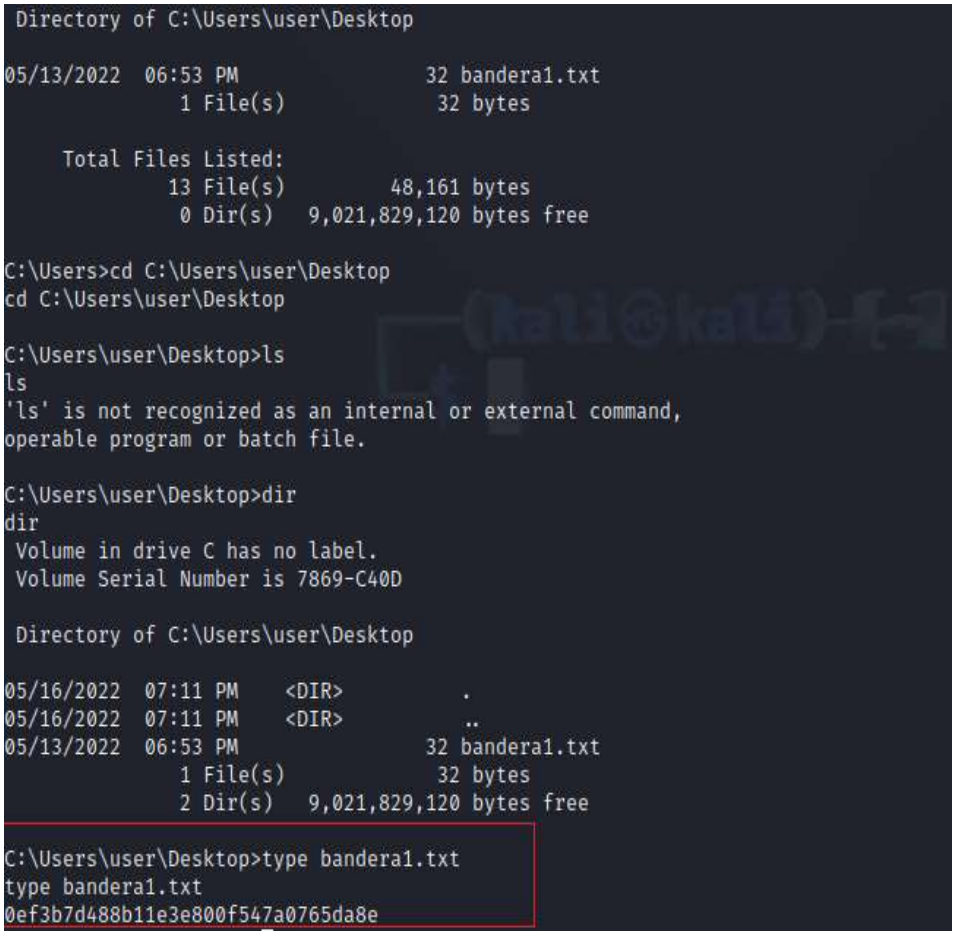
Luego de movernos por los directorios pudimos encontrar la primera bandera con extensión.txt y lo leemos con type como lo muestra la siguiente figura.

Ilustración 75. – Encontrando bandera



Por último, nos quedaría encontrar la siguiente bandera nos movemos a Users, para eso acudimos a Bing con la búsqueda de inteligencia artificial para que me dé un comando en la cual pueda encontrar archivos .txt en todo el sistema y no estar entrando en cada uno de las carpetas y subcarpetas para que al final mostrar la bandera faltante.

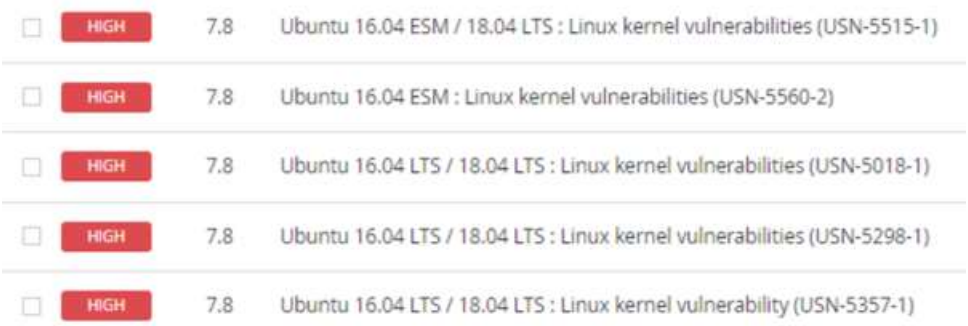
Ilustración 76. – Lectura de un archivo de la maquina víctima.



4.3.4 Escalada de privilegios.

Una táctica común cuando se logra acceso a un sistema con un usuario sin privilegios es llevar a cabo una búsqueda exhaustiva de vulnerabilidades y debilidades en el sistema que permitan obtener privilegios más elevados para conseguir el control completo del sistema. A través de la explotación de vulnerabilidades en diversos sistemas, se avanza gradualmente a través de la red, aumentando los privilegios paso a paso hasta alcanzar un usuario con control total en el sistema deseado.

Ilustración 77. – Vulnerabilidades del kernel de Linux



Es evidente que existe información sobre vulnerabilidades que presentan un alto grado de riesgo y que son susceptibles de ser aprovechadas mediante diversas técnicas de escalada de privilegios.

.

Ilustración 78. – Información de la vulnerabilidad del kernel

Para explotar estas vulnerabilidades, ejecutamos el siguiente comando para verificar la versión del kernel en nuestra máquina Linux.

Ilustración 79.– kernel de la maquina victima

```
sergio@equipo:~/Descargas/39772/ebpf_mapfd_doubleput_exploit$ uname -a
Linux equipo 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64
 x86_64 x86_64 GNU/Linux
```

Después de confirmar la versión de kernel que estamos utilizando, procedemos a buscar un exploit específico para esa versión que nos permita elevar los privilegios de nuestro usuario sin permisos.

En la siguiente pagina podemos encontrar, URL del exploit: https://www.exploit-db.com/exploits/39772

Ilustración 80. – página de exploit db

Lo primero es descargar y descomprimir el exploit en la maquina víctima.

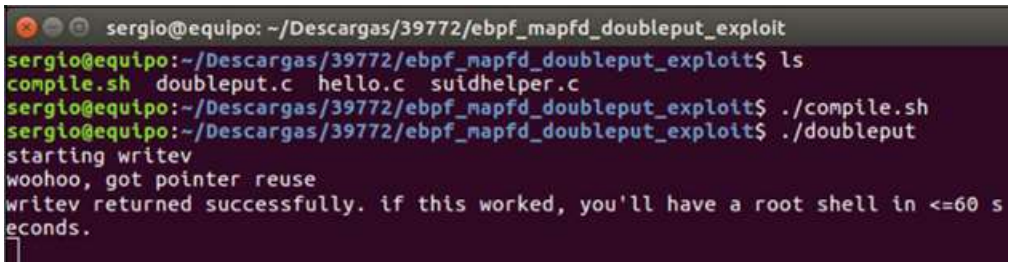
Ilustración 81. – Descarga del exploit

Archivos dentro de la carpeta que se descargó, la descomprimimos

Ilustración 82. – Archivos del exploit

Una vez que hemos extraído los archivos, compilamos y ejecutamos el script del exploit, después esperamos un momento hasta que se complete su ejecución.

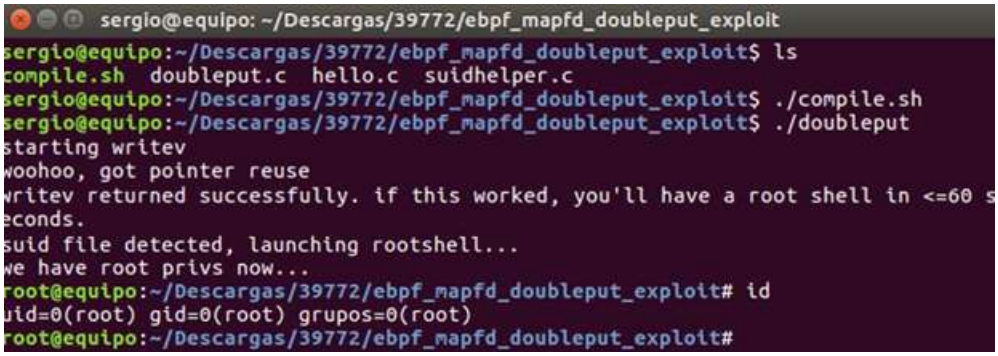
Ilustración 83. – Compilado y ejecución del exploit



Después de que el proceso haya finalizado, se realizará automáticamente un cambio de usuario a "root" con plenos privilegios en el sistema.

.

Ilustración 84. – Escalada de privilegios a root



Así, mediante el uso de Nessus, hemos identificado varias vulnerabilidades en el sistema Linux, gracias a la información proporcionada, hemos determinado que estas vulnerabilidades son susceptibles de ser explotadas tanto con Metasploit como con distintos exploits independientes para la escalada de privilegios. A través del uso de un exploit específico, hemos logrado llevar a cabo la escalada de privilegios, cambiando nuestro usuario a root y obteniendo así el control total del equipo.

4.4 Parches para mitigación de vulnerabilidades.

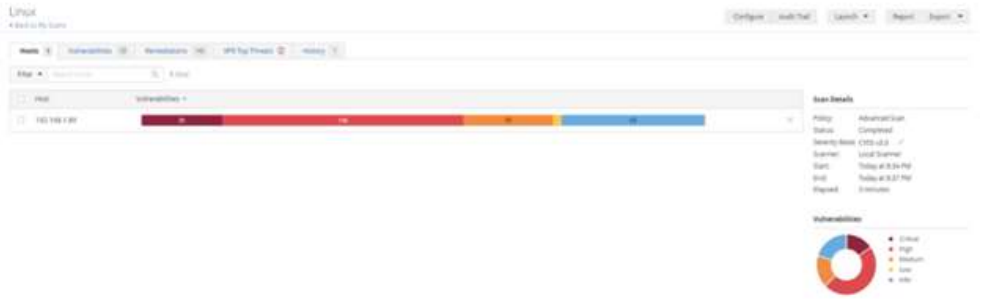
En esta sección, procederemos a identificar las vulnerabilidades que se encuentran en los dispositivos del entorno y nos esforzaremos por remediar todas las posibles. Normalmente, para abordar estas vulnerabilidades, se implementan actualizaciones del sistema, se realizan ajustes en la configuración o se actualiza el software vulnerable.

Una vez que hayamos aplicado los parches necesarios para solucionar las vulnerabilidades, efectuaremos un nuevo escaneo para asegurarnos de que estas hayan sido corregidas. Asimismo, destacaremos la notable diferencia y la relevancia de contar con un sistema operativo que continúe recibiendo soporte en comparación con uno que ya no lo tenga.

4.4.1 Ubuntu

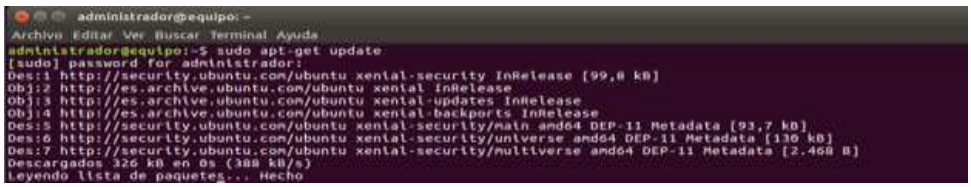
Vamos a aplicar parches al primer equipo que utiliza Ubuntu. Este equipo presenta las siguientes vulnerabilidades.

Ilustración 85. – Vulnerabilidades Ubuntu



Comenzaremos por ingresar el siguiente comando para actualizar la lista de paquetes disponibles en este momento.

Ilustración 86. – comando Update

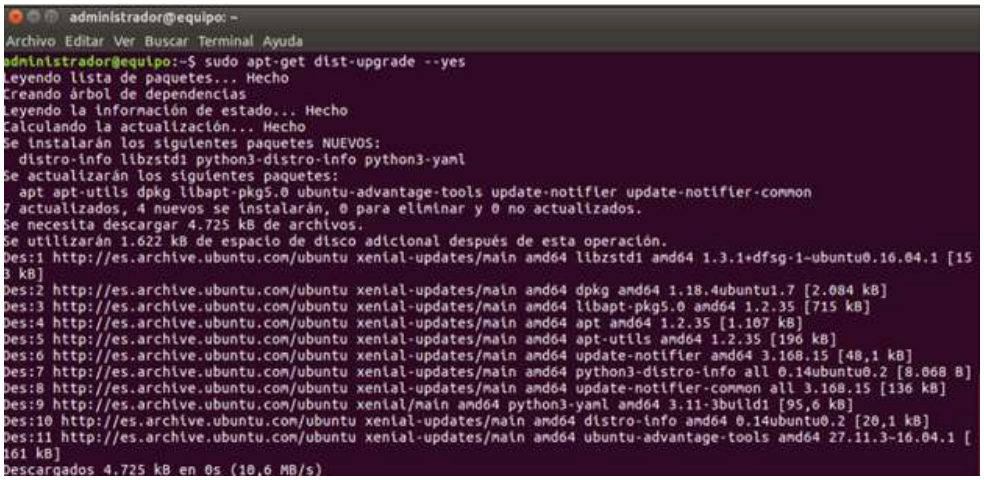


Luego, ejecutaremos el siguiente comando para proceder a actualizar los paquetes disponibles..

Ilustración 87.– *Comando Upgrade*

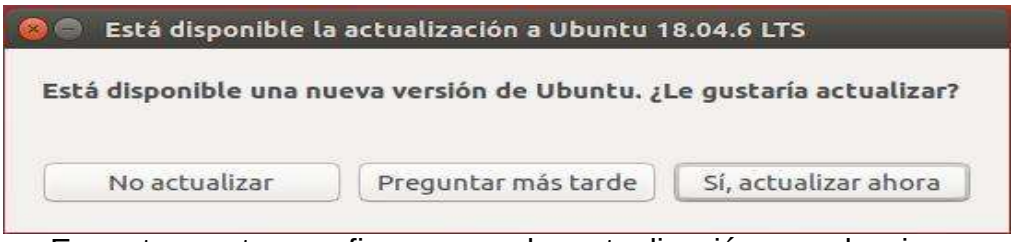
Luego, procederemos a ejecutar el siguiente comando para instalar los paquetes que aún no estén presentes en el sistema y para eliminar de manera automática los paquetes obsoletos que puedan estar presentes.

Ilustración 88. – comando dist-upgrade



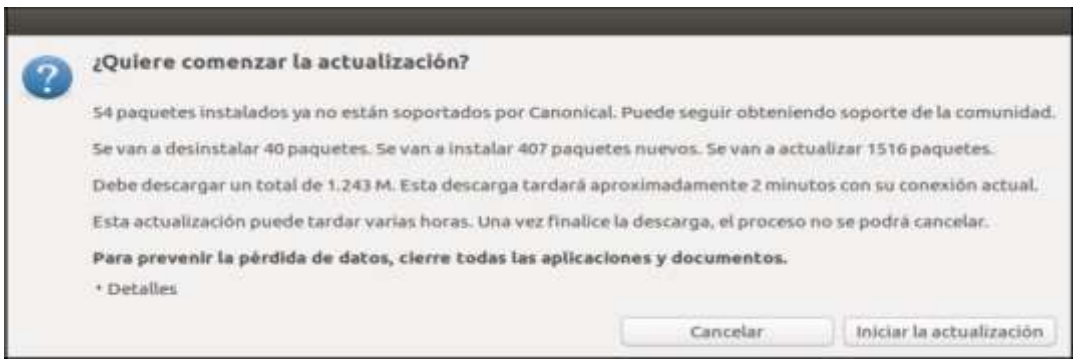
Una vez que se hayan descargado y actualizado todos los paquetes en el equipo, recibiremos una notificación que indica la disponibilidad de una nueva versión del sistema operativo.

Ilustración 89.– actualización ubuntu



En este punto, confirmaremos la actualización y seleccionaremos "Iniciar la actualización" cuando se nos solicite.

