FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

EFECTO DEL HACKING ÉTICO EN LA INFRAESTRUCTURA INFORMÁTICA DE LA NOTARÍA CAVIDES LUNA - PUNCHANA 2021

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS INFORMÁTICA

PRESENTADO POR:

FRANCO ANIELLO DÁVILA LAGE

JORGE MIGUEL JOSSEMAIR BRAYN ICOMEDES GARCÍA

ASESOR:

Lic. MANUEL TUESTA MORENO, Mgr.

IQUITOS, PERÚ

2021

ACTA DE SUSTENTACIÓN

UNAP

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE SUSTENTACIÓN DE TESIS – 2021

En Iquitos, en la modalidad presencial, a los **17** días del mes de **diciembre del 2021**, a horas **7:00pm**, se dio inicio a la sustentación de la Tesis titulada: "***EFECTO DEL HACKING ÉTICO EN LA INFRAESTRUCTURA INFORMÁTICA DE LA NOTARIA CAVIDES LUNA – PUNCHANA 2021***", Aprobado con **Resolución Decanal N° 200-D-FISI-UNAP-2021**, presentado por los Bachilleres: Franco Aniello Dávila Lage **y Jorge Miguel Jossemair Brayn Icomedes García**, para optar el Título Profesional de **Ingeniero de Sistemas e Informática.**, que otorga la Universidad de acuerdo a Ley y Estatuto.

El Jurado calificador y dictaminador designado mediante **Resolución Decanal N° 195-D-FISI-UNAP-2021**, está integrado por:

- ✓ Lic. Ángel Enrique López Rojas, Dr. — Presidente
- ✓ Ing. Alejandro Reátegui Pezo, Dr. — Miembro
- ✓ Ing. José Edgar García Díaz, Mgr. — Miembro

Luego de haber el Jurado escuchado con atención y formulado las preguntas necesarias, las cuales fueron respondidas: CORRECTAMENTE.

El jurado después de las deliberaciones correspondientes, llegó a las siguientes conclusiones:

La Sustentación de la Tesis ha sido: APROBADO con la calificación de: 18

Estando los Bachilleres aptos para obtener el Título Profesional de **Ingeniero de Sistemas e Informática.**

Siendo las 19:35 se dio por terminado el acto de sustentación.

Lic. Ángel Enrique López Rojas, Dr.
Presidente

Ing. Alejandro Reátegui Pezo, Dr.
Miembro

Ing. José Edgar García Díaz, Mgr.
Miembro

Lic. Manuel Tuesta Moreno, Mgr.
ASESOR

TESIS APROBADA EN SUSTENTACIÓN PÚBLICA EL DÍA VIERNES 17 DE DICIEMBRE DEL 2021

EFECTO DEL HACKING ÉTICO EN LA INFRAESTRUCTURA INFORMÁTICA DE LA NOTARÍA CAVIDES LUNA PUNCHANA 2021

Lic. Angel Enrique López Rojas, Dr.
Presidente

Ing. Alejandro Reátegui Pezo, Dr.
Miembro

Ing. José Edgar García Díaz, Mgr.
Miembro

Lic. Manuel Tuesta Moreno, Mgr.
Asesor

A mi dios Jehová, por su infinita misericordia,
a mi madre Marisa por haber luchado y ser
mi sostén para lograr mis metas, y a mi
hija Ainhoa por darme un motivo
de vivir día a día.

Aniello

A Dios, por sobre todas las cosas, a mis padres
Jorge Luis y Madita, por ser mi ejemplo y
apoyo incondicional; y a mis hijos
Jhossif y Fabiano, que día a día
son la motivación más
grande en mi vida.

Jorge

AGRADECIMIENTO

- A mi alma máter, Universidad Nacional de la Amazonía Peruana, por la formación en ciencias, tecnológica y humanidades, promoviendo el desarrollo de la región Loreto.
- A la facultad de Ingeniería de Sistemas e Informática, por acogernos entre sus aulas y formarnos como profesionales.
- A los docentes de la facultad de Ingeniería de Sistemas e Informática, quienes nos brindaron los conocimientos necesarios para nuestro desarrollo profesional.
- A nuestro asesor, Manuel Tuesta Moreno, por su dedicación al guiarnos y acompañarnos en este hermoso viaje que fue la presente investigación.
- Al notario Jorge Isidoro Cavides Luna, por permitir la ejecución de la presente investigación en su notaría.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE GRÁFICOS

Pág.

RESUMEN

La presente investigación tuvo como objetivo, determinar el efecto del hacking ético en la infraestructura informática de la notaría Cavides Luna – Punchana 2021, en consecuencia, de los miles de intentos en ciberataque que se están presentando en todo el Perú, además de cumplir con lo que indica la ley 29733 “ley de protección de datos personales”, planteándose la siguiente interrogante ¿Cuál es el impacto del hacking ético a la infraestructura informática en relación a la ciberseguridad en la notaría Cavides Luna - Punchana 2021?. Para ello se formuló como hipótesis general “la aplicación del hacking ético mejora la seguridad de la infraestructura informática en términos de la confidencialidad, integridad y disponibilidad de la información en la notaría Cavides Luna - Punchana 2021”, la investigación fue de tipo aplicada, con intervención no experimental, analítico, longitudinal y prospectivo. Recolectando datos por medio de la observación directa haciendo uso de fichas de observación, los cuales fueron procesados con el software IBM SPSS Statistics versión 22, para determinar las diferencias se aplicó la estadística no paramétrica Chi Cuadrado de homogeneidad con un nivel de significancia del 5%; obteniendo como resultado una mejora en términos de confidencialidad e integridad de 0% a 48.1%, y en términos de disponibilidad de 0% a 51.9%, en cuanto a la ciberseguridad se refiere. Llegando a la conclusión de que existe una diferencia significativa en cuanto a la ciberseguridad con respecto a la confidencialidad, integridad y disponibilidad.

Palabras claves: hacking ético, ciberseguridad, seguridad informática, infraestructura informática.

ABSTRACT

The objective of this research was to determine the effect of ethical hacking on the computer infrastructure of the Cavides Luna - Punchana 2021 notary public office, consequently, of the thousands of cyberattack attempts that are being presented throughout Peru, in addition to complying with the that indicates the law 29733 "law of protection of personal data", posing the following question: What is the impact of ethical hacking to the computer infrastructure in relation to cybersecurity in the Cavides Luna - Punchana 2021 notary's office? For this, the general hypothesis was formulated "the application of ethical hacking improves the security of the computer infrastructure in terms of confidentiality, integrity and availability of information in the Cavides Luna - Punchana 2021 notary's office", the investigation was of an applied type, with non-experimental, analytical, longitudinal and prospective intervention. Collecting data through direct observation using observation files, which were processed with the IBM SPSS Statistics version 22 software, to determine the differences, the non-parametric Chi-square statistic of homogeneity was applied with a significance level of 5%; Obtaining as a result an improvement in terms of confidentiality and integrity from 0% to 48.1%, and in terms of availability from 0% to 51.9%, in terms of cybersecurity is concerned. Concluding that there is a significant difference in cybersecurity with respect to confidentiality, integrity and availability.

Keywords: ethical hacking, cybersecurity, IT security, IT infrastructure

INTRODUCCIÓN

Según el laboratorio de análisis e inteligencia de amenazas de la compañía FortiGuard Labs, el Perú ocupa la tercera ubicación en América Latina en ataques cibernéticos, con más de 4,700 millones de intentos en ciberataques en lo que va del primer semestre del año 2021; lo cual podemos ver algunos casos que sucedieron en el Perú, como la vulneración de la plataforma del Bono Familiar Universal para apropiarse de dinero (Neyra, 2020), el hackeo a la página web del diario Expreso (La Republica, 2020) y en el ámbito local a las instituciones en nuestra región, como tal es el caso del intento de ataque cibernético al Gobierno Regional de Loreto donde un grupo de hackers intentaron apoderarse ilegalmente de 5 millones 200 mil soles de los fondos de la institución (Gobierno Regional de Loreto, 2021).

Es por ello que la administración de la notaría Cavides Luna decide llevar a cabo una auditoria de seguridad de la información por medio de un proceso de hacking ético, con el cual se obtiene el estado actual de los equipos de cómputo, analizándose las vulnerabilidades en su infraestructura informática, lo cual nos lleva a adoptar acciones correctivas, mitigando en lo máximo posible la exposición de su información, surgiendo la siguiente interrogante:

¿Cuál es el impacto del hacking ético a la infraestructura informática en relación a la ciberseguridad en la notaría Cavides Luna - Punchana 2021?

Con la finalidad de responder la interrogante, se plantea como objetivo general:

Determinar el efecto del hacking ético en la infraestructura informática de la notaría Cavides Luna – Punchana 2021.

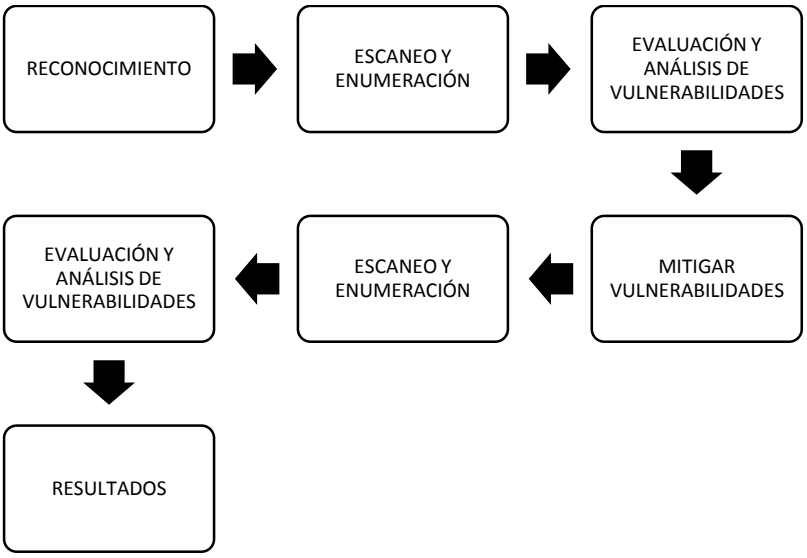
Además, se plantean los siguientes objetivos específicos:

- Evaluar las vulnerabilidades de red en la infraestructura informática de la notaría Cavides Luna – Punchana 2021 previo a la aplicación del hacking ético.
- Evaluar las vulnerabilidades de red en la infraestructura informática de la notaría Cavides Luna – Punchana 2021 con la aplicación del hacking ético.
- Determinar si existe diferencia significativa, entre el estado anterior y el estado actual con la aplicación del hacking ético en la ciberseguridad de la infraestructura informática de la notaría Cavides Luna – Punchana 2021.

El hacking ético a la infraestructura informática de la notaría Cavides Luna es de mucha importancia porque genera beneficios a la misma, en las cuales se identifican las debilidades de seguridad informática, vulnerabilidades de red, sistemas desactualizados, información sensible expuesta, niveles de accesos a su información sin ningún control, sistemas sin contraseñas y malas prácticas en el uso de su información, permitiendo con todo ello, realizar las acciones correctivas y así subsanarlas y/o eliminarlas.

En el diseño metodológico se tiene como propósito de investigación, la investigación aplicada con intervención no experimental en la que se demuestra una relación causal analítico, con medición longitudinal y de toma de datos prospectivo, teniendo como población de estudio 27 dispositivos informáticos los cuales constituyen la infraestructura informática de la notaría Cavides Luna, y tomando como muestra todos los elementos de la población.

Se realizará el hacking ético de tipo interno, en la modalidad de hacking de caja gris, y para la aplicación del hacking ético, se siguen las siguientes fases:



Fuente: Elaboración propia.

Además, no existe limitación para la aplicación del proceso de hacking ético, por ser una solución informática y contar con la autorización de la administración de la Notaría Cavides Luna, respetando siempre la confidencialidad de los datos.

La presente investigación se encuentra estructurada de la siguiente manera:

Capítulo I Marco Teórico, en el cual se habla de investigaciones previas con el hacking ético, y sobre las bases teóricas necesarias para la realización de la presente investigación, además, de definir los términos básicos.

Capítulo II Hipótesis y variables, en el cual se menciona la formulación de la hipótesis general y las hipótesis específicas, y además de la variable independiente que es el hacking ético y la variable dependiente que es la infraestructura informática de la notaría Cavides Luna.

Capítulo III Metodología, tenemos el diseño metodológico en el cual se menciona el enfoque de investigación, el tipo y diseño de la misma, la población de estudio que consta de los 27 dispositivos que conforman la infraestructura informática, el procedimiento de recolección de datos basándose en los procedimientos del hacking ético, técnicas e instrumentos de recolección de datos que consta en la observación directa y fichas de observación, procesamiento y análisis de datos por medio de la prueba estadística Chi Cuadrado de homogeneidad con un nivel de significancia del 5% y mencionando los aspectos éticos para la ejecución de la presente investigación.

Capítulo IV Resultados, se mencionan los hallazgos obtenidos en la investigación referentes a confidencialidad, integridad y disponibilidad.

Capítulo V Discusión, se contrasta los resultados obtenidos comparándolos con el resultado de otras investigaciones y conocimientos.

Capítulo VI Conclusiones, se menciona la existencia de la diferencia significativa entre el estado anterior y el actual de la infraestructura informática luego de la aplicación del hacking ético.

Capítulo VII Recomendaciones, se dan a conocer las recomendaciones propuestas por el equipo de investigación.

Capítulo VIII Referencias bibliográficas, en ella se mencionan las fuentes de información que sustentan la realización de la presente investigación.

Por último, tenemos los Anexos en la parte final del presente documento.

CAPÍTULO I: MARCO TEÓRICO

1.1. Antecedentes

En 2020, se desarrolló la investigación de tipo descriptivo y diseño no experimental que incluyó como población de estudio los trabajadores del área de soporte y redes de la empresa Infonet Soluciones E.I.R.L. en la que se determinó ejecutar un ethical hacking al servidor de la empresa Infonet Soluciones E.I.R.L. para detectar vulnerabilidades de seguridad que exponga los datos de la empresa y en el que se concluyó que la versión MS Windows 2008 Server R2 es muy vulnerable, existiendo además un bajo conocimiento en seguridad informática de los profesionales de TI. (Criollo Ortiz, 2020)

En 2020, se desarrolló una investigación que incluyó como población de estudio a la infraestructura informática del Grupo Electrodata realizándose un hacking ético para mejorar la seguridad en la infraestructura informática del grupo electrodata en el que se concluyó que la explotación de las vulnerabilidades que presenta la infraestructura informática puede comprometer de forma critica la información sensible que posee el Grupo Electrodata, evidenciado que cualquier dispositivo conectado a la red informática de grupo Electrodata tiene visibilidad completa de toda la infraestructura informática. (Tovar Romero, 2020)

En 2020, se desarrolló una investigación que tiene como objetivo, detectar las intrusiones a la red de datos de la Municipalidad Distrital de Victor Larco Herrera – Trujillo, llevando a los atacantes hacia una red controlada haciéndoles creer que se encuentran dentro de la red real de la Municipalidad Distrital de Victor Larco Herrera, y de esa forma, identificar los métodos que

utiliza el atacante y cuál es su objetivo para así mejorar la seguridad de la red en el sistema real, y en la cual se concluyó que mediante una red Honeypot nos ayuda a determinar cuáles son las intenciones de un atacante hacia nuestra infraestructura y que métodos utiliza para llevar a cabo sus objetivos, siendo una opción muy viable para proteger nuestro sistema de red informático. (Valdiviezo Avalo, 2020).

En 2017, se desarrolló una investigación de tipo descriptivo y diseño no experimental que incluyó como población de estudio los trabajadores de la empresa Complex del Perú S.A.C., en la que se determinó la detección y evaluación de vulnerabilidades de red a las que se encuentra expuesta la empresa Complex del Perú S.A.C. y en el que se concluyó evaluar los problemas de vulnerabilidades de red y formular propuestas tecnologías de seguridad. (Bermeo Oyola, 2017).

En 2016, se desarrolló una investigación de tipo aplicativo y de diseño pre experimental, teniendo como objetivo evaluar la forma en que el uso de la herramienta de ethical hacking ayudara con el diagnostico de vulnerabilidades de la seguridad de la información en la red de la sede central de la universidad de Huánuco, concluyendo que la red cuenta con muchas vulnerabilidades que comprometen la confidencialidad, integridad y disponibilidad de la información en la red de la sede central de la universidad de Huánuco. (Gonzales Cotera, 2016).

1.2. Bases teóricas

1.2.1. Seguridad de la información

“Es un conjunto de medidas preventivas y acciones que permiten proteger la información” (Fundación Wikimedia, Inc., 2021), pretendiendo mantener la **confidencialidad**, el cual se refiere a que la información solo puede ser accedida por personas o usuarios autorizados; **integridad**, se refiere a que la información no haya sido alterada o modificada y se mantenga tal cual fue almacenada o generada; y **disponibilidad** la cual hace referencia a que la información sea accesible en cualquier momento para las personas o usuarios autorizados, (UNIR, 2021) sin importar en que medio se encuentre, pudiendo ser medios físicos o medios informáticos.