Ilustración 90. – inicio actualización Ubuntu

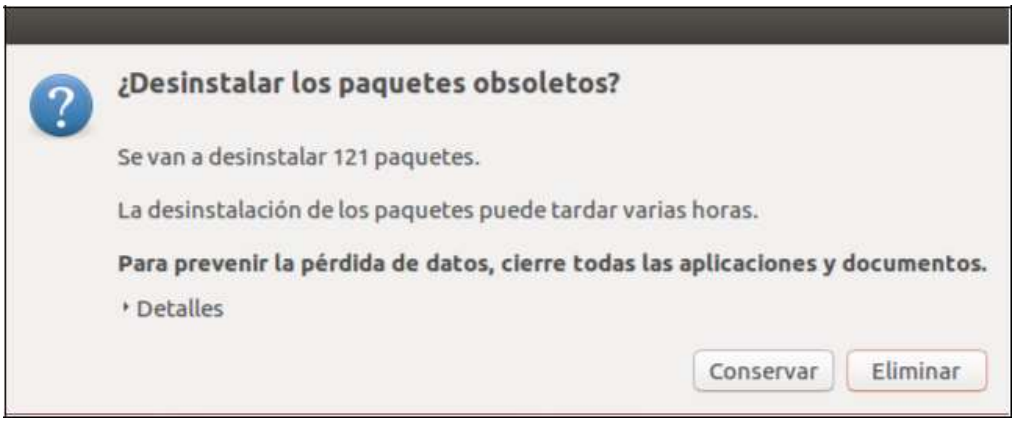


Luego, simplemente esperaremos a que el proceso de actualización de nuestro sistema operativo se complete.

Ilustración 91.– Progreso de la actualización

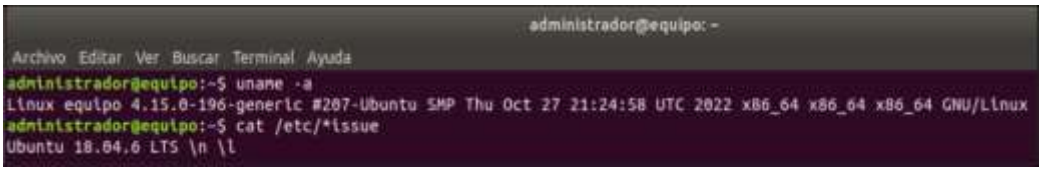
Durante este proceso, es posible que el sistema nos consulte si deseamos eliminar los paquetes obsoletos, y en ese caso, seleccionaremos la opción para eliminarlos.

Ilustración 92. – Eliminar paquetes obsoletos



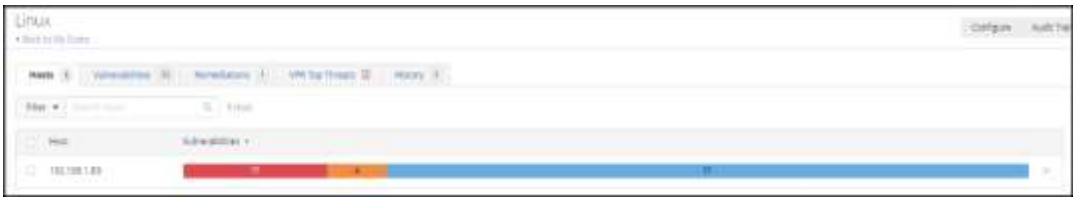
Una vez finalizada la instalación de la actualización del sistema, aparecerá un mensaje indicándonos que reiniciemos la computadora. Posteriormente, ejecutamos los comandos especificados para verificar la versión actual del kernel y asegurarnos de que el sistema haya realizado la transición exitosa de la versión 16.04 a la 18.04.

Ilustración 93. – comandos de versión



Después de confirmar la versión del sistema, nuestro siguiente paso es realizar un nuevo análisis de la computadora.

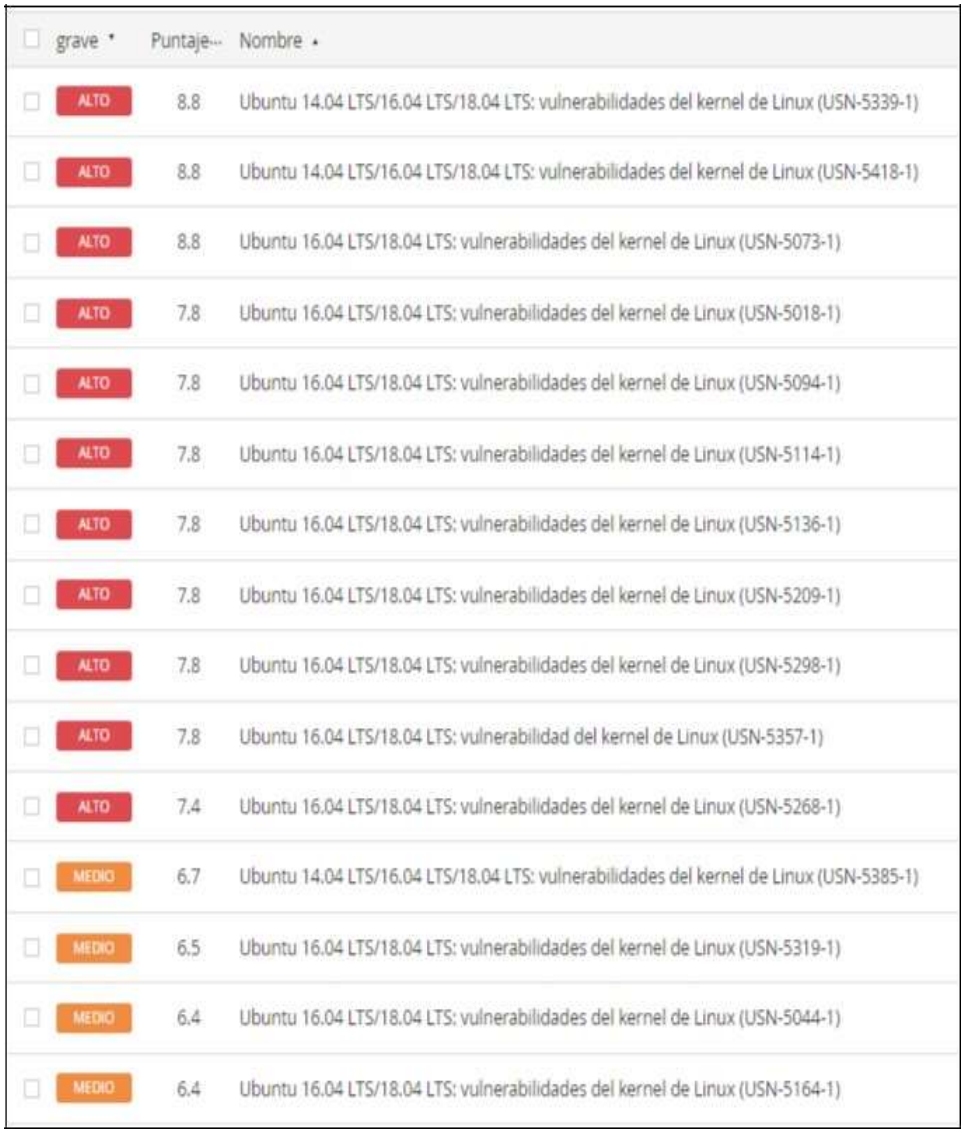
Ilustración 94. – 2º Escaneo de Vulnerabilidades Ubuntu



Tras examinar el último escaneo, es evidente que ha habido una disminución en la cantidad de vulnerabilidades que anteriormente afectaban a la computadora. En el futuro, nuestro enfoque se centrará en evaluar las vulnerabilidades que aún persisten.

.

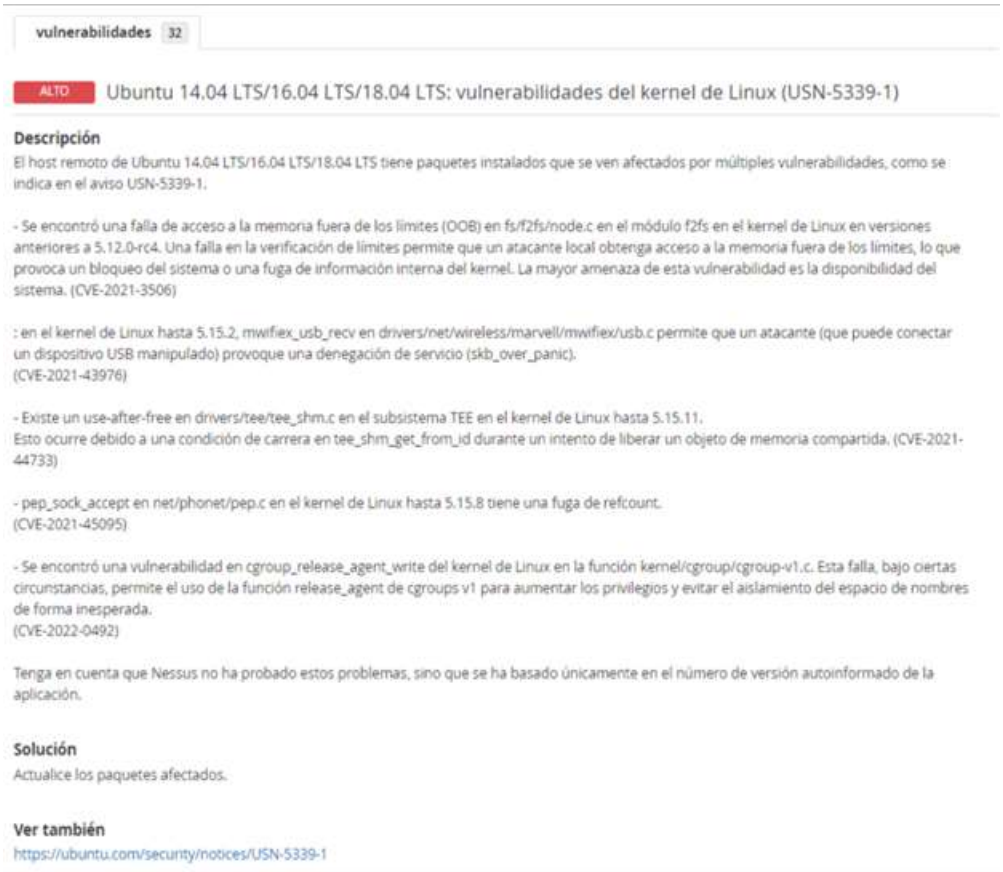
Ilustración 95. – Listado de vulnerabilidades Ubuntu



grave	Puntaje...	Nombre
ALTO	8.8	Ubuntu 14.04 LTS/16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5339-1)
ALTO	8.8	Ubuntu 14.04 LTS/16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5418-1)
ALTO	8.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5073-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5018-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5094-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5114-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5136-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5209-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5298-1)
ALTO	7.8	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidad del kernel de Linux (USN-5357-1)
ALTO	7.4	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5268-1)
MEDIO	6.7	Ubuntu 14.04 LTS/16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5385-1)
MEDIO	6.5	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5319-1)
MEDIO	6.4	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5044-1)
MEDIO	6.4	Ubuntu 16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5164-1)

Según los datos presentados en la imagen, está claro que las vulnerabilidades restantes están directamente relacionadas con la ausencia de una actualización del kernel. Para resolver eficazmente estas vulnerabilidades, se recomienda encarecidamente realizar una actualización del kernel.

Ilustración 96. – Información sobre las vulnerabilidades del Kernel



vulnerabilidades 32

ALTO Ubuntu 14.04 LTS/16.04 LTS/18.04 LTS: vulnerabilidades del kernel de Linux (USN-5339-1)

Descripción

El host remoto de Ubuntu 14.04 LTS/16.04 LTS/18.04 LTS tiene paquetes instalados que se ven afectados por múltiples vulnerabilidades, como se indica en el aviso USN-5339-1.

- Se encontró una falla de acceso a la memoria fuera de los límites (OOB) en fs/f2fs/node.c en el módulo f2fs en el kernel de Linux en versiones anteriores a 5.12.0-rc4. Una falla en la verificación de límites permite que un atacante local obtenga acceso a la memoria fuera de los límites, lo que provoca un bloqueo del sistema o una fuga de información interna del kernel. La mayor amenaza de esta vulnerabilidad es la disponibilidad del sistema. (CVE-2021-3506)

: en el kernel de Linux hasta 5.15.2, mwifiex_usb_recv en drivers/net/wireless/marvell/mwifiex/usb.c permite que un atacante (que puede conectar un dispositivo USB manipulado) provoque una denegación de servicio (skb_over_panic).
(CVE-2021-43976)

- Existe un use-after-free en drivers/tee/tee_shm.c en el subsistema TEE en el kernel de Linux hasta 5.15.11.
Esto ocurre debido a una condición de carrera en tee_shm_get_from_id durante un intento de liberar un objeto de memoria compartida. (CVE-2021-44733)

- pep_sock_accept en net/phonet/pep.c en el kernel de Linux hasta 5.15.8 tiene una fuga de refcount.
(CVE-2021-45095)

- Se encontró una vulnerabilidad en cgroup_release_agent_write del kernel de Linux en la función kernel/cgroup/cgroup-v1.c. Esta falla, bajo ciertas circunstancias, permite el uso de la función release_agent de cgroups v1 para aumentar los privilegios y evitar el aislamiento del espacio de nombres de forma inesperada.
(CVE-2022-0492)

Tenga en cuenta que Nessus no ha probado estos problemas, sino que se ha basado únicamente en el número de versión autoinformado de la aplicación.

Solución

Actualice los paquetes afectados.

Ver también

https://ubuntu.com/security/notices/USN-5339-1

Ejecutamos el siguiente comando con el fin de proceder a actualizar el kernel..

Ilustración 97. – Comando actualización de Kernel

```
administrador@equipo:~$ sudo apt-get install --install-recommends linux-generic-hwe-18.04 xserver-xorg-hwe-18.04
[sudo] contraseña para administrador:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  linux-headers-5.4.0-131-generic linux-headers-generic-hwe-18.04 linux-hwe-5.4-headers-5.4.0-131
  linux-image-5.4.0-131-generic linux-image-generic-hwe-18.04 linux-modules-5.4.0-131-generic
  linux-modules-extra-5.4.0-131-generic xserver-xorg-core-hwe-18.04 xserver-xorg-input-all-hwe-18.04
  xserver-xorg-input-libinput-hwe-18.04 xserver-xorg-legacy-hwe-18.04 xserver-xorg-video-all-hwe-18.04
  xserver-xorg-video-amdgpu-hwe-18.04 xserver-xorg-video-ati-hwe-18.04 xserver-xorg-video-fbdev-hwe-18.04
  xserver-xorg-video-intel-hwe-18.04 xserver-xorg-video-nouveau-hwe-18.04 xserver-xorg-video-qxl-hwe-18.04
  xserver-xorg-video-radeon-hwe-18.04 xserver-xorg-video-vesa-hwe-18.04 xserver-xorg-video-vmware-hwe-18.04
Paquetes sugeridos:
  fdutils linux-hwe-5.4-doc-5.4.0 | linux-hwe-5.4-source-5.4.0 linux-hwe-5.4-tools xfonts-100dpi | xfonts-75dpi
  firmware-amd-graphics xserver-xorg-video-r128 xserver-xorg-video-mach64 firmware-misc-nonfree
Paquetes recomendados:
```

Después de completar con éxito la actualización del kernel, el siguiente paso es reiniciar el sistema y utilizar comandos adicionales para verificar la versión actual del sistema y asegurarse de que el kernel se haya actualizado a una versión más reciente.

Ilustración 98. – comandos de versión

Después de actualizar el kernel, procedemos con un escaneo posterior y, como se muestra en la imagen proporcionada, hemos erradicado de manera efectiva todas las vulnerabilidades Criticas.