1.2.1.1. Seguridad informática

Se enfoca en la protección de la información que se encuentra en medios informáticos, como pueden ser computadoras, dispositivos móviles, servidores, sistemas de redes y datos, etcétera. Otra definición de seguridad informática es la de proteger los sistemas informáticos de ataques maliciosos, identificando y mitigando las vulnerabilidades existentes. (Fundación Wikimedia, Inc., 2021)

1.2.2. Base legal informática

Para el tratamiento de los datos personales, se debe adoptar medidas correspondientes que garanticen su seguridad y eviten la alteración, pérdida, tratamiento o acceso no autorizado, además los que intervengan en su tratamiento, están obligados a guardar confidencialidad de los mismos. (Gobierno del Perú, 2011)

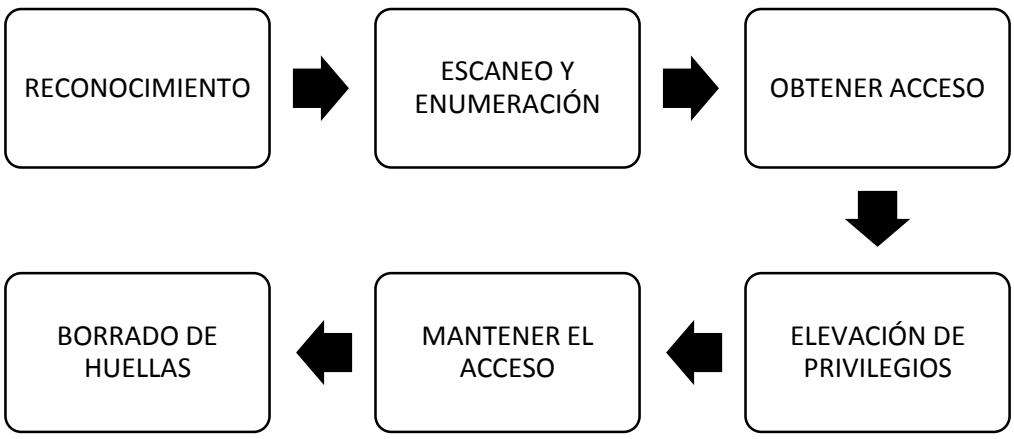
El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, vulnerando las medidas de seguridad establecidas para impedirlo o inutiliza, total o parcialmente, un sistema informático, impidiendo el acceso a este, entorpeciendo su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad. (Gobierno del Perú, 2013)

1.2.3. Hacking ético

Es una disciplina dentro del campo de la seguridad informática, cuyos procesos permiten detectar, investigar y explotar vulnerabilidades existentes en un sistema informático, mediante pruebas acordadas con el cliente para evaluar la seguridad física y lógica de la red donde se encuentran los sistemas. (Gonzáles Pérez, 2020).

Fases del hacking

Las fases del hacking ético lo basamos en la metodología de Certified Ethical Hacker (CEH) que traducido al español dice Certificación de Hacker Ético, el cual menciona 6 fases:



Fuente: Hacking Ético: Cacería de vulnerabilidades OWASP LATAM TOUR 2015.

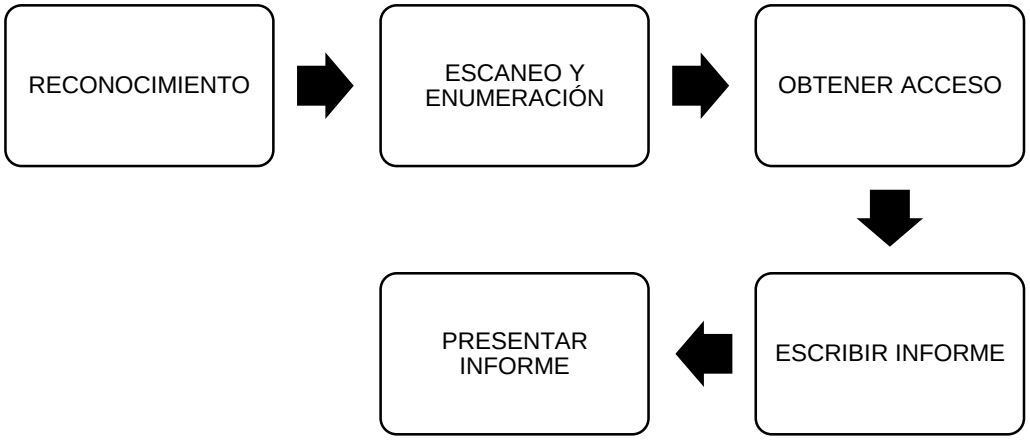
1. **Reconocimiento**. Llamado también footprinting, proceso por el cual se recopila la mayor cantidad de información relevante sobre el objetivo, teniendo como principal fuente al internet. Para la recopilación de la información hacemos uso de las siguientes herramientas:

    - Google/Bing Hacking.
    - Protocolo Whois.
    - Foca.
    - Maltego.
    - Ingenieria Social.

    (Gonzáles Pérez, 2020)

2. **Escaneo y enumeración**. Se identifican los hosts vivos, determinamos los puertos abiertos de dichos equipos, enumeramos los servicios que están ejecutándose en los hosts identificados. Para realizarlo tenemos diversas herramientas como: Nmap para el escaneo de puertos de los hosts y también permite el análisis de vulnerabilidades, Nessus para el análisis de vulnerabilidades de los hosts.
3. **Obtener acceso**. Se explotan las vulnerabilidades encontradas. Una de las herramientas que permiten la explotación de las vulnerabilidades es Metasploit, Core Impact Pro, Immunity Canvas.
4. **Mantener el acceso**. Se trata de retener la posesión sobre el objetivo atacado, para el cual debemos ser sigilosos en todas las acciones que realicemos dentro del sistema atacado, para evitar ser descubiertos por el personal o los sistemas de seguridad que posea el objetivo.
5. **Borrar huellas**. Se eliminan las evidencias del hackeo o intrusión. (Baeza Meza, 2019)

El hacking ético presenta una pequeña diferencia en relación a las fases del hacking, como se puede observar a continuación.



(Astudillo B., 2013)

Para llevar a cabo los procesos o fases del hacking ético, se realizan diversas pruebas tales como:

Auditoria de vulnerabilidades. En estas pruebas se tiene como objetivo la identificación de vulnerabilidades conocidas, existiendo una colaboración entre el auditor y la empresa, donde la empresa tiene total conocimiento de lo que se va a realizar.

Test de intrusión. En estas pruebas el auditor toma el rol de un atacante y se busca realizar intrusiones al sistema, tomando control sobre los equipos informáticos, donde la empresa tiene total conocimiento de lo que se va a realizar.

Ejercicios de Red Team. En estas pruebas se simula una intrusión real a un sistema y donde la empresa desconoce cuándo y por quien van a ser realizadas las acciones de intrusión. (Arriols Nuñez, 2016)

Tipos de Hacking Ético

Dependiendo desde donde se ejecuten las pruebas del hacking ético tenemos:

Hacking ético externo. Se realiza desde internet sobre la infraestructura informática pública del cliente.

Hacking ético interno. Se realiza desde la infraestructura informática interna del cliente, es decir se tiene acceso a la red interna del cliente.

Modalidades del hacking ético

Black box hacking (hacking de caja negra). Se aplica al hacking ético de tipo externo, porque el hacker ético solo conoce el nombre de la empresa o institución cliente.

Gray box hacking (hacking de caja gris). Se aplica al hacking ético de tipo interno; en ella el cliente proporciona cierta información, pero limitada al hacker ético.

White box hacking (hacking de caja blanca). Se aplica al hacking ético de tipo interno, en ella el cliente le brinda información detallada de toda la infraestructura informática que posee, también llamado hacking transparente.

1.3. Definición de términos básicos

- Hacking ético: Es una disciplina que ayuda a detectar, prevenir y mitigar las vulnerabilidades que posean los sistemas informáticos. (Gonzáles Pérez, 2020)
- Confidencialidad: Se refiere a la información que utilice, almacene o genere cada personal y que pueda ser accedida por el personal correspondiente. (UNIR, 2021)
- Integridad: Se refiere a la información se conserve tal cual fue recopilada, generada y almacenada por el personal, sin que haya sido modificado por algún factor externo. (UNIR, 2021)
- Disponibilidad: Se refiere a que la información esté disponible cuando se desee para el personal que cuente con autorización para tratar dicha información y no para el personal sin autorización. (UNIR, 2021)
- Hacker: Investigador de seguridad, alguien que disfruta de tener una comprensión profunda del funcionamiento de algún sistema, computadoras o redes de computadoras, con frecuencia se usa el termino en un contexto peyorativo. (IETF)
- Hacking: Es la acción o actividad que realiza un hacker.
- Host: Sistema particular en el que reside información valiosa. (Baeza Meza, 2019)
- Red: Conjunto de dispositivos conectados por medio de un canal de comunicación con el propósito de compartir información. (Baeza Meza, 2019)
- Malware: Archivo que pretende hacer algo dentro de una computadora sin el consentimiento del usuario. (Baeza Meza, 2019)

- Vulnerabilidad: Hace referencia a un punto débil en un sistema o red el cual puede ser utilizado por un atacante como punto de entrada para lograr su objetivo. (CEH v10 - EC Council)
- Exploit: Traducido al español significa explotar, el cual crea una brecha de seguridad en un sistema o red utilizando alguna vulnerabilidad existente. (CEH v10 - EC Council)
- Pentesting: Es el proceso por el cual evaluamos el nivel de seguridad de un sistema de información. (Baeza Meza, 2019)
- Ciberseguridad: conocida también como seguridad informática, que es un área el cual se enfoca en la protección de la infraestructura informática y todo lo relacionado con ésta. (Fundación Wikimedia, Inc., 2021)
- Ciberdelincuente: Alguien que valiéndose de técnicas hacking comete delitos informáticos.
- Delito informático; Es el acceso sin autorización a un sistema informático, vulnerando medidas de seguridad establecidas para permitir el acceso al sistema informático. (Gobierno del Perú, 2018)
- IP: Traducido al español significa Protocolo de Internet, es un protocolo de comunicación de datos y funciona en la capa de red de acuerdo al modelo de interconexión de sistemas abiertos (modelo OSI), el cual permite identificar un dispositivo dentro de una red. (Fundación Wikimedia, Inc., 2021)
- Google chrome: Es un motor de búsqueda en la web, que pertenece a la empresa Google LLC. (Fundación Wikimedia, Inc., 2021)

- Bing: Es un motor de búsqueda en la web, que pertenece a la empresa Microsoft, actualmente se llama Microsoft Bing. (Fundación Wikimedia, Inc., 2021)
- Foca: Es una herramienta para extracción de metadatos, además permite el descubrimiento de la red y búsqueda de vulnerabilidades. (Alonso, y otros, 2016)
- Nmap: Network Mapper que es español significa mapeador de red. Es una herramienta para el descubrimiento de redes y auditoria de seguridad. Es de código abierto y gratuito. (NMAP)
- Metasploit: Es un framework que posee un conjunto herramientas para desarrollar y ejecutar exploits contra los equipos a auditar. (Gonzáles Pérez, y otros, 2015)
- Burp suite: Es una herramienta para el análisis de vulnerabilidades web. (Gonzáles Pérez, y otros, 2015)
- Kali linux: Es una distribución que está basada en Debian, y que contiene cientos de herramientas para realizar pentest y auditoria, en el ámbito de la seguridad informática, además de permitir el análisis forense, reversing, gathering o la explotación; esta distribución es gestionada por offensive security. (Gonzáles Pérez, y otros, 2015)
- Nessus: Es una herramienta para el escaneo y análisis de vulnerabilidades de sistemas informáticos, desarrollado por Tenable Network Security. (Gonzáles Pérez, y otros, 2015).

CAPÍTULO II: HIPÓTESIS Y VARIABLES

2.1. Formulación de la hipótesis

Hipótesis general:

- La aplicación del hacking ético mejora la seguridad de la infraestructura informática en términos de la confidencialidad, integridad y disponibilidad de la información en la notaría Cavides Luna - Punchana 2021.

Hipótesis específica:

- La aplicación del hacking ético mejora la confidencialidad de la infraestructura informática de la notaría Cavides Luna - Punchana 2021.
- La aplicación del hacking ético mejora la integridad de la infraestructura informática de la notaría Cavides Luna - Punchana 2021.
- La aplicación del hacking ético mejora la disponibilidad de la infraestructura informática de la notaría Cavides Luna - Punchana 2021.

2.2. Operacionalización de variables

Variable	Definición	Tipo por su naturaleza	Indicador	Escala de medición	Categorías	Valores de la categoría	Medios de verificación
Independiente: hacking ético	Es una disciplina que ayuda a detectar, prevenir y mitigar las vulnerabilidades que posean los sistemas informáticos.	Cualitativa	Aplicar hacking ético	Ordinal	No aplica hacking ético (Antes) Aplica hacking ético (después)	0 1	Infraestructura informática de la notaría Cavides Luna 2021

Variable	Definición	Dimensiones	Tipo por su naturaleza	Indicador	Escala de medición	Categorías	Valores de la categoría	Medios de verificación
Dependiente: Infraestructura Informática de la notaría Cavides Luna 2021	Es el conjunto de sistemas informáticos (redes, computadoras, modem, cámaras de vigilancia) que se utiliza para la recopilación, monitoreo, almacenamiento y generación de información para el negocio.	**Confidencialidad**: Se refiere a la información que utilice, almacene o genere cada personal y que pueda ser accedida por el personal correspondiente.	Cualitativa	El respectivo personal accede a la información almacenada.	Nominal	El personal autorizado y no autorizado tiene acceso a toda la información almacenada.	0	Infraestructura informática de la notaría Cavides Luna 2021
						Solo el personal autorizado tiene acceso a la información almacenada correspondiente.	1	
		Integridad: Se refiere a la información se conserve tal cual fue recopilada, generada y almacenada por el personal, sin que haya sido modificado por algún factor externo.	Cualitativa	La información almacenada no presenta modificaciones.	Nominal	La información almacenada puede ser modificada por el personal autorizado y no autorizado.	0	
						La información almacenada puede ser modificada solo por el personal autorizado.	1	
		Disponibilidad: Se refiere a que la información esté disponible cuando se desee para el personal que cuente con autorización para tratar dicha información y no para el personal sin autorización.	Cualitativa	La información está disponible en el momento que sea requerido por el personal autorizado.	Nominal	No está disponible la información en el momento requerido.	0	
						Está disponible la información en el momento requerido	1	

CAPÍTULO III: METODOLOGÍA

3.1. Diseño metodológico

Enfoque: cuantitativo, porque se utilizó la estadística para lograr responder la interrogante, los objetivos y probar la hipótesis.

Tipo de investigación:

- Según propósito de la investigación: es **aplicada**, porque se mitigan los problemas de seguridad que posee la infraestructura informática de la notaría Cavides Luna, en cuanto a confidencialidad, integridad y disponibilidad de la información.
- Según la intervención del investigador: es **con intervención no experimental** porque se analizan los efectos del hacking ético en la infraestructura informática de la notaría Cavides Luna – Punchana 2021.
- Según el alcance que tienen de demostrar una relación causal: es **analítico** porque se busca establecer una relación causa – efecto entre el hacking ético y la mejora de la seguridad en la infraestructura informática de la notaría Cavides Luna – Punchana 2021.
- Según el número de mediciones: es **longitudinal** porque se realizan dos mediciones de la variable dependiente, antes y después de la implementación del hacking ético.
- Según la planificación de la toma de datos: es **prospectivo** porque se recopilan datos durante la investigación.

Diseño de la investigación:

Se usa un diseño longitudinal de tendencia por que se analiza el efecto del hacking ético en la infraestructura informática de la notaría Cavides Luna – Punchana 2021; dicho efecto se observa desde agosto a octubre del 2021.

$$G.: O_1 \quad X \quad O_2$$

G: Población (infraestructura informática desde agosto a octubre del 2021).

O_1: Evaluación de vulnerabilidades de la infraestructura informática antes de la aplicación del hacking ético.

X: Aplicación del hacking ético y medidas correctivas.

O_2: Evaluación de vulnerabilidades de la infraestructura informática después de la aplicación del hacking ético.

3.2. Diseño muestral

Población de estudio. Está constituida por 27 dispositivos informáticos.

Muestra. La investigación analiza todos los elementos de la población.

Muestreo. Es censal, porque se analizan todos los dispositivos informáticos considerados en la población.

3.3. Procedimientos de recolección de datos

- Identificación de los dispositivos electrónicos parte de la infraestructura informática de la notaría Cavides Luna.

- Evaluación de vulnerabilidades en la infraestructura informática antes de la implementación del hacking ético.
- Análisis de vulnerabilidades.
- Mitigación de vulnerabilidades.
- Evaluación de vulnerabilidades en la infraestructura informática después de la implementación del hacking ético.
- Análisis de datos.
- Elaboración de resultados, discusión, conclusiones y recomendaciones referente a la ciberseguridad de la infraestructura informática de la notaría Cavides Luna.

3.4. Técnicas e instrumentos de recolección de datos

- **Técnicas**: Observación directa.
- **Instrumentos**: Ficha de observación (anexo 02).

3.5. Procesamiento y análisis de datos

Para el procesamiento de los datos se usa el software informático IBM SPSS Statistics versión 22.0, en español, para Windows.

Para el análisis descriptivo de la infraestructura informática de la notaría Cavides Luna, respecto a las dimensiones de confidencialidad, integridad y disponibilidad, se usa tablas estadísticas para variable cualitativa, frecuencia, porcentaje y moda; y para determinar las diferencias entre antes y después de la aplicación del hacking ético, se aplicó la estadística no paramétrica Chi Cuadrado de homogeneidad con un nivel de significancia del 5%.

3.6. Aspectos éticos

- Carta de aceptación de la notaría Cavides Luna (anexo 03).
- Carta de conformidad de ejecución del plan de tesis (anexo 04).
- Conforme al artículo 17 (confidencialidad de datos personales) de la ley de protección de datos personales (ley N° 29733) nos vemos en la obligación de guardar confidencialidad respecto a los datos utilizados para la presente investigación.

CAPÍTULO IV: RESULTADOS

4.1. Confidencialidad de la infraestructura informática.

Tabla N° 01

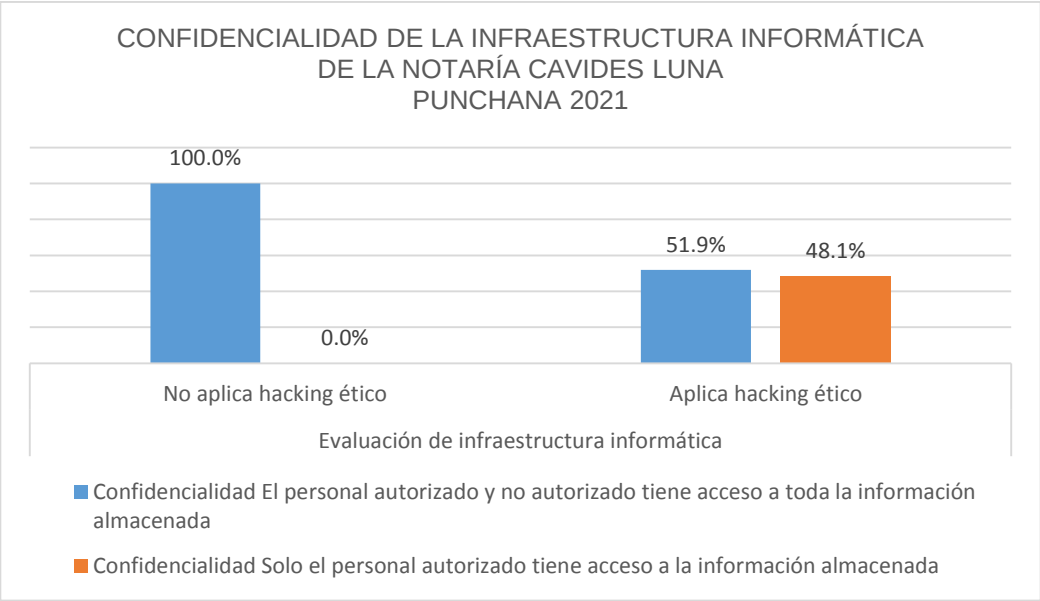
CONFIDENCIALIDAD DE LA INFRAESTRUCTURA INFORMÁTICA
DE LA NOTARÍA CAVIDES LUNA
PUNCHANA 2021