Ilustración 99. – Escaneo de Vulnerabilidades Ubuntu

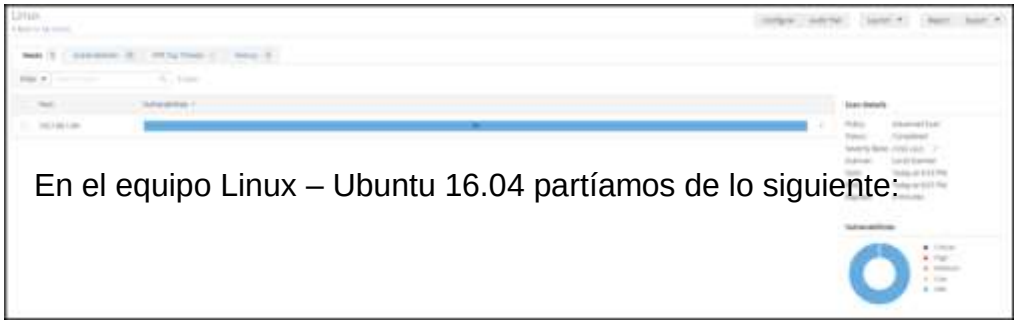


Ilustración 100. – Primer escaneo – Ubuntu

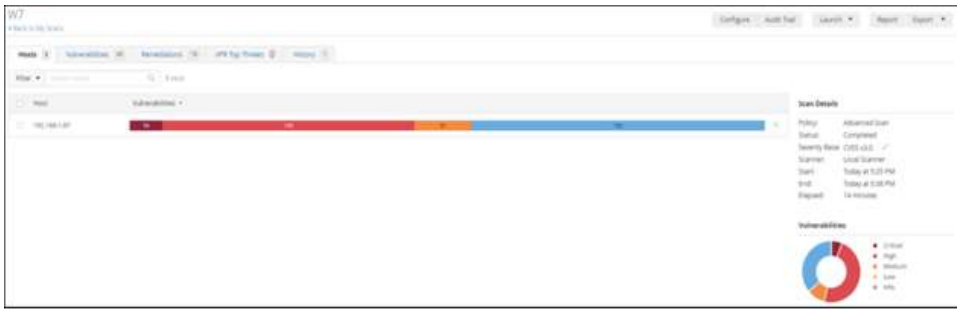
Y hemos terminado así:

Ilustración 101. – Último escaneo – Ubuntu

4.4.2 Windows 7

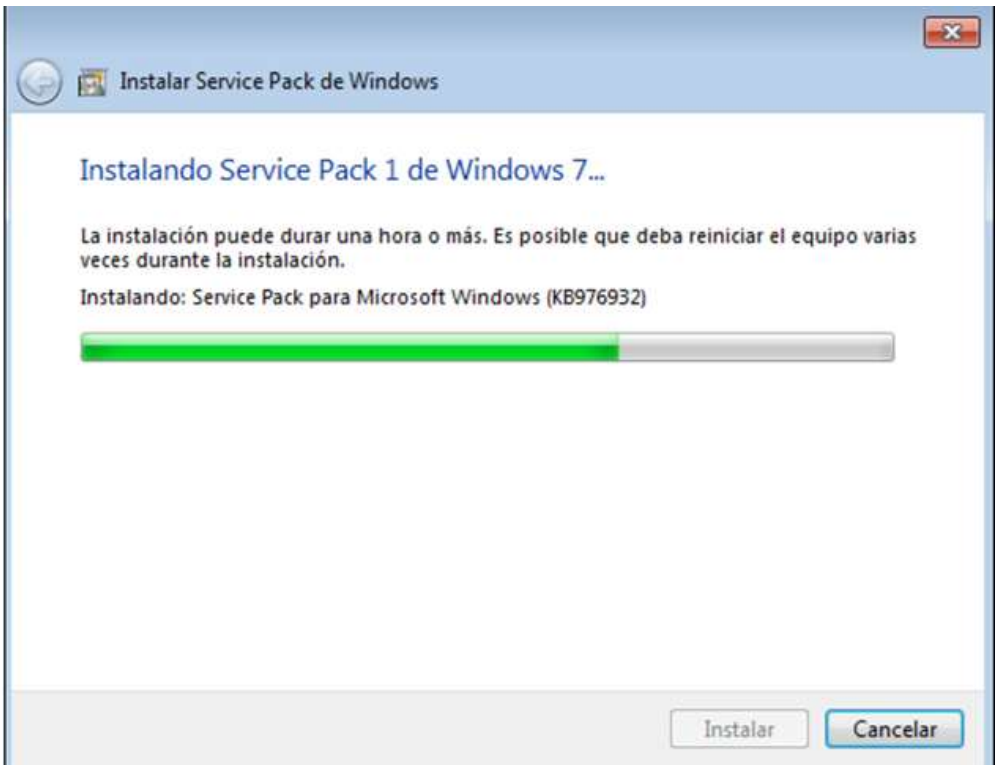
El siguiente equipo que abordaremos es el que utiliza Windows 7 y que presenta las siguientes vulnerabilidades.

Ilustración 102.– 1º Escaneo de Vulnerabilidades Windows 7



El primer paso consistirá en actualizar Windows 7 a la última versión, instalando el Service Pack 1.

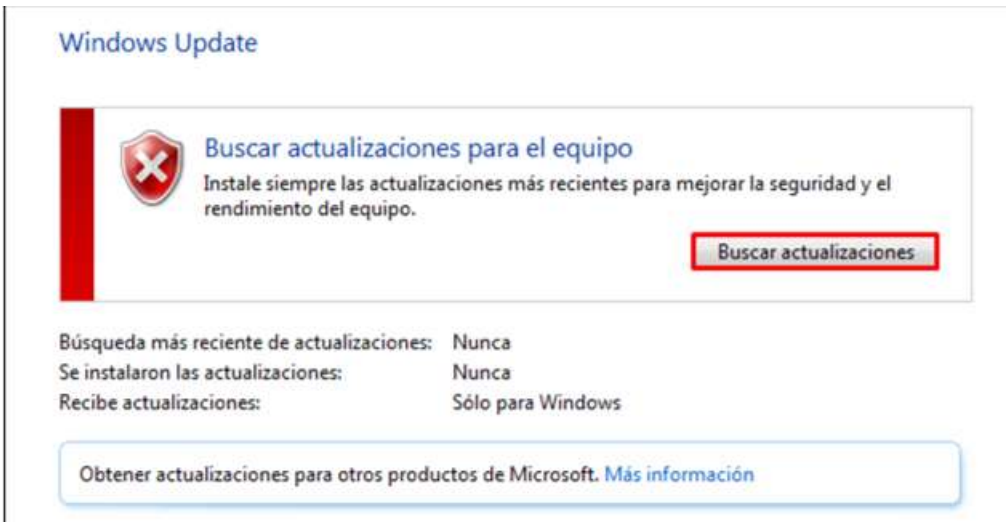
Ilustración 103.– Instalando Service Pack



Una vez que hayamos completado la instalación del Service Pack 1, procederemos a reiniciar el equipo y esperaremos a que la actualización se aplique correctamente. Tras el reinicio, accederemos al instalador de actualizaciones de Windows 7, conocido como 'Windows Update', siguiendo los siguientes pasos:

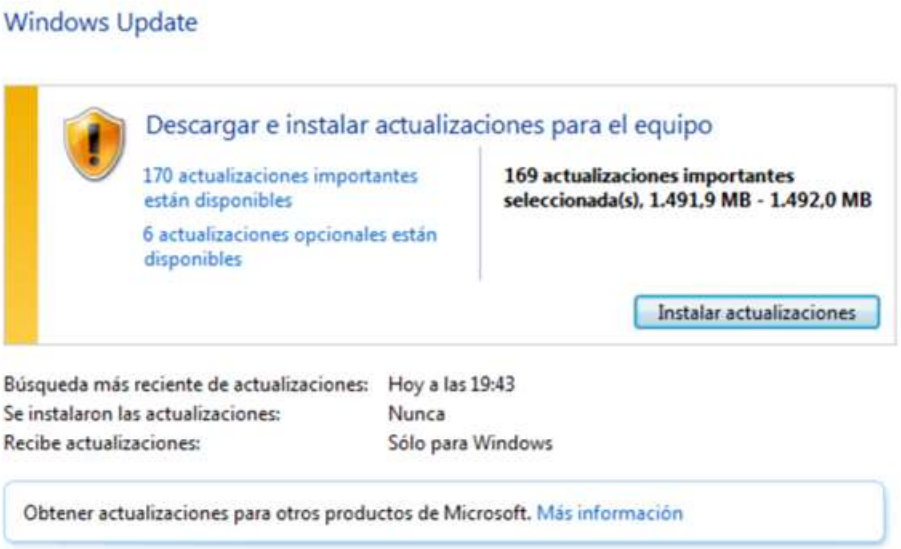
- Accederemos al Panel de control.
- Seleccionaremos la opción de Sistema y seguridad.
- Encontraremos la opción de Windows Update y haremos clic en ella.
- Dentro de Windows Update, elegiremos la opción de buscar actualizaciones.
- De esta manera, podremos buscar e instalar las actualizaciones disponibles para nuestro equipo con Windows 7.

Ilustración 104. – Windows update



Después de que finalice la búsqueda de actualizaciones, Windows Update nos presentará una lista de las actualizaciones disponibles, y procederemos a hacer clic en "Instalar" para que comience la descarga e instalación de estas.

Ilustración 105. – Instalar actualizaciones

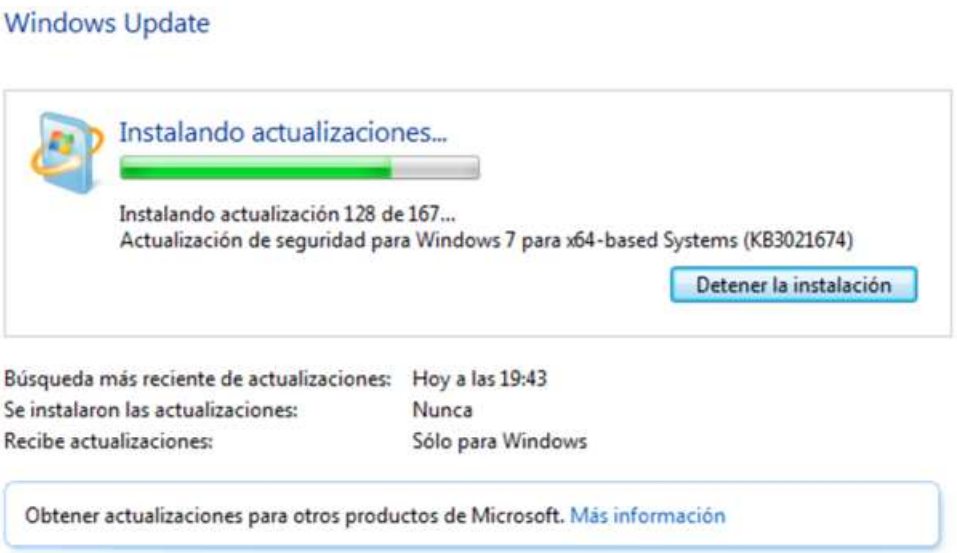


Nuestro equipo anticipa pacientemente la finalización del proceso de descarga de todas las actualizaciones necesarias..

Ilustración 106. – Descarga de las actualizaciones

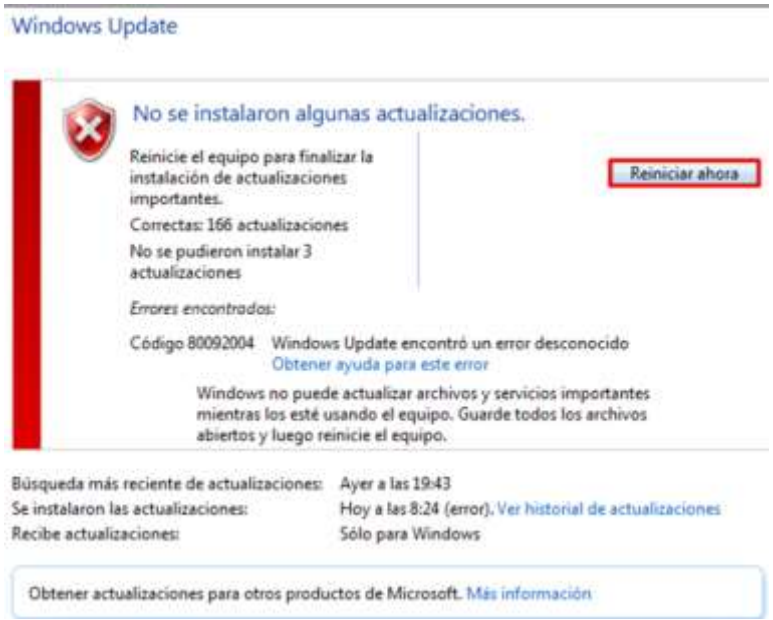
Una vez que se han descargado los archivos, el proceso de instalación comienza automáticamente.

Ilustración 107. – Instalación de las actualizaciones



Después de la instalación de las actualizaciones disponibles, el siguiente paso es reiniciar la computadora.

Ilustración 108.– Numero de actualizaciones instaladas



Nuestra expectativa es que las actualizaciones que se han descargado se implementen con precisión..

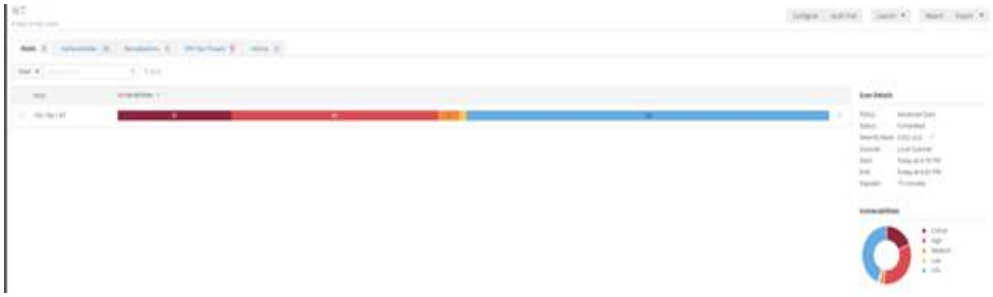
Ilustración 109. – Configuración de las actualizaciones

Al cargar el arranque del equipo nos dirigimos al apartado de Windows Update para comprobar que se han instalado todas las actualizaciones.

Ilustración 110. – Windows Update sin actualizaciones

Una vez instaladas todas las actualizaciones del sistema, procedemos a generar un nuevo escaneo para evaluar el estado actual y el rendimiento del ordenador.

Ilustración 111. – 2º Escaneo de Vulnerabilidades Windows 7



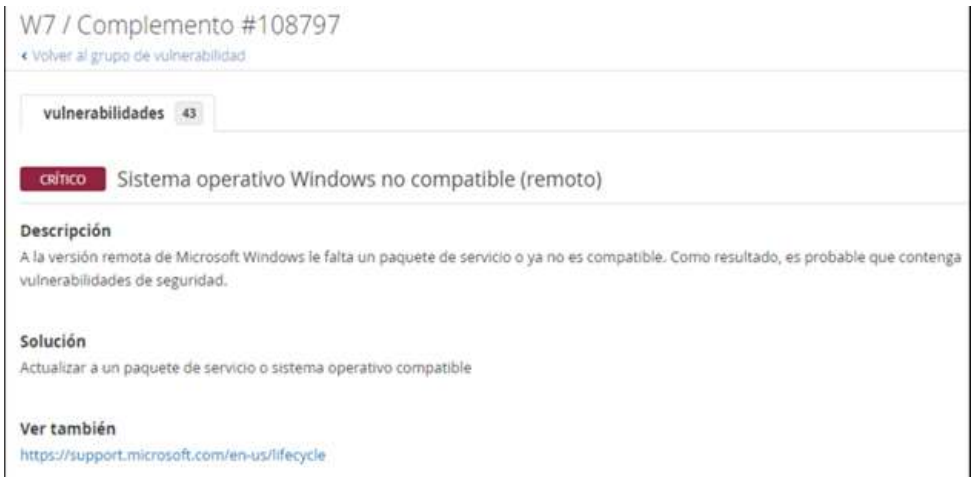
Ingresamos a las más críticas para poder analizarlas.

Ilustración 112.– Vulnerabilidad – Sistema Operativo sin soporte

Es evidente que ciertas vulnerabilidades siguen sin abordarse, y esto es por mantener el uso de un SO sin soporte.