			Evaluación de infraestructura informática	
			No aplica hacking ético	Aplica hacking ético
Confidencialidad	El personal autorizado y no autorizado tiene acceso a toda la información almacenada	Recuento	27	14
		% dentro de Evaluación de infraestructura informática	100.0%	51.9%
	Solo el personal autorizado tiene acceso a la información almacenada	Recuento	0	13
		% dentro de Evaluación de infraestructura informática	0.0%	48.1%
Total		Recuento	27	27
		% dentro de Evaluación de infraestructura informática	100.0%	100.0%

Fuente: Ficha de observación aplicada

P – valor del Chi Cuadrado de homogeneidad: 0.00

Gráfico N° 01



Fuente: Ficha de observación aplicada

Interpretación:

De los resultados mostrados en la tabla y gráfico N° 01, sobre la evaluación de confidencialidad a 27 dispositivos de la infraestructura informática de la notaría Cavides Luna - Punchana 2021, se puede afirmar que:

- La evaluación, antes de aplicar el hacking ético, 100%, en los 27 dispositivos, permitían el acceso a la información almacenada al personal autorizado y no autorizado.
- La evaluación, después de aplicar el hacking ético, 51.9%, o sea en 14 dispositivos, podían acceder a la información almacenada el personal autorizado y no autorizado; y, 48.1%, en 13 dispositivos, podían acceder a la información almacenada solo el personal autorizado.

El P – valor del Chi Cuadrado de homogeneidad de 0.00, indica que se acepta la hipótesis del investigador.

4.2. Integridad de la infraestructura informática.

Tabla N° 02

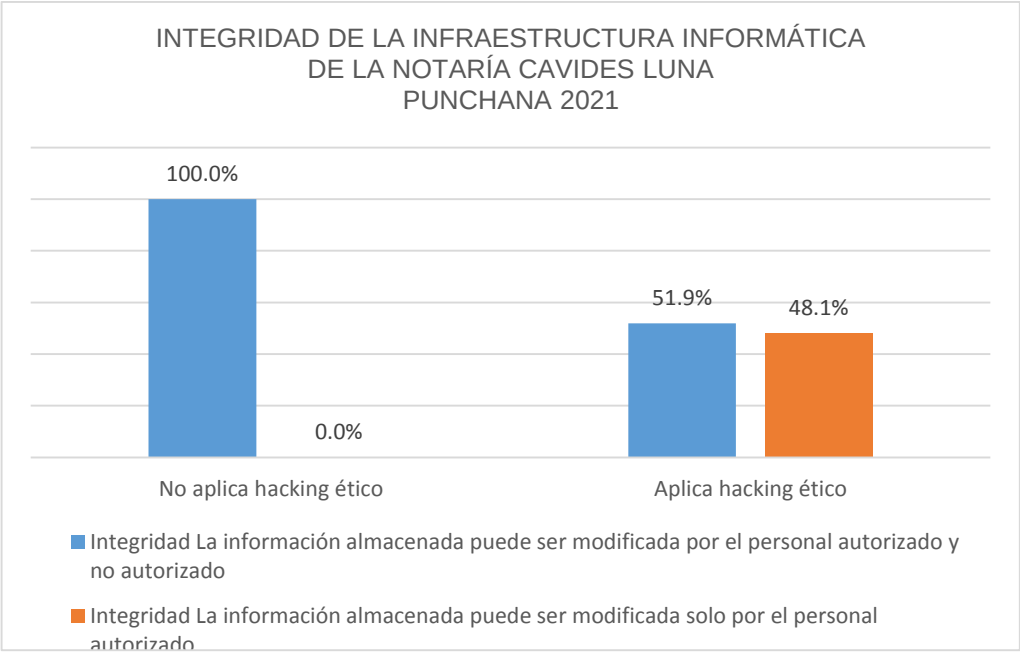
INTEGRIDAD DE LA INFRAESTRUCTURA INFORMÁTICA
DE LA NOTARÍA CAVIDES LUNA
PUNCHANA 2021

			Evaluación de infraestructura informática	
			No aplica hacking ético	Aplica hacking ético
Integridad	La información almacenada puede ser modificada por el personal autorizado y no autorizado	Recuento	27	14
		% dentro de Evaluación de infraestructura informática	100.0%	51.9%
	La información almacenada puede ser modificada solo por el personal autorizado	Recuento	0	13
		% dentro de Evaluación de infraestructura informática	0.0%	48.1%
Total		Recuento	27	27
		% dentro de Evaluación de infraestructura informática	100.0%	100.0%

Fuente: Ficha de observación aplicada

P – valor del Chi Cuadrado de homogeneidad: 0.00

Gráfico N° 02



Fuente: Ficha de observación aplicada

Interpretación:

De los resultados mostrados en la tabla y gráfico N° 02, sobre la evaluación de integridad a 27 dispositivos de la infraestructura informática de la notaría Cavides Luna - Punchana 2021, se puede afirmar que:

- La evaluación, antes de aplicar el hacking ético, 100%, en los 27 dispositivos, permitían la modificación de la información almacenada al personal autorizado y no autorizado.
- La evaluación, después de aplicar el hacking ético, 51.9%, o sea en 14 dispositivos, permitían la modificación de la información almacenada el personal autorizado y no autorizado; y, 48.1%, en 13 dispositivos, permitían la modificación de la información almacenada solo al personal autorizado.

El P – valor del Chi Cuadrado de homogeneidad de 0.00, indica que se acepta la hipótesis del investigador.

4.3. Disponibilidad de la infraestructura informática

Tabla N° 03

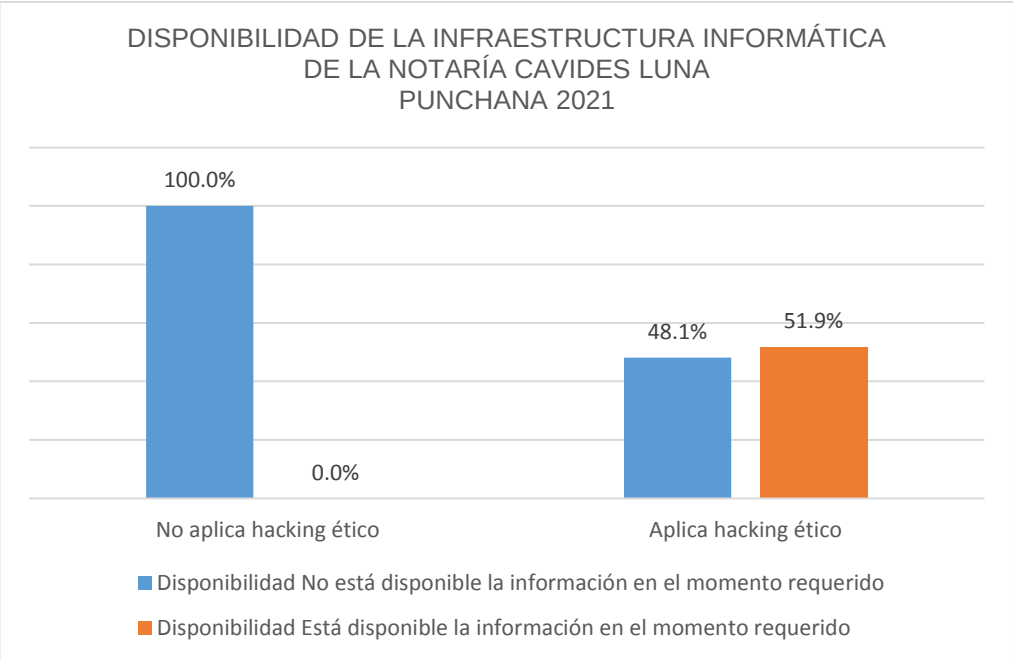
DISPONIBILIDAD DE LA INFRAESTRUCTURA INFORMÁTICA
DE LA NOTARÍA CAVIDES LUNA
PUNCHANA 2021

			Evaluación de infraestructura informática	
			No aplica hacking ético	Aplica hacking ético
Disponibilidad	No está disponible la información en el momento requerido	Recuento	27	13
		% dentro de Evaluación de infraestructura informática	100.0%	48.1%
	Está disponible la información en el momento requerido	Recuento	0	14
		% dentro de Evaluación de infraestructura informática	0.0%	51.9%
Total		Recuento	27	27
		% dentro de Evaluación de infraestructura informática	100.0%	100.0%

Fuente: Ficha de observación aplicada

P – valor del Chi Cuadrado de homogeneidad: 0.00

Gráfico N° 03



Fuente: Ficha de observación aplicada

Interpretación:

De los resultados mostrados en la tabla y gráfico N° 03, sobre la evaluación de disponibilidad a 27 dispositivos de la infraestructura informática de la notaría Cavides Luna - Punchana 2021, se puede afirmar que:

- La evaluación, antes de aplicar el hacking ético, 100%, en los 27 dispositivos, permitían que la información almacenada no esté disponible en el momento requerido.
- La evaluación, después de aplicar el hacking ético, 48.1%, o sea en 13 dispositivos, permitían que la información almacenada no esté disponible en el momento requerido; y, 51.9%, en 14 dispositivos, permitían que la información almacenada esté disponible en el momento requerido.

El P – valor del Chi Cuadrado de homogeneidad de 0.00, indica que se acepta la hipótesis del investigador.

CAPÍTULO V: DISCUSIÓN

Basándonos en la definición de seguridad de la información como lo menciona (Fundación Wikimedia, Inc., 2021) y (UNIR, 2021) que es el conjunto de acciones que nos permiten proteger la confidencialidad, integridad y disponibilidad de la información, y conforme lo menciona la Ley N° 29733 de protección de datos personales, obligando a los actores que intervengan en el tratamiento de los datos personales, deban adoptar medidas que salvaguarden dichos datos, evitando la alteración, pérdida, tratamiento indebido o acceso no autorizado, guardando confidencialidad de los mismos; la administración de la notaría Cavides Luna Punchana 2021, decide realizar una auditoría de seguridad de la información aplicando hacking ético que según nos dice (Gonzáles Pérez, 2020), que el hacking ético es una disciplina dentro del campo de la seguridad informática, que nos permite descubrir, analizar y explotar vulnerabilidades existentes en un sistema informático, brindándonos una imagen el estado actual de los equipos de cómputo, y así poder tomar acciones correctivas, mitigando en lo máximo posible las debilidades presentes en su infraestructura informática. Para la aplicación del hacking ético en la notaría Cavides Luna Punchana 2021, que, al no contar con un área o encargado de su infraestructura informática, desconocía de cómo está estructurada la misma, con lo cual se obtuvo muy poca información de parte de la administración de la notaría Cavides Luna sobre su infraestructura informática, y como nos dice (Astudillo B., 2013) que cuando el cliente proporciona cierta información, pero de forma limitada, se realiza un hacking de caja gris (gray box hacking) el cual es un hacking ético interno.

En el proceso de la aplicación del hacking ético a la notaría Cavides Luna, (Arriols Nuñez, 2016) nos dice podemos realizar diferentes pruebas, siendo una de ellas la prueba de auditoria de vulnerabilidades de red, la cual se llevó a cabo en los veintisiete (27) dispositivos que conforman la infraestructura informática de la notaría Cavides Luna - Punchana 2021, dando como resultados el estado del antes y después de la aplicación del hacking ético, y la mitigación de las vulnerabilidades encontradas. Para el proceso del hacking ético utilizamos las siguientes herramientas: distribución Kali Linux que sirve para pentest y auditoría de seguridad informática, Nessus para el escaneo y análisis de vulnerabilidades de sistemas informáticos, Burp suite para análisis de vulnerabilidades web, FOCA para la extracción de metadatos, descubrimiento de la red y búsqueda de vulnerabilidades, según lo mencionan (Alonso, y otros, 2016) y (Gonzáles Pérez, y otros, 2015).

Dichos resultados se mencionan a continuación:

En la tabla 01, tabla 02 y tabla 03, referente a confidencialidad, integridad y disponibilidad respectivamente, se puede notar que, previo a la aplicación del hacking ético, el 100% de los veintisiete (27) dispositivos presentan vulnerabilidades de red, en relación a la confidencialidad, integridad y disponibilidad, exponiendo y permitiendo el libre acceso, además de su posible modificación a toda la información almacenada, al personal autorizado y no autorizado, lo cual coincide con (Tovar Romero, 2020) en su investigación de hacking ético a la infraestructura informática del grupo electrodata, evidenciando que cualquier dispositivo que esté conectado a la red informática tiene acceso a toda la infraestructura de red, lo que consiste en un fallo de seguridad, tal como concluye (Gonzales Cotera, 2016) en su investigación del

uso de la herramienta de ethical hacking a la red de la sede central de la universidad de Huánuco, mencionando que la red presenta muchas vulnerabilidades de red que comprometen la confidencialidad, integridad y disponibilidad de la información; y que luego de la aplicación del hacking ético y las medidas correctivas, el 48.1% de los veintisiete (27) dispositivos, es decir, 13 dispositivos, mitigaron sus vulnerabilidades referente a la confidencialidad e integridad, y un 51.9% de los veintisiete (27) dispositivos, es decir, 14 dispositivos, mitigaron sus vulnerabilidades referente a disponibilidad, permitiendo con ello la exposición, acceso y manipulación a la información almacenada solo al personal autorizado, coincidiendo así con (Gonzáles Pérez, 2020) quien recomienda dentro de las buenas prácticas en las auditorías de seguridad informática, la resolución inmediata de los fallos de seguridad encontrados.

Además, con la finalidad de probar la hipótesis de la presente investigación, se analizaron veintisiete (27) dispositivos que conforman la infraestructura informática de la notaría Cavides Luna - Punchana 2021 para conocer y mitigar los fallos de seguridad informática mediante la implementación del hacking ético, referente a la confidencialidad, integridad y disponibilidad de la seguridad de la información, se ha probado que:

- Existe diferencia significativa entre el antes y después de la aplicación del hacking ético, referente a la confidencialidad de la información almacenada y/o generada en la infraestructura informática de la notaría Cavides Luna - Punchana 2021; se incrementó de 0% a un 48%.
- Existe diferencia significativa entre el antes y después de la aplicación del hacking ético, referente a la integridad de la información almacenada y/o

generada en la infraestructura informática de la notaría Cavides Luna Punchana 2021; se incrementó de 0% a un 48%.

- Existe diferencia significativa entre el antes y después de la aplicación del hacking ético, referente a la disponibilidad de la información almacenada y/o generada en la infraestructura informática de la notaría Cavides Luna Punchana 2021; se incrementó de 0% a un 51.9%

Todo esto permite afirmar que la aplicación del hacking ético mejora la seguridad de la infraestructura informática en términos de la confidencialidad, integridad y disponibilidad de la información en la notaría Cavides Luna Punchana 2021.

CAPÍTULO VI: CONCLUSIONES

6.1. Evaluar las vulnerabilidades de red en la infraestructura informática de la notaría Cavides Luna – Punchana 2021 previo a la aplicación del hacking ético, se concluye que:

- Referente a la confidencialidad, se puede afirmar que el 100% de los dispositivos (27) que conforman la infraestructura informática de la notaría Cavides Luna, presentan vulnerabilidades que comprometen la confidencialidad de la información que se genera y/o almacena, permitiendo el acceso a la información al personal autorizado y no autorizado.
- Referente a la integridad, se puede afirmar que el 100% de los dispositivos (27) que conforman la infraestructura informática de la notaría Cavides Luna, presentan vulnerabilidades que comprometen la integridad de la información que se genera y/o almacena, permitiendo que la información pueda ser modificada por el personal autorizado y no autorizado.
- Referente a la disponibilidad, se puede afirmar que el 100% de los dispositivos (27) que conforman la infraestructura informática de la notaría Cavides Luna, presentan vulnerabilidades que comprometen la disponibilidad de la información que se genera y/o almacena, permitiendo que la información.

6.2. Evaluar las vulnerabilidades de red en la infraestructura informática de la notaría Cavides Luna – Punchana 2021 con la aplicación del hacking ético.

- Referente a la confidencialidad, se puede afirmar que se mejoró en un 48.1% el número de dispositivos que se mitigaron los problemas de

vulnerabilidad que comprometen la confidencialidad de la información en la infraestructura informática de la notaría Cavides Luna, o sea en 13 dispositivos, permitiendo el acceso a la información que se genera y/o almacena, solo al personal autorizado.

- Referente a la integridad, se puede afirmar que se mejoró en un 48.1% el número de dispositivos que se mitigaron los problemas de vulnerabilidad que comprometen la integridad de la información en la infraestructura informática de la notaría Cavides Luna, o sea en 13 dispositivos, permitiendo la modificación de la información que se genera y/o almacena, solo al personal autorizado.
- Referente a la disponibilidad, se puede afirmar que se mejoró en un 51.9% el número de dispositivos que se mitigaron los problemas de vulnerabilidad que comprometen la disponibilidad de la información en la infraestructura informática de la notaría Cavides Luna, o sea en 14 dispositivos, permitiendo que la información que se genera y/o almacena, este disponible en el momento que sea requerido, solo al personal autorizado.

6.3. Determinar si existe diferencia significativa, entre el estado anterior y el estado actual con la aplicación del hacking ético en la ciberseguridad de la infraestructura informática de la notaría Cavides Luna – Punchana 2021.

- Referente a la confidencialidad, llegamos a la conclusión de que existe diferencia significativa, entre el estado anterior y el estado actual con la aplicación del hacking ético, en la confidencialidad de la información de la infraestructura informática de la notaría Cavides Luna – Punchana 2021.