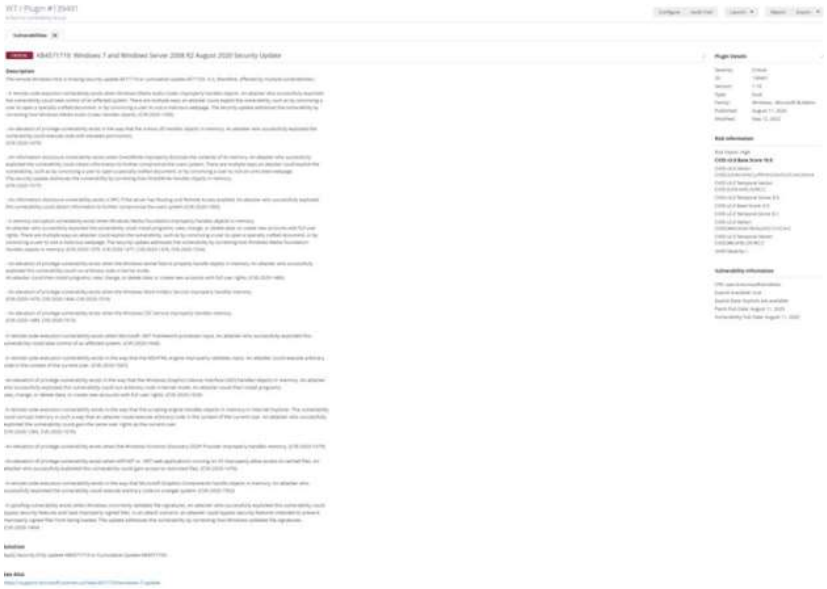
Ilustración 113. – Vulnerabilidad – Versión sin soporte

Ilustración 114.– Vulnerabilidad – Versión del SO sin soporte



A medida que avanzamos con nuestra evaluación de vulnerabilidades, se hace evidente que todavía hay actualizaciones de seguridad pendientes que deben instalarse. En consecuencia, navegamos a los enlaces proporcionados para las respectivas soluciones y seguimos los pasos necesarios.

Ilustración 115. – Vulnerabilidad – Falta de actualizaciones de seguridad

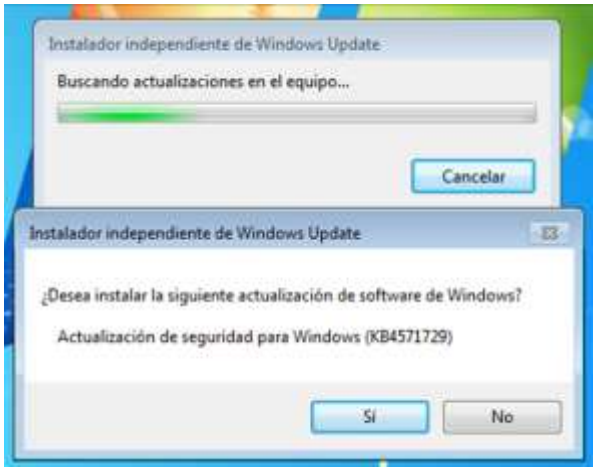


Para garantizar una seguridad óptima, procederemos con la instalación de todos los parches pendientes. Esto requiere acceder a la página web designada para descargas de actualizaciones de Windows: (https://www.catalog.update.microsoft.com/Home.aspx) y buscamos la que nos faltan.

Ilustración 116. – Actualizaciones de seguridad a instalar

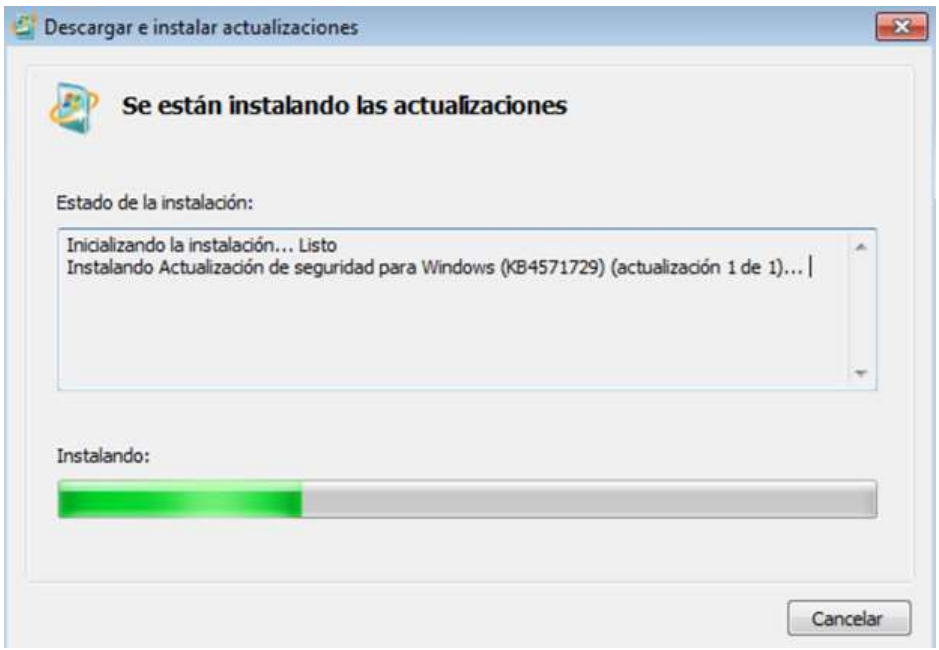
El proceso de instalación comienza una vez completada la descarga, procediendo una a una de la siguiente manera. Iniciamos la instalación ejecutando el archivo .exe y seleccionando la opción "sí" para comenzar la instalación.

Ilustración 117. – Actualización KB4571729



Posteriormente, anticipamos pacientemente la finalización del proceso de instalación.

Ilustración 118.– Progreso de la actualización



Después de instalar cada actualización, será imprescindible reiniciar el equipo y luego continuaremos explorando en busca de más vulnerabilidades con el objetivo de eliminar todas las posibles. En la imagen siguiente, Nessus nos informa que el servicio SMB se encuentra inactivo, lo que podría abrir la puerta a posibles ataques de un atacante sin necesidad de credenciales. Por lo tanto, procederemos a habilitarlo.

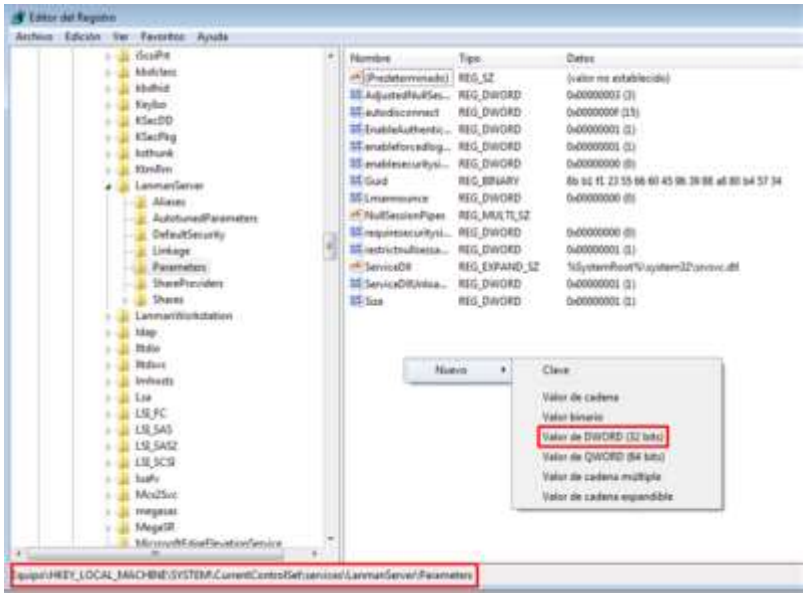
Ilustración 119.– Vulnerabilidad – SMB desactivado

Para habilitar el servicio de SMB, accedemos al registro de Windows ingresando "regedit" en la barra de búsqueda de Windows. Una vez dentro del registro, navegamos a la siguiente ubicación:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters

En esta ubicación, creamos un nuevo valor de tipo 'DWORD'.

Ilustración 120.– creación de valor

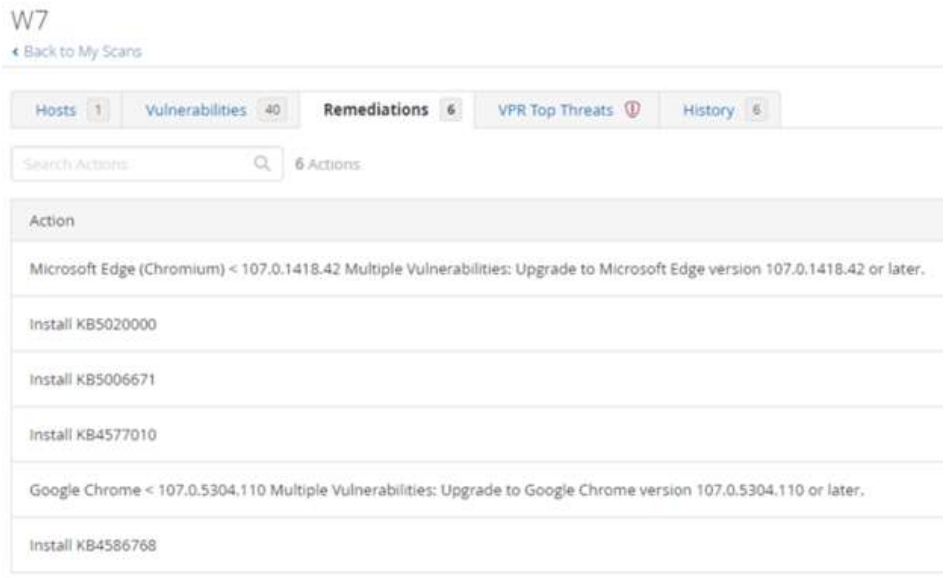


Le asignamos un nombre, como es para samba lo llamaremos "SMB1" y le daremos el valor de 1.

Ilustración 121.– Valor a 1

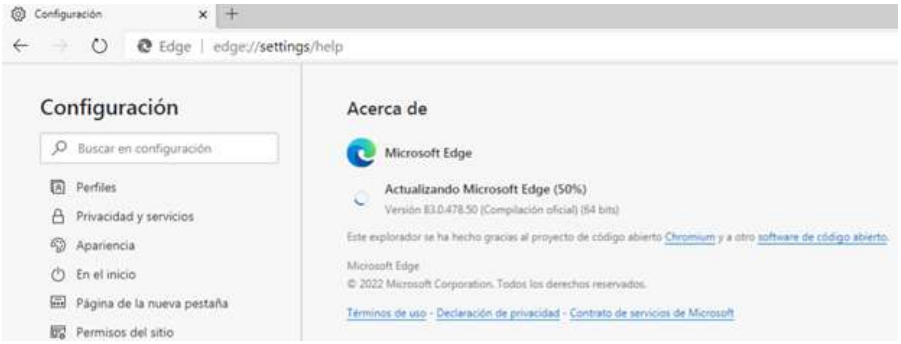
Con el objetivo de evitar la necesidad de analizar cada vulnerabilidad de manera individual, podemos dirigirnos a la pestaña de 'Remediations' en Nessus y seguir las instrucciones proporcionadas en esa sección para abordar la mayoría de las vulnerabilidades.

Ilustración 122.– Pestaña 'Remediations'



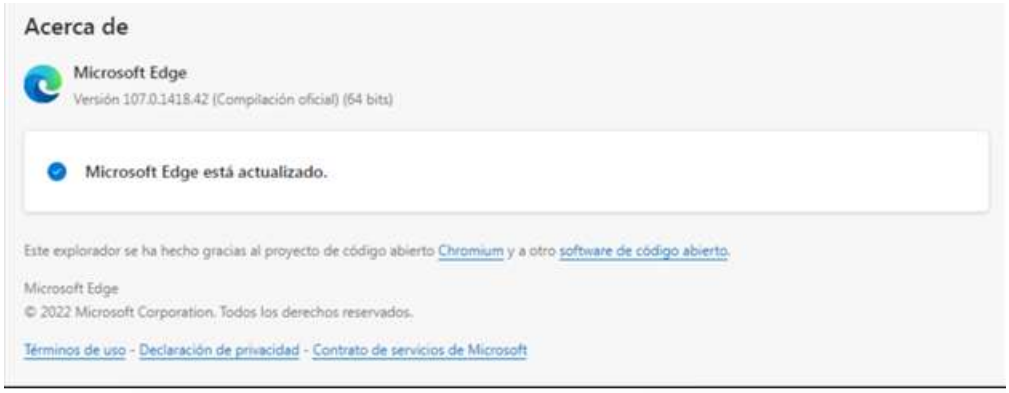
Instalaremos cada actualización que se nos indique, comenzando por Microsoft Edge. Podemos optar por actualizarlo o desinstalarlo. Para llevar a cabo esta acción, ingresamos a la configuración de Microsoft Edge y elegimos la opción de actualización.

Ilustración 123.– Configuración Microsoft Edge



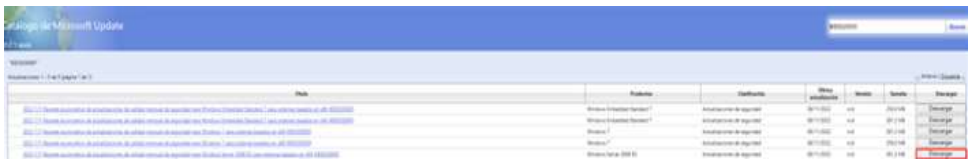
Una vez que se haya completado la actualización, reiniciamos el navegador y volvemos a abrirlo para asegurarnos de que esté actualizado.

Ilustración 124.– Microsoft Edge actualizado



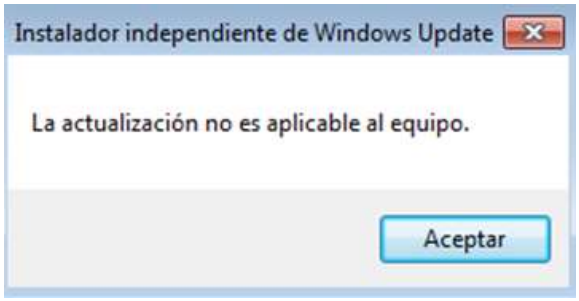
Pasemos al siguiente paso que implica la instalación de la actualización KB5020000. Para hacerlo, realizamos una búsqueda en el catálogo de actualizaciones y procedemos a descargarla.

Ilustración 125. – KB5020000



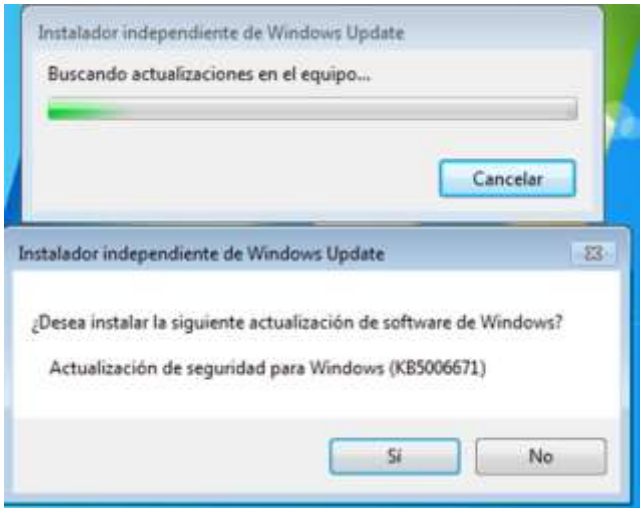
Una vez que se ha descargado el archivo ejecutable de la actualización, lo ejecutamos. Sin embargo, observamos un mensaje que indica que no es aplicable a nuestro equipo. En consecuencia, esta actualización no puede ser instalada en nuestra configuración actual.