- Referente a la integridad, llegamos a la conclusión de que existe diferencia significativa, entre el estado anterior y el estado actual con la aplicación del hacking ético, en la integridad de la información de la infraestructura informática de la notaría Cavides Luna – Punchana 2021.
- Referente a la disponibilidad, llegamos a la conclusión de que existe diferencia significativa, entre el estado anterior y el estado actual con la aplicación del hacking ético, en la disponibilidad de la información de la infraestructura informática de la notaría Cavides Luna – Punchana 2021.

6.4. En efecto, la aplicación del hacking ético, en la ciberseguridad de la infraestructura informática de la notaría Cavides Luna, se puede considerar como positiva, porque permitió mitigar los problemas de vulnerabilidad con referencia a la confidencialidad, integridad y disponibilidad de la información, los cuales son los tres (3) pilares de la seguridad de la información, permitiendo el acceso, modificación y disponibilidad de la información por el personal autorizado, mejorando la ciberseguridad de la infraestructura informática de la notaría Cavides Luna - Punchana 2021. Logrando con ello el objetivo general, respondiendo la interrogante de la investigación y probando la hipótesis del de la presente investigación.

CAPÍTULO VII: RECOMENDACIONES

Se recomienda:

- A la administración de la notaría Cavides Luna, implementar políticas de seguridad de la información para el manejo de los sistemas que posee.
- Capacitación sobre seguridad informática al personal que utiliza la infraestructura informática de la notaría.
- Implementación de una área o personal encargado de la infraestructura informática de la notaría Cavides Luna.
- El reemplazo de los dispositivos que presentan vulnerabilidades críticas, como aquellas que tienen instalado el Sistema Operativo Windows 7, dispositivos con configuraciones que se encuentra por defecto.
- Mitigar las vulnerabilidades que presentan los equipos y sistemas críticos que no pudieron ser solucionados.
- Minimizar la exposición a los servicios que presenta la infraestructura informática.
- Aplicar el mínimo de privilegios posibles a los usuarios de los servicios de la infraestructura informática.
- Aplicar continuamente el hacking ético a la infraestructura informática.

CAPÍTULO VIII: REFERENCIAS BIBLIOGRÁFICAS

Alonso, Chema, y otros. 2016. *Pentesting con FOCA.* primera. mostoles : 0xWord, 2016. págs. 13-15. 978-84-616-6319-4.

Arriols Nuñez, Eduardo. 2016. Nociones Básicas. *Curso Completo de Hacking Ético- Udemy.* [digital]. 2016.

Baeza Meza, Alan Joaquin. 2019. Amenazas y ataques comunes. *Curso de Ethical Hacking - Platzi.* [digital]. 26 de abril de 2019.

Baeza Meza, Alan Joaquin. 2019. Conceptos ¿Qué es y que no es un Pentesting? *Curso de Ethical Hacking - Platzi.* [digital]. 2019.

Baeza Meza, Alan Joaquin. 2019. Conceptos Básicos. *Curso de Ethical Hacking- Platzi.* [digital]. 2019.

Baeza Meza, Alan Joaquin. 2019. Fases del Hacking. *Curso de Ethical Hacking - Platzi.* [digital]. 26 de abril de 2019.

Bermeo Oyola, Jean Carlos. 2017. *Implementación de Hacking Ético para la detección y evaluación de vulnerabilidades de red en la empresa Complex del Perú S.A.C.-Tumbes; 2017.* Facultad de Ingeniría, Universidad Católica los Angeles de Chimbote. Tumbes : s.n., 2017. pág. 103, Tesis de Maestria.

Criollo Ortiz, Paul. 2020. *Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la empresa Infonet soluciones E.I.R.L. - Sullana; 2020.* Facultad de Ingeniería, Universidad Católica Los Angeles Chimbote. Sullana : s.n., 2020. pág. 86, Tesis para Título Profesional.

Fundacion Wikimedia, Inc. 2021. Wikipedia la enciclopedia libre. [En línea] 18 de julio de 2021. [Citado el: 01 de agosto de 2021.] https://es.wikipedia.org/wiki/Google.

Fundacion Wikimedia, Inc. 2021. 2021. Wikipedia la enciclopedia libre. [En línea] 30 de junio de 2021. [Citado el: 01 de agosto de 2021.] https://es.wikipedia.org/wiki/Microsoft_Bing.

Fundación Wikimedia, Inc. 2021. Wikipedia la enciclopedia libre. [En línea] 29 de marzo de 2021. [Citado el: 26 de junio de 2021.] www.es.wikipedia.org/wiki/protocolo_de_internet.

Fundacion Wikimedia, Inc. 2021. 2021. Wikipedia la enciclopedia libre. [En línea] 21 de Mayo de 2021. [Citado el: 26 de Junio de 2021.] https://es.wikipedia.org/wiki/Seguridad_informática.

Fundacion Wikimedia, Inc. 2021. 2021. Wikipedia la enciclopedia libre. [En línea] 22 de Junio de 2021. [Citado el: 26 de Junio de 2021.] https://es.wikipedia.org/wiki/Seguridad_de_la_informacion.

Fundacion Wikimedia, Inc. 2021. 2021. Wikipedia la enciclopedia libre. [En línea] 22 de Junio de 2021. [Citado el: 26 de Junio de 2021.] https://es.wikipedia.org/wiki/Seguridad_de_la_informacion.

García Rambla, Juan Luís y Alonso, Chema. 2014. *Ataques en redes de datos IPv4 e IPv6.* Segunda. Madrid : 0xWord, 2014. págs. 24-37. 978-84-616-8383-3.

García Rambla, Juan Luís y Alonso, Chema. 2014. *Ataques en redes de datos IPv4 e IPv6.* segunda. mostoles : 0xWord, 2014. págs. 39-70. 978-84-616-8383-3.

Gobierno del Perú. 2013. Ley de Delitos Informáticos. *Ley N° 30096.* [digital]. Lima, Perú : Editorial Peru, 21 de octubre de 2013.

Gobierno del Perú. 2011. Ley de Protección de Datos Personales. *Ley N° 29733.* [digital]. Lima, Perú : Editora Perú, 21 de junio de 2011.

Gobierno del Perú. 2018. Ley N° 30096. *Ley de Delitos Informáticos.* [digital]. Lima, Lima, Peru : s.n., 20 de diciembre de 2018.

Gobierno Regional de Loreto. 2021. Gobierno Regional de Loreto. [En línea] 23 de marzo de 2021. [Citado el: 14 de abril de 2021.] Intentaron robar 5 millones 200 mil soles de los fondos del Gobierno Regional de Loreto. https://www.regionloreto.gob.pe/noticias/2021/03/23/gorel-sufrio-intento-de-ataque-cibernético.

Gonzales Cotera, Bernier. 2016. *Uso de Herramientas de Ethical Hacking con Kali Linux para el diagnóstico de vulnerabilidades de la seguridad de la información en la red de la sede central de la universidad de Huánuco.* Facultad de Ingeniería, Uiversidad de Huánuco. Huánuco : s.n., 2016. pág. 97, Trabajo de suficiencia profesional.

Gonzáles Pérez, Pablo, Sánchez Garcés, Germán y Soriano de la Cámara, Jose Miguel. 2015. *Pentesting con Kali 2.0.* Madrid : 0xWord, 2015. págs. 45-78. 978-84-608-3207-2.

Gonzáles Pérez, Pabo. 2020. *Ethical Hacking teoria y práctica para la realización de un pentesting.* 2da edicion, revisada y ampliación. Madrid : 0xWORD, 2020. pág. 232. 978-84-092-0460-1.

IETF. Diccionario de Usuarios de Internet. [En línea] [Citado el: 26 de junio de 2021.] www.datatracker.ietforg/doc/html/rfc1392.

La Republica. 2020. La República. [En línea] 29 de Junio de 2020. [Citado el: 14 de Abril de 2021.] El portal de noticias fue hakeada. https://larepublica.pe/sociedad/2020/06/29/diario-expreso-denuncia-hackeo-de-su-pagina-web-mdga.

Neyra, Carlos. 2020. El Comercio. [En línea] 05 de Abril de 2020. [Citado el: 13 de Abril de 2021.] Roban dinero de la Plataforma Bono Familiar Universal. https://elcomercio.pe/lima/sucesos/coronavirus-en-peru-hackers-vulneraron-plataforma-del-bono-familiar-para-apropiarse-de-dinero-noticia/.

NMAP. NMAP.org. [En línea] [Citado el: 01 de agosto de 2021.] https://nmap.org/.

Tovar Romero, Luis Miguel. 2020. *Hacking Ético para mejorar la seguridad en la infraestructura informática del grupo electrodata.* Facultad de Ingeniería, Uiversidad Tecnológica del Perú. Lima : s.n., 2020. pág. 103, Tesis Títuo Profesional.

UNIR. 2021. UNIR la Uiversidad de Internet. *UNIR la Uiversidad de Internet.* [En línea] 2021. [Citado el: 26 de Junio de 2021.] https://www.unir.net/ingenieria/revista/iso-27001/.

Valdiviezo Avalo, Jormy Jean Franco. 2020. *Desarrollo de una Red Honeypot para la Detección de Intrusiones en la Municipalidad Distrital de Víctor Larco Herrera - Trujillo.* Facultad de Ingeniería y Arquitectura, Universidad Cesar Vallejo. Trujillo : s.n., 2020. pág. 67, Tesis Título Profesional.