Ilustración 126. – Actualización no aplicable



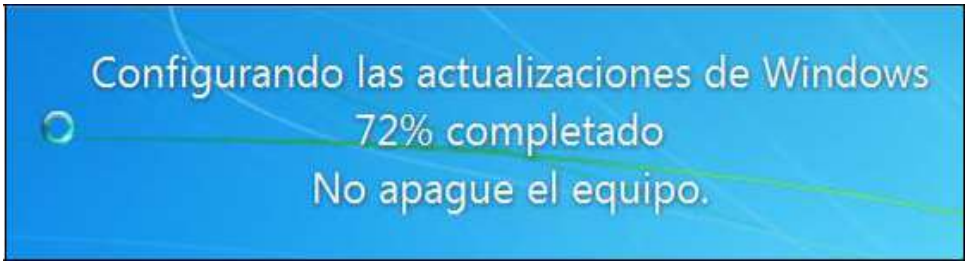
Testeamos a instalar el siguiente KB y repetimos los pasos para la descarga y la instalación.

Ilustración 127.– Actualización KB5006671



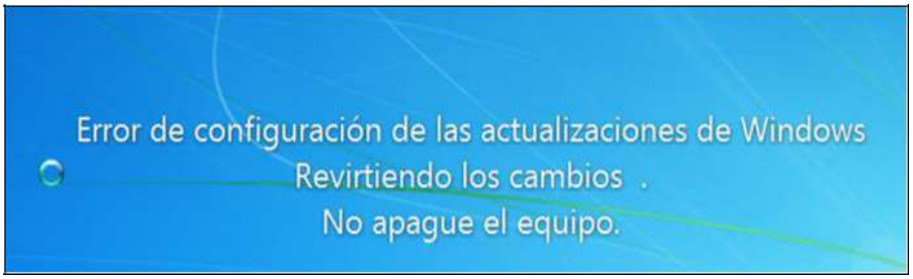
Después de que la actualización se haya instalado con éxito, reiniciamos el equipo y esperamos a que termine de aplicar la actualización.

Ilustración 128.– Configuración de la actualización



Una vez que la instalación y aplicación de la actualización ha finalizado, nos encontramos con el siguiente error.

Ilustración 129.– Error en la configuración de la actualización



Esta situación se repite tanto con KB5006671, KB4577010 y KB4586768, lo que indica que no podemos implementar las últimas actualizaciones de seguridad. Esto se debe a que Windows 7 ya no cuenta con soporte, lo que nos imposibilita parchear cualquier otra vulnerabilidad, dejando el sistema en su estado actual:

Ilustración 130. – 3º Escaneo de Vulnerabilidades Windows 7

En el equipo Windows – 7 partíamos de lo siguiente:

Ilustración 131. – Primer escaneo – Windows 7

Y finalizamos de esta manera:

Ilustración 132. – Último escaneo – Windows 7

El principal desafío de los sistemas operativos que quedan sin soporte es que obligan a los usuarios a migrar hacia otras plataformas, ya que no pueden recibir actualizaciones para solucionar problemas de seguridad. En estos casos, la seguridad se puede mejorar en cierta medida mediante el uso de firewalls y antivirus, como una forma de mitigar los riesgos asociados a la falta de soporte y actualizaciones.

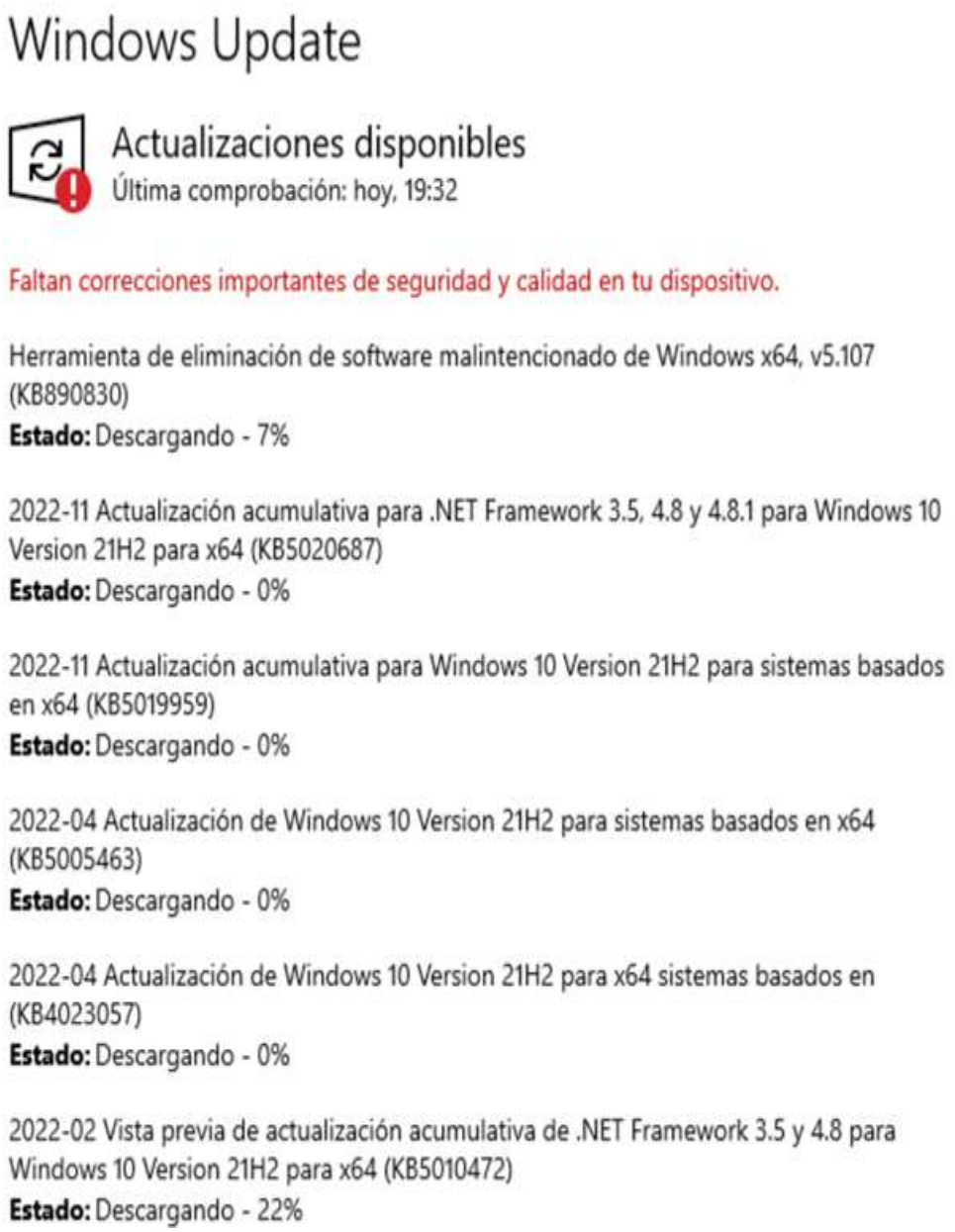
4.4.3 Windows 10

Este equipo de Windows 10 parte con las siguientes vulnerabilidades.

Ilustración 133.– 1º Escaneo de Vulnerabilidades Windows 10

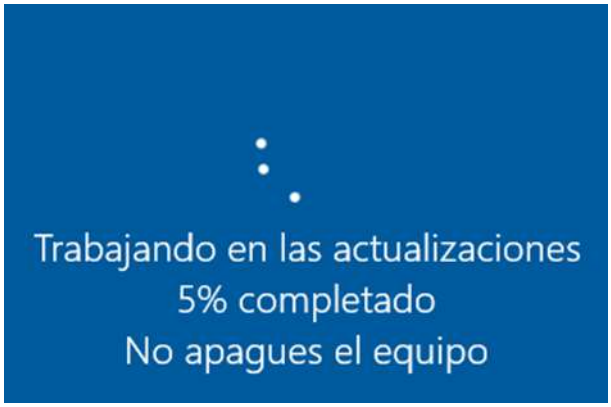
Para empezar, nuestro primer paso es buscar actualizaciones disponibles para Windows Update. Para lograr esto, navegamos por la ruta de configuración-actualización y seguridad.

Ilustración 134.– Descarga e instalación de actualizaciones Windows 10



Luego de asegurarnos de que se han completado todas las descargas, procedemos a reiniciar el equipo e iniciar el proceso de carga de actualizaciones.

Ilustración 135. – Configuración de las actualizaciones Windows 10



En nuestra búsqueda estamos investigando si alguna actualización no se ha instalado o si la instalación de la nueva actualización requiere de las anteriores.

Ilustración 136. – 2º descarga de actualizaciones Windows 10

Luego de ello procedemos a reiniciar el ordenador una vez más para poder iniciar el proceso de instalación.

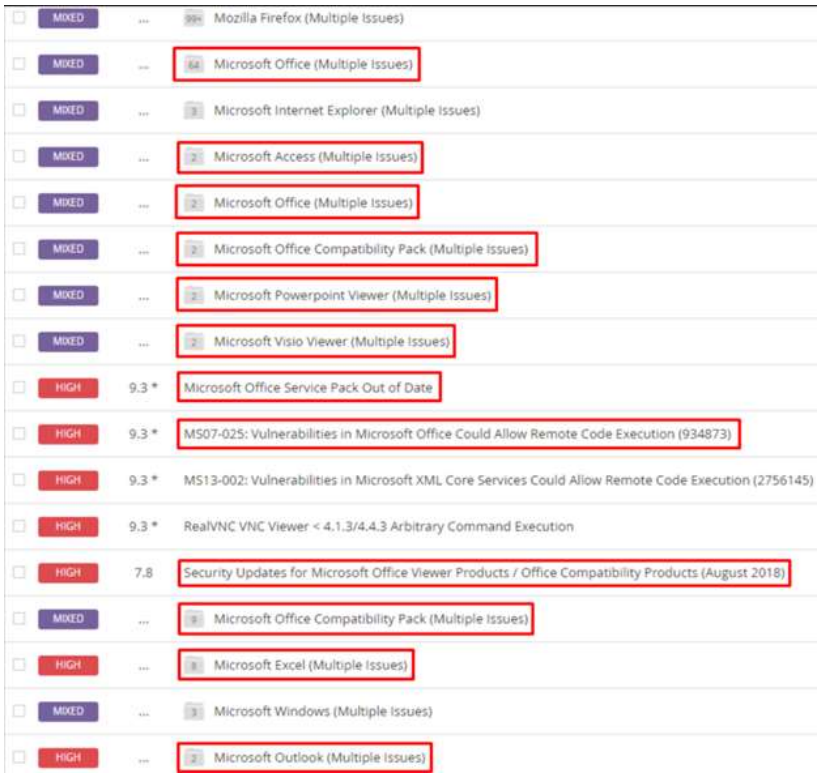
Ilustración 137. – 2º Configuración de las actualizaciones Windows 10

Una vez finalizado el procedimiento, procedimos a iniciar un nuevo escaneo, observando una disminución notable en las vulnerabilidades que estaban inicialmente presente.

Ilustración 138. – 2º Escaneo de Vulnerabilidades Windows 10

Al acceder a la sección de vulnerabilidades, resulta evidente que los problemas provienen del paquete de Microsoft Office. Posteriormente, procedemos a investigar e identificar los problemas específicos que nos ocupan.

Ilustración 139. – Vulnerabilidad Microsoft Office



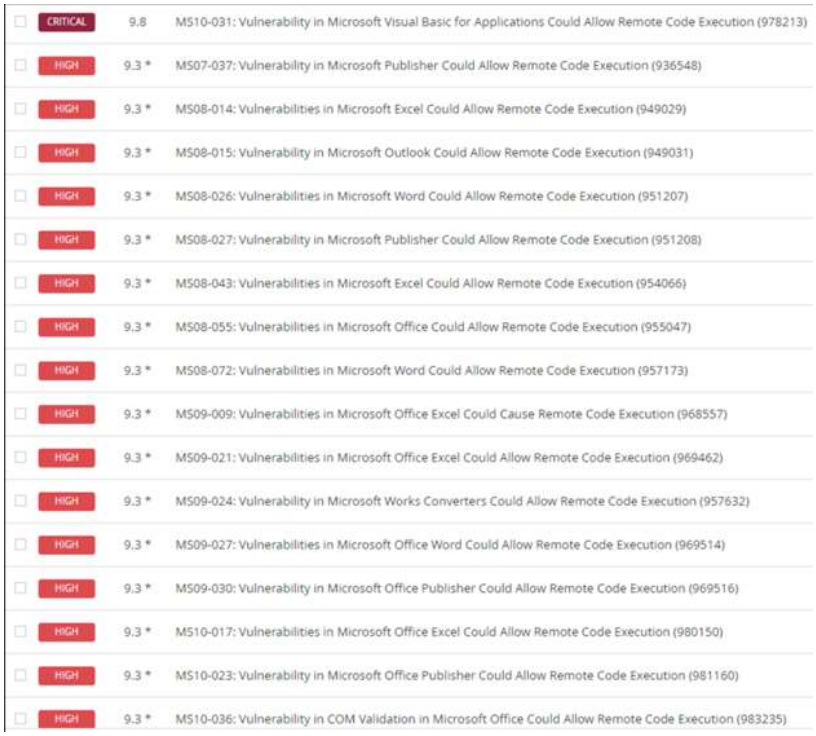
Según la tabla, Nessus nos proporciona la información de que nuestra versión de Office está desactualizada.

Ilustración 140. – Vulnerabilidad Microsoft Office – Versión obsoleta

Sev	Score	Name
CRITICAL	10.0	Microsoft Office Compatibility Pack Unsupported Version Detection
INFO		Microsoft Office Compatibility Pack Installed (credentialed check)

La presencia de esta vulnerabilidad indica que Nessus puede ser susceptible de ser explotado por un atacante externo, lo que permite la ejecución remota de código. Por lo tanto, es necesario eliminar Microsoft Office o instalar las últimas actualizaciones.

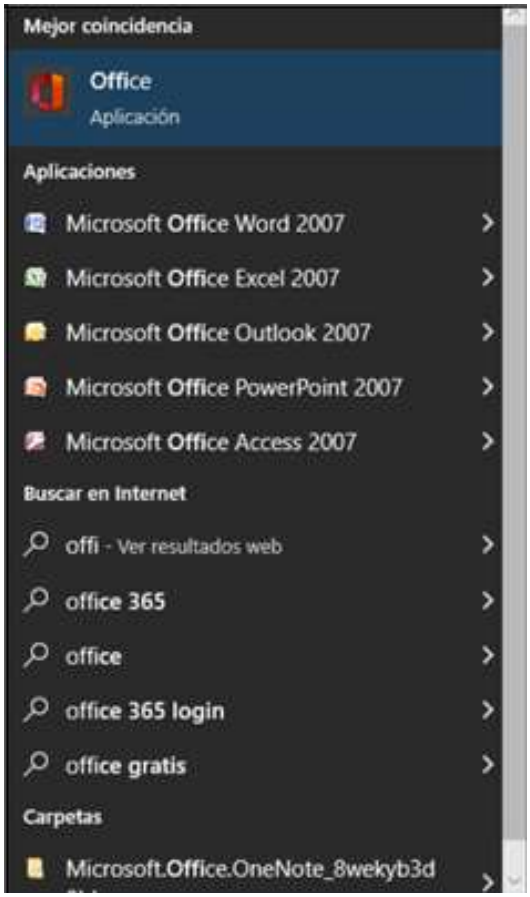
Ilustración 141. – Vulnerabilidad Microsoft Office – Code Execution



CRITICAL	9.8	MS10-031: Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213)
HIGH	9.3 *	MS07-037: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (936548)
HIGH	9.3 *	MS08-014: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (949029)
HIGH	9.3 *	MS08-015: Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (949031)
HIGH	9.3 *	MS08-026: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (951207)
HIGH	9.3 *	MS08-027: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (951208)
HIGH	9.3 *	MS08-043: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (954066)
HIGH	9.3 *	MS08-055: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (955047)
HIGH	9.3 *	MS08-072: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (957173)
HIGH	9.3 *	MS09-009: Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)
HIGH	9.3 *	MS09-021: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)
HIGH	9.3 *	MS09-024: Vulnerability in Microsoft Works Converters Could Allow Remote Code Execution (957632)
HIGH	9.3 *	MS09-027: Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (969514)
HIGH	9.3 *	MS09-030: Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (969516)
HIGH	9.3 *	MS10-017: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)
HIGH	9.3 *	MS10-023: Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (981160)
HIGH	9.3 *	MS10-036: Vulnerability in COM Validation in Microsoft Office Could Allow Remote Code Execution (983235)

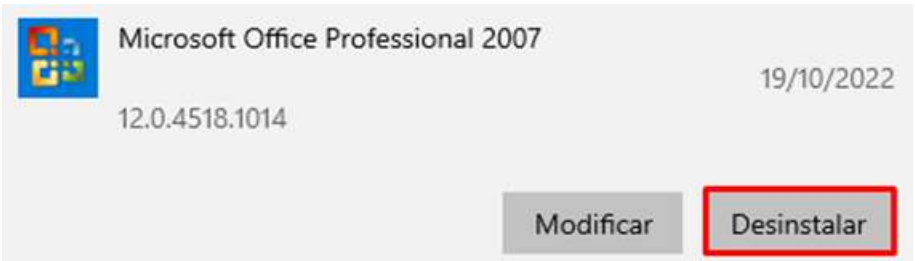
Entramos al equipo para verificar que versión tenemos de Office

Ilustración 142. –Versión Microsoft Office



Como se puede notar, esta es una versión del año 2007, lo que la convierte en una versión antigua y sin respaldo. Por lo tanto, decidimos desinstalarla.

Ilustración 143. –Desinstalación Microsoft Office



Tras desinstalar el Microsoft Office, procedemos a examinar las demás vulnerabilidades, y una de ellas se relaciona con VNC, un programa que se utiliza para conexiones remotas.

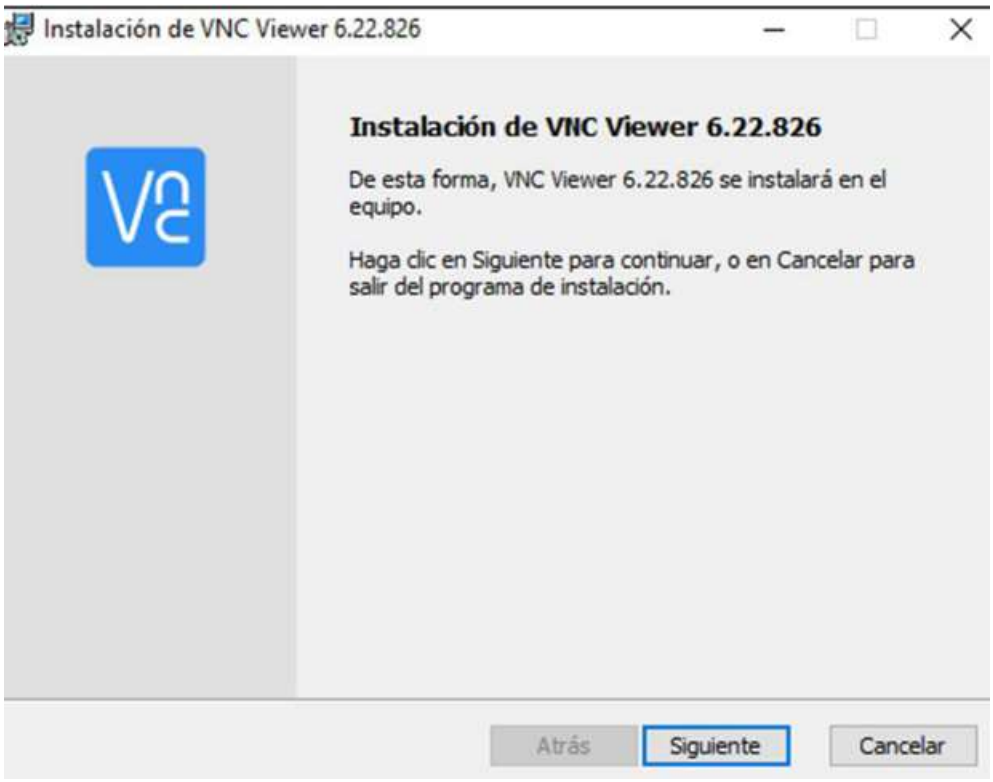
Ilustración 144. – Vulnerabilidad VNC

Tenemos la versión 4.1.2 que es antigua y procederemos para actualizarla, pero primero desinstalamos.

Ilustración 145. –Desinstalación VNC

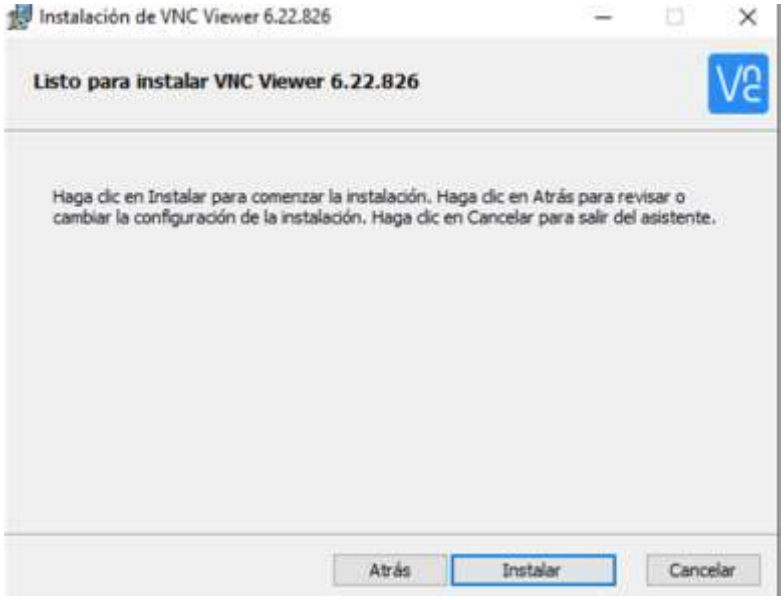
Ahora instalamos la versión nueva 6.2

Ilustración 146. – Nueva versión VNC



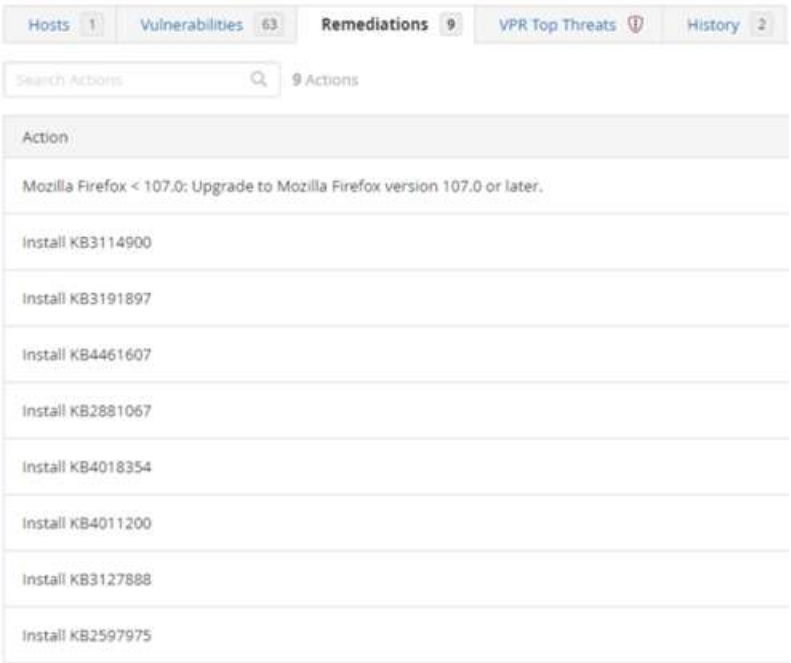
Instalamos la nueva versión y ponemos en instalar.

Ilustración 147.– Instalación nueva versión VNC



Después de solucionar estas vulnerabilidades, navegamos a la sección "Remediations" para evaluar lo que aún queda pendiente.

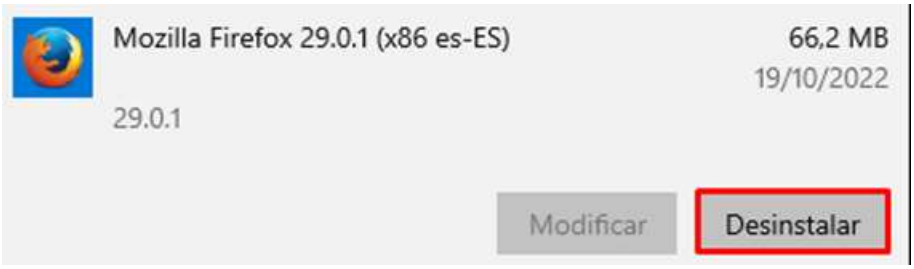
Ilustración 148. –Pestaña 'Remediations'



La próxima vulnerabilidad que abordaremos se relaciona con la versión desactualizada de Firefox. Para resolver esto, comenzaremos desinstalando

la versión actual de Firefox antes de proceder con la actualización. Esto se hace para evitar la presencia de archivos residuales de versiones anteriores en el equipo.

Ilustración 149. – Desinstalación Mozilla Firefox



Luego instalamos el .exe de la versión actual y la instalamos.

Ilustración 150. – .exe de la nueva versión de Mozilla Firefox

Para verificar que es la versión que está actualizada, entramos en ayuda > Acerca de Firefox y corroboramos que está bien.

Ilustración 151. – Mozilla Firefox actualizado

Después de actualizar los programas que produjeron vulnerabilidades, procedemos con otro análisis.

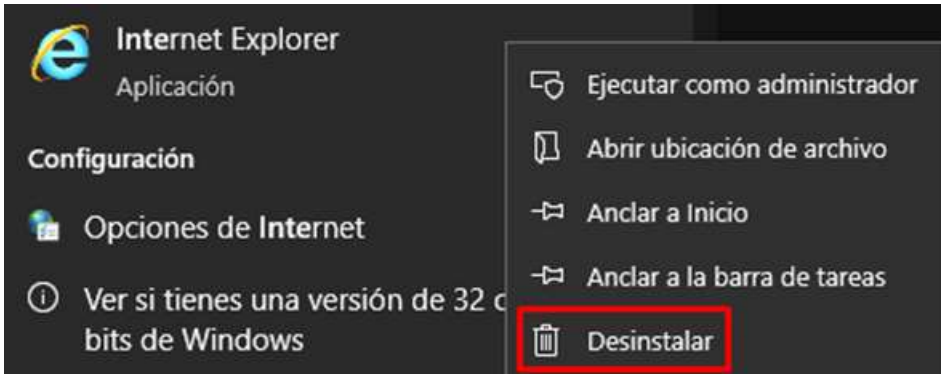
Ilustración 152. – 3º Escaneo de Vulnerabilidades Windows 10

Tras un examen cuidadoso, resulta evidente que una parte importante de las vulnerabilidades se han solucionado con éxito. Además, Nessus destaca la presencia de una vulnerabilidad dentro del Microsoft Internet Explorer instalado.

Ilustración 153.– Vulnerabilidad Microsoft Internet Explorer

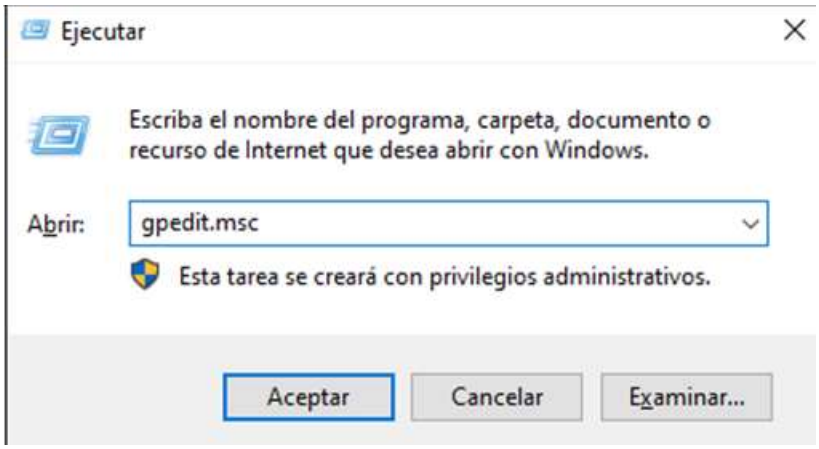
Eliminaremos la versión no compatible de Microsoft Internet Explorer debido a su única vulnerabilidad crítica, ya que la nueva versión de Edge ya está instalada.

Ilustración 154. – Desinstalación Microsoft Internet Explorer



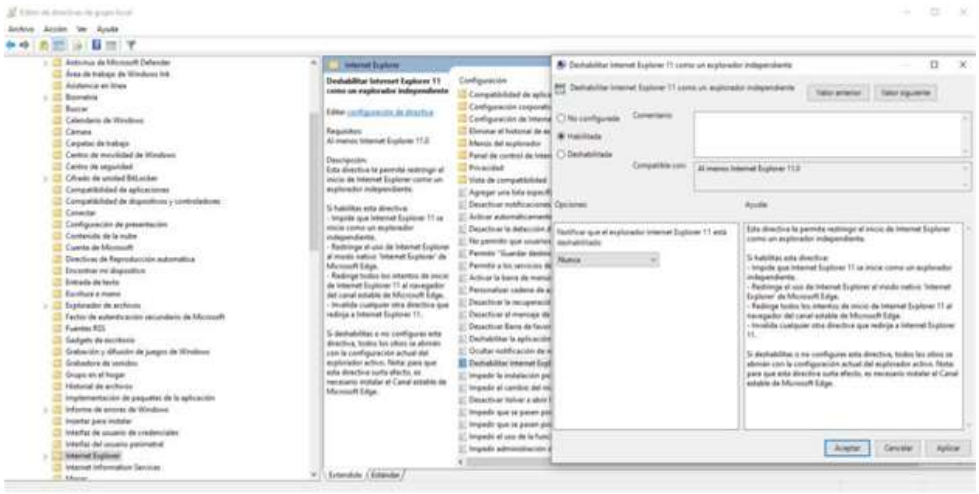
Una vez desinstalado, utilizaremos gpedit.msc para deshabilitar Internet Explorer, evitando que queden rastros de archivos y configuraciones obsoletas en el sistema.

Ilustración 155. – comando: gpedit.msc



Ingresamos a la ruta de la configuración del equipo/ Plantillas administrativas\Componentes de Windows\Internet Explorer y localizamos la directiva 'Deshabilitar Internet Explorer 11 como un explorador independiente', luego procedemos a activarla.

Ilustración 156.– Directiva 'Deshabilitar Internet Explorer 11 como explorador independiente'



Tras un examen más detallado de las vulnerabilidades restantes, resulta evidente que la computadora está afectada por dos directivas inadecuadamente configuradas o ausentes, comprometiendo así la integridad del sistema.

Ilustración 157. – Vulnerabilidad - WinVerifyTrust

Para abordar la vulnerabilidad, podemos resolverla abriendo un bloc de notas y modificando el registro con directivas específicas. Estos cambios deben guardarse como "WinVerifyTrust.reg" y ejecutarse posteriormente.

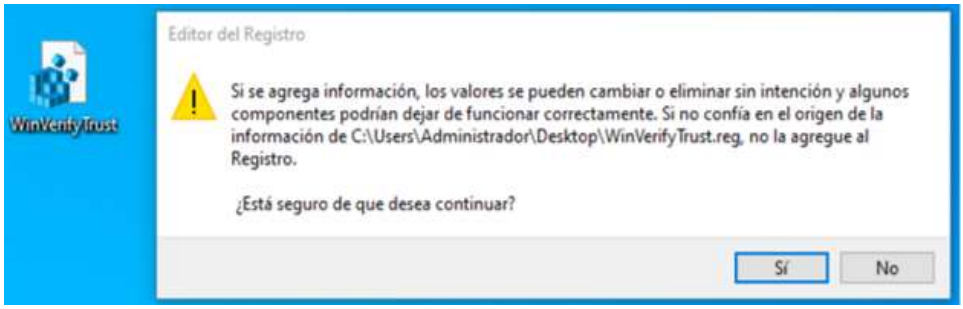
Ilustración 158. – Código para la modificación de las directivas

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config]
"EnableCertPaddingCheck"="1"

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config]
"EnableCertPaddingCheck"="1"
```

Aceptamos la creación de ambas variables en el registro.

Ilustración 159. – Ejecución del script 'WinVerifyTryst.reg'



Observamos que modificó el registro de Windows sin problema.

Ilustración 160. – Correcta modificación del registro

Ilustración 161. – Directiva 1

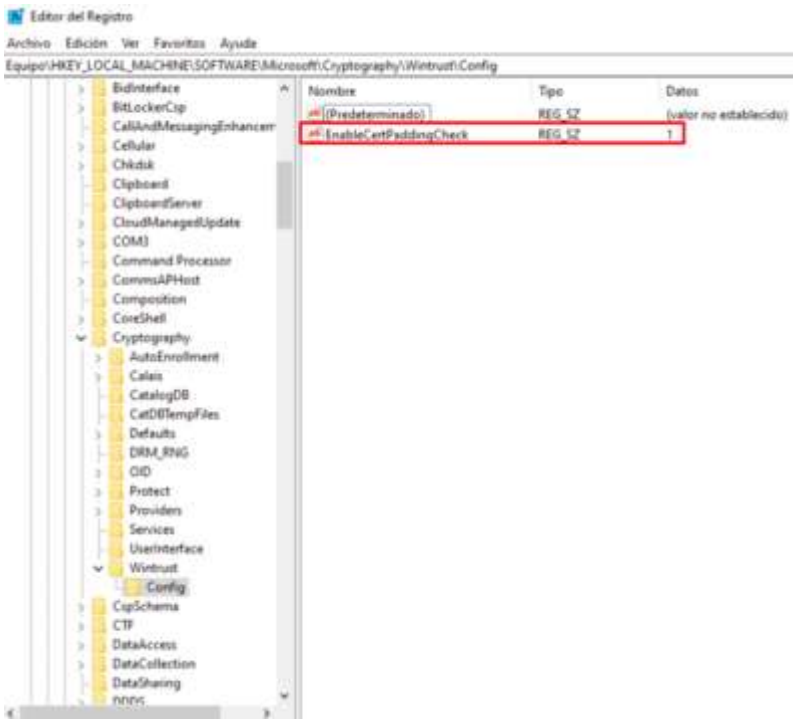
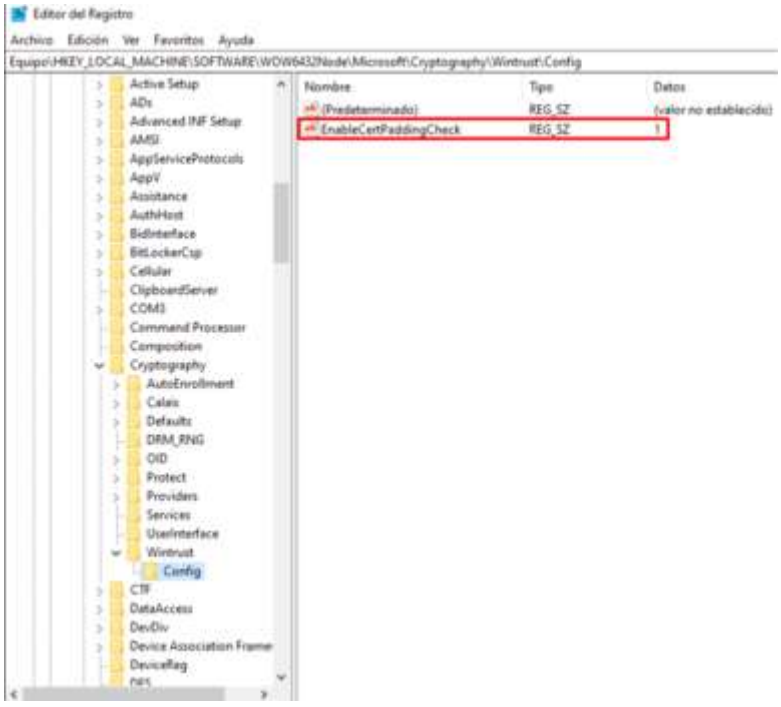


Ilustración 162. – Directiva 2

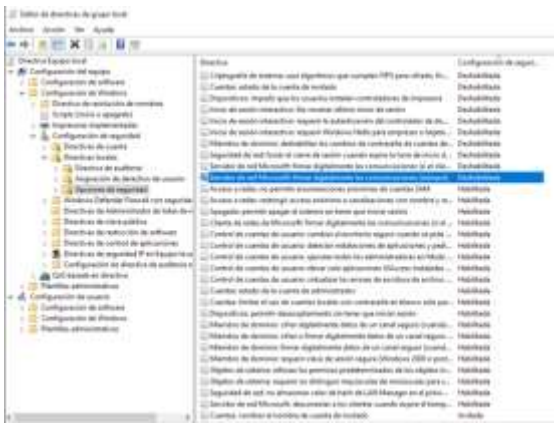


La última vulnerabilidad que identificamos radica en la desactivación de la función de firma SMB en el sistema, lo que potencialmente permitiría a un atacante acceder al equipo sin necesidad de autenticación.

Ilustración 163. – Vulnerabilidad - SMB

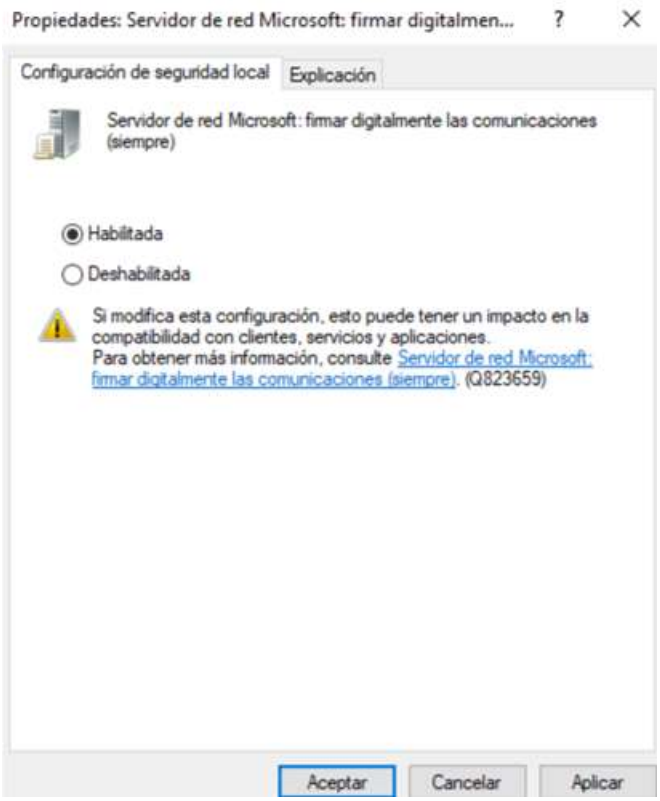
Para habilitar la política deseada, podemos acceder al terminal gpedit.msc y realizar las modificaciones necesarias.

Ilustración 164. – Modificación directiva SMB



Aplicamos y aceptamos el cambio.

Ilustración 165. – Habilitar directiva SMB



Reiniciamos la computadora para que los cambios realizados surtan efecto y, una vez que hemos abordado las vulnerabilidades detectadas, procedemos a realizar un nuevo escaneo para verificar si quedan problemas pendientes de resolución.

Ilustración 166. – Ultimo escaneo de Vulnerabilidades Windows 10

La imagen de escaneo de vulnerabilidades más reciente de Windows 10 y Ubuntu revela que estos dos sistemas operativos tienen la capacidad de recibir actualizaciones y parches completos, lo que garantiza que estén libres

de vulnerabilidades importantes. Esto es posible gracias al apoyo continuo que reciben. Por el contrario, las versiones anteriores, como Windows 7, carecen de la capacidad de abordar y rectificar vulnerabilidades, lo que las deja susceptibles a una posible explotación.

En el equipo Windows – 10 partimos de lo siguiente:

Ilustración 167.– Primer escaneo – Windows 10

Hemos acabado así:

Ilustración 168.– Último escaneo – Windows 10

4.5 Ransomware y dispositivos móviles.

El ciberdelincuente sabe que puede aprovechar del usuario que no tiene tanta seguridad informática y mucho más si no están mezclado muchos en el mundo de la tecnología. Por eso puede usar un malware para robar los datos confidenciales de algún teléfono inteligente.

Se mencionan algunos consejos que ayudan a proteger los dispositivos móviles.

- Tener precaución con la instalación de aplicaciones dudosas ya que estas son una fuente de malware, antes de instalar cualquier aplicación debe de asegurarse que es descargada de las tiendas oficiales de las telefonías, incluso aún así se han encontrado varias en la tienda de Google Play Store.
- Instalar parches de seguridad. El ransomware puede contagiar a un dispositivo a través de descarga no autorizadas. Esto puede suceder al momento que uno visita accidentalmente sitios fraudulentos o también son redirigidos a web sospechosas a causas

de un malware, para asegurarse tienen que estar actualizados las aplicaciones y sistemas operativos.

- Mantenerse informado sobre las últimas amenazas y tendencias de cibercrimen.
- Realizar una copia de seguridad de todos los archivos, siempre es una muy buena idea.

4.5.1 En caso de infección del ransomware.

En caso de producirse un incidente relacionado al ransomware, debes de considerar los siguientes pasos.

- **Antes de apagar el sistema.** Se sugiere tomar una copia de la memoria del sistema si es posible debido a la presencia de malware, la instantánea permitirá identificar la forma en que el ransomware atacó y encontrar cualquier información criptográfica que pueda ayudar a desencriptar los datos.
- **Apague el sistema.** Para prevenir una mayor propagación de la infección de ransomware y minimizar el daño a los datos, es esencial apagar el sistema infectado
- **Identificar el vector de ataque.** La capacidad del usuario para identificar el momento exacto en que se pierden los accesos a los datos, así como para detectar correos electrónicos que puedan contener ransomware.
- **Bloquear el acceso a la red.** Es crucial impedir el acceso a la red, ya que varios tipos de ransomware tienen la capacidad de expandirse a través de la red donde reside el equipo infectado. Por lo tanto, es esencial bloquear cualquier servidor de comando y control que el malware pueda estar utilizando. Sin acceso a estos servidores, el malware no podrá cifrar los datos.

4.6 Medidas de protección contra los ataques de ransomware para las PYMEs y sistemas de prevención.

Esta lista de consejos será de gran utilidad tanto para las empresas como para las personas individuales. Se han formulado recomendaciones basadas en los medios más habituales de difusión de esta amenaza.

4.6.1 Adjuntos de correo electrónico.

El mail sigue siendo una de las formas más comunes que los atacantes utilizan para difundir el ransomware. Si su correo está recibiendo notificaciones de otras páginas que usted no ha visitado posiblemente está su información comprometida en alguna brecha de seguridad por lo cual puede verificarlo en esta página Web https://monitor.mozilla.org/ para saber si su mail estuvo o no expuesto, en caso de que sea que sí tiene que cambiar urgentemente su clave en todas las páginas que aparezca su correo y en caso de que no pueda estar tranquilo.

Al momento de recibir un correo de una persona conocida o de algún pidiendo actualización de datos o simulando que es un amigo tuyo y te pide que hagan click en un enlace y no estás seguro de que sea confiable entonces puedes entrar a la siguiente página https://www.virustotal.com en donde puedes copiar el link y pegarlo en la página para verificar si tiene algún virus detrás de esa dirección.

Para reducir el riesgo de ser víctima de este tipo de ataque, se deben seguir estos consejos de prevención:

- Abrir solo archivos adjuntos de remitentes confiables.
- Verificar la dirección de correo electrónico del remitente para asegurarse de que es correcta.
- Tener en cuenta que los nombres de dominio y los nombres para mostrar pueden ser falsificados con facilidad.
- No abrir archivos adjuntos que requieran habilitar las macros. Si se piensa que el archivo adjunto es legítimo, buscar

ayuda o asesoramiento del departamento de TI en el caso de las empresas.

4.6.2 Direcciones maliciosas.

Los atacantes también utilizan correos electrónicos para enviar enlaces maliciosos, que son una forma común de distribuir ransomware. Aquí hay algunos consejos de prevención:

- Estar atento a todos los enlaces incrustados en correos electrónicos y mensajes directos.
- Verificar la URL colocando el cursor sobre el enlace antes de hacer clic en él.
- Utilizar CheckShortURL para expandir URL acortadas.
- Intentar ingresar manualmente los enlaces en el navegador para evitar clics en enlaces de phishing.

4.6.3 Publicidad engañosa.

Normalmente se aprovecha la curiosidad de algunos usuarios es bastante sencillo que muchas personas hagan clic sobre este tipo de publicidad, por lo que vale la pena tomar en cuenta ciertas pautas.

Consejos de prevención:

• Mantener el sistema operativo, aplicaciones y navegadores webs actualizados.

• Deshabilitar los complementos que no usa habitualmente.

• Utilizar un bloqueador de anuncios.

• Habilitar los complementos de reproducción por clic en el navegador web, lo que evita que complementos como *Flash* y *Java* se ejecuten automáticamente. Una gran cantidad de publicidad maliciosa se basa en la explotación de estos complementos.

4.6.4 Protocolo de escritorio remoto.

Vulnerabilidades pueden ser un peligro para los usuarios debido a que a menudo se descuidan las verificaciones en las computadoras. Por lo tanto, este método de infección se utiliza comúnmente.

Consejos de prevención:

• Utilice contraseñas fuertes y seguras, aunque pueda sonar repetitivo.

• Cambie el puerto RDP desde el puerto estándar 3389.

• Habilite RDP solo si es realmente necesario.

• Use una VPN.

• Active una autenticación de dos factores (2FA) para las sesiones remotas.

4.6.5 Descargas automáticas.

Las descargas automáticas son un riesgo para los usuarios ya que se llevan a cabo sin su participación y por lo tanto, a menudo pasan desapercibidas. Consejos de prevención:

• Mantener el software actualizado con las últimas actualizaciones de seguridad.

• Desinstalar extensiones de navegador no necesarias.

• Instalar un bloqueo de anuncios.

4.6.6 Propagación de la red.

En este nivel de riesgo se incrementa ya que existen cepas que tienen algunas funciones dedicadas a esparcir el ransomware en otros equipos dentro de la misma red conectada.

Consejos de prevención:

- Segmentar la red
- Mantener una estrategia de respaldo e implementación de ransomware
- Si por cualquier motivo un equipo de la red llega a estar infectado, se debe de desconectar de inmediato, con el fin de que se siga propagando a otros equipos conectados de la red.

4.6.7 Software ilegal.

En el mundo del internet se encuentra distintas páginas en las que uno se puede descargar software gratis para activar algún programa de pago, por medio de activadores o crack, estos archivos al ejecutarlos en la pc son los que instalan el ransomware, o dejan abierta una puerta por donde luego será implantada la infección.

Consejos de prevención:

- Tener cuidado con las ofertas de software que son demasiada buenas para ser verdad.
- Evitar el uso de software pirata.
- Evitar sitios web que alojan software pirateado, cracks, activadores o generadores de claves.

4.6.8 Dispositivos portátiles.

Las unidades USB y los equipos portátiles infectados pueden ser fuentes de propagación de ransomware. Para prevenir esto, es importante no conectar dispositivos desconocidos, tener políticas sólidas de seguridad BYOD, utilizar un software antivirus confiable y regular la conexión de equipos portátiles a la red.

CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones.

- Se pudo observar debido a las pruebas que se realizaron a distintos sistemas operativos que usando Kali Linux y sus herramientas, efectivamente se pudo analizar los ataques que manejan actualmente hacia un objetivo son por falta de una mejor configuración en su red y posiblemente de un desconocimiento de tener puertos disponibles sin necesidad de usarlos por ende quedan expuestos a posibles ataques externos a su red, por los cuales estos mismos puertos nos dan información de que versiones del sistema operativo maneja el usuario que es atacado y saber identificar que vulnerabilidades tienen estos para saber como explotar esas fallas debido a su mala parametrización de red y mala revisión de diversos tipos ,sean estos no aplicar un parche para el sistema en general o una nueva versión de un programa que no ha sido actualizado y tenga un fallo en su versión antigua e incluso nos permita hacer escalada de privilegios al no ser renovados constantemente por eso su importancia de los ajustes pertinentes. Adicional de que debe de tener un conocimiento básico la persona que maneja el sistema sobre lo que es ciberseguridad y poder mitigar el riesgo de los ataques a su red.

- Luego de que se hizo las vulneraciones vimos la importancia de saber identificar cuáles son los errores corroborando con Kali y también con su herramienta de Nessus que nos indicaron los puntos rojos que son los más importantes y críticos que había que parchar rápidamente, se pudo observar cómo en gran mayoría disminuyeron las vulnerabilidades del sistema y así tapar parte los fallos de seguridad de la red, ya que no se pudo en el total de un sistema operativo ya que éste no tiene soporte oficial actualmente por

consiguiente queda expuesto en parte a un ataque sino se evoluciona a otro sistema operativo más actual pero de todas maneras al parchar varias extensiones del mismo sistema operativo o de un antivirus, algún navegador de red o un programa obsoleto se minimizaron los riesgos.

- Por eso es la importancia de tener una capacitación constante sobre ciberataques no sólo la persona que maneja una pyme sino en su mayoría que tenga una idea de poner un negocio incluso desde su casa ya que también hasta su propia red local puede ser afectada por no tener una buena configuración, ya que el eslabón más débil de toda esta cadena es el ser humano con desconocimiento.

5.2 Recomendaciones

De acuerdo con el estudio realizado se recomienda lo siguiente para tener puntos importantes para mitigar ataques informáticos:

1. Restringir la instalación de programas, extensiones y applets Java a usuarios sin privilegios de administrador.
2. Deshabilitar las unidades de red no utilizadas y el acceso no autorizado a puertos como RDP y SMB.
3. Realizar copias de seguridad de datos regulares y probadas para almacenarlas desconectadas después de verificar su integridad.
4. Mantener todas las aplicaciones y sistemas actualizados con los últimos parches de seguridad de todos los sistemas operativos que se usen en su organización y revisar regularmente que no falten actualizaciones críticas.
5. Al tener un sistema operativo que ya no le den soporte técnico se está en riesgo de que atacantes aprovechen fallos de este y lo mejor es actualizar a un sistema que si tenga soporte oficialmente, para minimizar amenazas.
6. Bloquear archivos adjuntos peligrosos mediante software antimalware con capacidades anti-ransomware habilitadas.
7. Desactivar la ejecución de código JavaScript en documentos PDF y Analizar los PDF con antivirus antes de abrirlos.
8. Segmentar la red para limitar el impacto en caso de infecciones y separar el tráfico crítico del estándar.
9. Capacitar a los empleados sobre amenazas actuales de ransomware y formas de infección mediante emails, anuncios web maliciosos, sitios falsos, etc.
10. Contar con un plan de respuesta a incidentes que incluya la recuperación de sistemas y archivos sin pagar rescates.
11. Al no estar seguro de visitar algún link que le hayan enviado por mail puede visitar la página de https://www.virustotal.com y pegarlo para poder comprobar si hay alguna especie de virus oculto detrás del link e

incluso puede subir un archivo para verificar si hay algún software malicioso detrás del mismo.

12. Utiliza contraseñas complejas y únicas para cada cuenta, y habilita la autenticación de dos factores (2FA) siempre que sea posible para una capa adicional de seguridad y podemos visitar https://password.kaspersky.com/es/ para saber si tenemos una buena contraseña fuerte para que sea difícil de romper por medio de ataque de diccionario.
13. Implementar servicios de copia de seguridad en la nube, como Google Drive, Dropbox, etc.
14. Hacer simulaciones de ataques a los equipos de empleados, para saber si están al tanto de los tipos de ataques que se presentan y puedan identificarlos y que sepan lo que tienen que hacer frente a uno.
15. Si les llega un correo de una persona conocida sea del trabajo o personal y tiene duda lo mejor es comunicarse con el directamente por el celular preguntando sobre el mismo para tener un panorama más claro y minimizar el riesgo de infección.

Bibliografía

Daasel. (2020). *Ciberseguridad: Consejos para proteger la empresa*. Daasel. https://daasel.com/ciberseguridad-consejos-para-proteger-la-empresa/

Anónimo. (14 de junio de 2021). *¿Qué es Mimikatz y cómo defenderse de esta herramienta de robo de contraseñas?* Tangerfiv. https://tangerfiv.com/es/que-a-9-es-mimikatz-y-como-defenderse-de-esta-herramienta-de-robo-de-contraseñas/

Alfonso. (5 de abril de 2019). *Actualizaciones de software: ¿Qué son, para qué sirven, cuándo instalarlas?* Idearius. https://www.idearius.com/es/blog/actualizaciones-de-software-que-son-para-que-sirven-cuando-instalarlas/

Arias, F. (2016). *El Proyecto de Investigación (5ta Edición).* Academia.edu. https://www.academia.edu/9103795/Fidias_G_Arias_El_Proyecto_de_Investigacion_5ta_Edicion

Ávila, Y. (2023). Ransomware, una amenaza latente en Latinoamérica. Revista electrónica de las sedes regionales de la Universidad de Costa Rica, 24, 1-17. https://www.scielo.sa.cr/pdf/is/v24n49/2215-2458-is-24-49-092.pdf

Briceño, L. (20 de enero de 2023). *¿Qué es phishing y cómo identificarlo?* GK City. https://gk.city/2023/01/19/que-es-phishing-como-identificarlo/

Cámara Zamora. (4 de noviembre de 2021). Ciberataques y cómo protegerse de ellos. Cámara Zamora. https://www.camarazamora.com/ciberataques-y-como-protegerse-de-ellos

Cano, M. (2019). *Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo.* ACIS. https://sistemas.acis.org.co/index.php/sistemas/article/view/13

Cano, J. (2020). Ciberataques. *Revista Uno*, 1(157), 1-12. https://doi.org/10.29236/sistemas.n157a6

Cisco. (2020). *Common*. Cyberattacks. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html?_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es

Cyberwar. (25 de enero de 2022). *Ciberataques en Ecuador 2021*. Cyberwar LA. https://www.cyberwar-la.com/post/ciberataques-ecuador-2021

Daasel. (2018). *Ciberseguridad: Consejos para proteger la empresa*. Daasel. https://daasel.com/ciberseguridad-consejos-para-proteger-la-empresa/

Diazgranados, H. (31 de agosto de 2021). *Los ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021.* Kaspersky Lab. https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Dion, J. (junio de 2020). *Risk Management for Cybersecurity.* Udemy. https://www.udemy.com/course/risk-management-for-cybersecurity/

Elevenpaths. (11 de febrero de 2021). *Mecanismos de ciberseguridad en el día a día*. Blogthinkbig. https://empresas.blogthinkbig.com/mecanismos-ciberseguridad-dia-a-dia/

Eset. (s/f). *Virus.* Eset. https://help.eset.com/glossary/es-ES/viruses.html

E-SPIN. (2019). *What is a Cyber Security Vulnerability Assessment?* E-SPIN. https://www.e-spincorp.com/what-is-a-cyber-security-vulnerability-assessment/

Friss. (26 de julio de 2018). *Robo de identidad: Un negocio lucrativo, perfecto y redondo*. Friss. https://www.friss.com/es/blog/robo-de-identidad-un-negocio-lucrativo-perfecto-y-redondo/

Galindo, X., Gómez, M., & Hernández, J. (2019). *Seguridad en la nube, evolución indispensable en el siglo XXI*. Revista 16(1), 110-127. https://orcid.org/0000-0003-3908-2763

García, A. (7 de abril de 2020). *El mayor vector de ataque en América Latina es el phishing*. Inforc. https://www.inforc.lat/post/el-mayor-vector-de-ataque-en-am%C3%A9rica-latina-es-el-phishing

Gartner. (2018). *Public Cloud 2020*. Gartner. http://139.59.48.110/wp-content/uploads/2021/06/Gartner-Public-Cloud-2020.pdf

Gartner. (s/f). *Next-Generation Firewalls (NGFWs).* Gartner. https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Gub. (2020). *Estadísticas de incidentes de seguridad informática 2020*. Centro Nacional de Respuesta a Incidentes de Seguridad Informática. https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas/estadistica-incidentes-seguridad-informatica-2020

Harán, J. M. (22 de agosto de 2022). *Empresas en América Latina: Incidentes de seguridad.* WeLiveSecurity. https://www.welivesecurity.com/la-es/2022/08/04/empresas-america-latina-incidentes-seguridad/

Hernández, M. (11 de febrero de 2021). *11 razones por las que Linux es increíble*. freeCodeCamp. https://www.freecodecamp.org/espanol/news/11-razones-por-las-que-linux-es-increible/

IBM. (s/f). IBM MQ *Security: Cryptography.* IBM. https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009780--htm

IBM. (30 de noviembre de 2022). *Cryptography.* IBM. https://www.ibm.com/docs/es/ibm-mq/9.0?topic=concepts-cryptography

Incibe. (2 de mayo de 2019). *Día Mundial de las Contraseñas: Aún utilizas "123456".* Incibe. https://www.incibe.es/protege-tu-empresa/blog/dia-mundial-las-contrasenas-aun-utilizas-123456

Incibe. (16 de enero de 2020). *Las 7 fases de un ciberataque, ¿las conoces?* Incibe. https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

Infospyware. (30 de agosto de 2021). *¿Qué es el phishing, cómo funciona y cómo protegerte?* Esferize. https://www.esferize.com/que-es-el-phishing-como-funciona-y-como-protegerte/

Ionos. (14 de octubre de 2020). *Función Hash: ¿Qué es y para qué sirve?* Ionos. https://www.ionos.es/digitalguide/servidores/seguridad/funcion-hash/

Jesús. (4 de mayo de 2022). *¿Qué es Kali Linux?* Dongee. https://www.dongee.com/tutoriales/que-es-kali-linux/

Kali. (2023). *Kali Linux Tools.* Kali. https://www.kali.org/tools/

Kaspersky. (9 de diciembre de 2021). *Virus y gusanos.* Kaspersky. https://www.kaspersky.es/resource-center/threats/viruses-worms

Kaspersky. (2022). *What is Cybersecurity?* Kaspersky. https://latam. kaspersky.com/resource-center/definitions/what-is-cyber-security

Lawrence, A. (12 de octubre de 2021). *Un ciberataque cierra el banco más grande de Ecuador, Banco Pichincha*. BleepingComputer. https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-ecuadors-largest-bank-banco-pichincha/

Life, B. (10 de abril de 2019). *Gestor de contraseñas: Cambiará la seguridad en línea*. BitLife Media. https://bitlifemedia.com/2019/04/gestor-de-contrasenas-cambiara-seguridad-online/

Malwarebytes. (2018). *Malware: ¿Qué es y cómo protegerte?* Malwarebytes. https://es.malwarebytes.com/malware/

Márquez, J. (2019). *Metodología de la Investigación*. Academia.edu. https://www.academia.edu/38170551/Metodologia_de_la_investigacion_Sampieri_pdf

Medina, E. (19 de agosto de 2022). *Razones para elegir Linux sobre Windows*. MuyComputer. https://www.muycomputer.com/2022/08/19/razones-linux-windows/

Metasploit. (8 de noviembre de 2023). *¿Qué es Metasploit y cómo utilizarlo correctamente?* PC Hardware Pro. https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente/

Muñoz, F. (21 de mayo de 2021). *¿Qué es un virus troyano en informática?* WeLiveSecurity. https://www.welivesecurity.com/la-es/2021/05/14/que-es-virus-troyano-informatica/

Nmap. (2023). *Manual de Nmap.* Nmap. https://nmap.org/man/es/index.html

Noel. (6 de septiembre de 2022). *11 razones para usar Linux*. LiGNUx. https://lignux.com/11-razones-para-usar-linux/

Ortíz, S. (2019). Hackers lanzan ofensiva global, atacan a Ecuador. El Comercio. https://www.elcomercio.com/actualidad/seguridad/hackers-ofensiva-global-ataque-ecuador.html

OSI. (20 de febrero de 2019). *Típicos errores que cometemos al usar nuestras contraseñas y cómo evitarlos.* OSI. https://www.osi.es/es/actualidad/blog/2019/02/20/tipicos-errores-que-cometemos-al-usar-nuestras-contrasenas-y-como

Owaida, A. (5 de enero de 2021). *Formas comunes en que los dispositivos pueden infectarse con malware.* WeLiveSecurity. https://www.welivesecurity.com/la-es/2021/01/05/formas-comunes-dispositivos-pueden-infectarse-con-malware/

Pérez, A. (2020). *La Seguridad en las Redes.* Google Books. https://books.google.es/books?hl=es&lr=&id=tbzTDwAAQBAJ&oi=fnd&pg=PP1&dq=seguridad+en+la+red&ots=

Proofpoint. (23 de diciembre de 2020). *Ransomware.* Proofpoint. https://www.proofpoint.com/us/threat-reference/ransomware

Reydes. (18 de noviembre de 2019). Algo de historia sobre Kali Linux. Reydes. https://www.reydes.com/d/?q=Algo_de_Historia_sobre_Kali_Linux

Rosenthal, M. (2018). *5 Tipos de Ciberseguridad*. Mind Core. https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-security/

Rudra, A. (18 de octubre de 2022). *¿Qué es Smishing?*. PowerDMARC. https://powerdmarc.com/es/what-is-smishing/

Sampieri, R. (2010). *Metodología de la Investigación*. Academia.edu. https://www.academia.edu/38170551/Metodologia_de_la_investigacion_Sampieri_pdf

Sardanyés, E. (30 de junio de 2022). *Pérdida de datos por ataques de malware en empresas.* ESED SL. https://www.esedsl.com/blog/perdida-datos-por-ataques-de-malware-empresas

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Orozco Crespo Samir Isaac**, con C.C: # **0922286554** autor del trabajo de titulación: **Ciberataques en el Ecuador que afectan a las PYMES, y análisis de sus vulnerabilidades con Linux,** previo a la obtención del título de **Ingeniero en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, **15** de f**ebrero** del **2024**

f. _____

Nombre: Orozco Crespo, Samir Isaac
C.C: 0922286554

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TEMA Y SUBTEMA:	Ciberataques en el Ecuador que afectan a las PYMES, y análisis de sus vulnerabilidades con Linux.		
AUTOR(ES)	Orozco Crespo Samir Isaac		
REVISOR(ES)/TUTOR(ES)	Ing. Ricardo Xavier Ubilla González, MsC		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones con mención en gestión empresarial		
FECHA DE PUBLICACIÓN:	15 de febrero del 2024	No. DE PÁGINAS:	163
ÁREAS TEMÁTICAS:	Seguridad de la Red, Sistemas Informáticos, Empresas.		
PALABRAS CLAVES/ KEYWORDS:	Ciberseguridad, Ataques Informáticos, Ransomware, Phishing, Malware, Puertos, Vulnerabilidades		

RESUMEN:

Este proyecto de investigación tiene como objetivo analizar los ciberataques que afectan a las Pymes del Ecuador y sus vulnerabilidades utilizando Linux y sus herramientas como Nessus, para encontrar fallos en la red y poder luego parcharlos. Se centra en los sistemas operativos mal configurados, la relevancia de actualizaciones, la exposición a diversos ataques externos y el impacto de mantener parches de seguridad y actualizar los sistemas e incluso los registros para minimizar el riesgo de que los ciberataques no logren explotar los puertos abiertos y obtener el control de forma remota para que no puedan escalar privilegios dentro de él. A la vez de comprender la importancia de no tener servicios activos del sistema sino se van a usar ya que es una compuerta abierta para filtraciones de datos Se enfatiza la formación continua en ciberseguridad para prevenir ataques e identificarlos para no caer en manos de ciberdelincuente por un desconocimiento de los métodos de ataques.

ADJUNTO PDF:	SI X	NO
CONTACTO CONAUTOR:	**Teléfono:** +593-969979306	**E-mail:** samirorozco87@gmail.com
CONTACTO CON LA INSTITUCIÓN(COORDINADOR DEL PROCESO UTE):	**Nombre:** Ing. Ricardo Xavier Ubilla González, MsC.	
	Teléfono: +593-999528515	
	E-mail: ricardo.ubilla@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	