ANEXOS

01. Matriz de consistencia.

02. Instrumento de recolección de datos (Ficha de observación).

03. Carta de aceptación notaría Cavides Luna.

04. Carta de conformidad de ejecución de plan de tesis.

05. Declaración jurada de no haber realizado plagio – Tesistas.

06. Declaración jurada de no haber realizado plagio – Asesor.

07. Base de Datos.

08. Aplicación de Hacking Ético

ANEXO N° 01. Matriz de consistencia

TITULO: "EFECTO DEL HACKING ÉTICO EN LA INFRAESTRUCTURA INFORMÁTICA DE LA NOTARÍA CAVIDES LUNA PUNCHANA 2021"

Problema	Objetivo	Hipótesis	Variables	Dimensión	Tipo por su Naturaleza	Indicador	Escala de Medición	Categorías	Valores de las categorías	Medios de verificación	Diseño metodológico y muestral	Técnicas e instrumentos. Procesamiento de datos
¿Cuál es el impacto del Hacking Ético a la infraestructura informática en relación a la ciberseguridad en la notaría Cavides Luna - Punchana 2021?	**Objetivo general** Determinar el efecto del Hacking Ético en la infraestructura informática de la notaría Cavides Luna – Punchana 2021. **Objetivos específicos** Identificar las vulnerabilidades de red en la infraestructura informática de la notaría Cavides Luna – Punchana 2021. Aplicar las medidas correctivas a las vulnerabilidades de red en la infraestructura informática de la notaría Cavides Luna – Punchana 2021. Evaluar el efecto del Hacking Ético en la infraestructura informática de la notaría Cavides Luna – Punchana 2021.	La aplicación del hacking ético mejorará la seguridad de la infraestructura informática en términos de la confidencialidad, integridad y disponibilidad de la información en la notaría Cavides Luna - Punchana 2021.	Independiente: Hacking Ético		Cualitativa	Aplicar Hacking Ético	Ordinal	No aplica Hacking Ético (Antes) Aplica Hacking Ético (después)	0 1	Infraestructura informática de la notaría cavides luna 2021	Aplicada, no experimental, analítico, longitudinal y prospectivo. Con diseño longitudinal de tendencia, una población que está constituido por 23 dispositivos informáticos tomados desde agosto a octubre del 2021, no se considerará muestra porque es posible analizar todos los elementos de la población, por lo que el muestreo no será probabilístico. se realizará la observación antes de la aplicación de hacking ético de fines de agosto hasta la segunda semana de setiembre; y la observación después de la aplicación del hacking ético de la segunda semana de octubre hasta el 31 de octubre del 2021.	Técnica: Observación directa. Instrumento: Ficha de observación. Para el procesamiento de datos se hará uso de programa informático IBM SPSS versión 22.0 en español para windows. respecto a las dimensiones de confidencialidad, integridad y disponibilidad, se hará uso de tablas estadísticas para variable cualitativa, frecuencia, porcentaje y moda; y para establecer la diferencia entre antes y después de la aplicación del Hacking Ético, respecto a dichas dimensiones, se hará uso de Chi Cuadrado de homogeneidad con un nivel de significancia del 5%.
			Dependiente: Infraestructura Informática de la notaría Cavides Luna Punchana 2021	**Confidencialidad**: Se refiere a la información que utilice, almacene o genere cada personal y que pueda ser accedida por el personal correspondiente.	Cualitativa	El respectivo personal accede a toda la información almacenada.	Nominal	El personal autorizado y no autorizado tiene acceso a toda la información almacenada.	0	Infraestructura informática de la notaría cavides luna 2021		
				Integridad: Se refiere a la información se conserve tal cual fue recopilada, generada y almacenada por el personal, sin que haya sido modificado por algún factor externo.	Cualitativa	La información almacenada no presenta modificaciones.	Nominal	Solo el personal autorizado tiene acceso a la información almacenada correspondiente.	1			
								La información almacenada puede ser modificada por el personal autorizado y no autorizado.	0			
				Disponibilidad: Se refiere a que la información esté disponible cuando se desee para el personal que cuente con autorización para tratar dicha información y no para el personal sin autorización.	Cualitativa	La información está disponible en el momento que sea requerido por el personal autorizado.	Nominal	La información almacenada puede ser modificada solo por el personal autorizado.	1			
								No está disponible la información en el momento requerido.	0			
								Está disponible la información en el momento requerido	1			

ANEXO N° 02. Instrumentos de recolección de datos
Ficha de observación.

FICHA DE OBSERVACIÓN						
Dispositivo Evaluado						
Descripción del Dispositivo						
Observación	**Antes**			**Después**		
Fecha de Observación	**Año:**	**Mes:**	**Día:**	**Año:**	**Mes:**	**Día:**
Vulnerable	**Si**	**No**		**Si**	**No**	
Confidencialidad ¿El personal autorizado y no autorizado tiene acceso a toda la información almacenada?						
Integridad ¿ La información almacenada puede ser modificada por el personal autorizado y no autorizado?						
Disponibilidad ¿La información no está disponible en el momento requerido?						

ANEXO N° 03. Carta de aceptación notaría Cavides Luna.

JORGE CAVIDES LUNA
Abogado - Notario de Maynas

"Año del Bicentenario del Perú: 200 años de independencia"

Iquitos, 23 de Julio del 2021

Señor Ingeniero
CARLOS ALBERTO GARCIA CORTEGANO
Decano de la Facultad de Ingeniería de Sistemas e Informática
UNAP
Moore N° 280
Ciudad. –

ASUNTO: **AUTORIZACIÓN PARA LA EJECUCIÓN DEL PLAN DE TESIS**

El que suscribe, Abogado Notario Jorge Isidoro Cavides Luna

AUTORIZA:

Al sr. Franco Aniello Dávila Lage, Bachiller en Ingeniería de Sistemas e Informática y al sr. Jorge Miguel Jossemair Brayn Icomedes García, Bachiller en Ingeniería de Sistemas e Informática, ejecutar el plan de tesis titulado **EFECTO DEL HACKING ÉTICO EN LA INFRAESTRUCTURA INFORMÁTICA DE LA NOTARIA CAVIDES LUNA- PUNCHANA 2021.**

Atentamente.

JORGE I. CAVIDES LUNA
Abogado - Notario de Maynas

Calle Edilberto Valles Nº 702 - Punchana - Maynas - Loreto - Telf. (065) 255037
E-mail: notariacavides@gmail.com www.notariacavides.com

ANEXO N° 04. Carta de conformidad de ejecución del plan de tesis.

JORGE CAVIDES LUNA
Abogado - Notario de Maynas

"Año del Bicentenario del Perú: 200 años de independencia"

Iquitos, 03 de diciembre del 2021

Señor
Dr. Ángel Enrique López Rojas
Decano de la Facultad de Ingeniería de Sistemas e Informática
UNAP
Moore N° 280
Iquitos. –

ASUNTO: **CONFORMIDAD EN LA EJECUCIÓN DEL PLAN DE TESIS**

Es grato dirigirme a usted, para saludarlo cordialmente y hacer de su conocimiento que el sr. Franco Aniello Dávila Lage y el sr. Jorge Miguel Jossemair Brayn Icomedes García, ambos Bachilleres en Ingeniería de Sistemas e Informática, ejecutaron de manera **CONFORME** el plan de tesis titulado **EFECTO DEL HACKING ÉTICO EN LA INFRAESTRUCTURA INFORMÁTICA DE LA NOTARIA CAVIDES LUNA- PUNCHANA 2021**, con lo cual se obtuvo una mejora en la seguridad de nuestra infraestructura informática, y conocer sobre ciberseguridad para una posterior gestión de la seguridad informática.

Sin otro en particular, hago propicia la oportunidad para expresarle las muestras de mi especial consideración y estima.

Atentamente.

JORGE CAVIDES LUNA
Abogado - Notario de Maynas

Calle Ediberto Valles N° 702 - Punchana - Maynas - Loreto - Telf. (065) 255037
E-mail: notariacavides@gmail.com www.notariacavides.com

ANEXO N° 05. Declaración Jurada de no haber realizado plagio – Tesistas.

DELARACIÓN JURADA DE NO HABER REALIZADO PLAGIO - TESISTAS

Yo Franco Aniello Dávila Lage, peruano identificado con D.N.I. N° 46326199, domiciliado en el Jr. Atahualpa N° 1062 – Iquitos; y Jorge Miguel Jossemair Brayn Icomedes García, peruano identificado con D.N.I. N° 46189132, domiciliado en calle Manco Capac N°150 - Punchana.

DECLARAMOS BAJO JURAMENTO LO SIGUIENTE:

DE NO HABER REALIZADO PLAGIO PARA EL DESARROLLO DEL PROYECTO DE TESIS TITULADO “EFECTO DEL HACKING ETICO EN LA INFRAESTRUCTURA INFORMATICA DE LA NOTARÍA CAVIDES LUNA – PUNCHANA 2021”.

Iquitos, 06 de setiembre del 2021

Franco Aniello Dávila Lage
DNI: 46326199

Jorge Miguel Jossemair Brayn Icomedes Garcia
DNI: 46189132

ANEXO N° 06. Declaración Jurada de no haber realizado plagio – Asesor.

DELARACION JURADA DE NO HABER REALIZADO PLAGIO - ASESOR

Yo Manuel Tuesta Moreno, peruano identificado con D.N.I. N° 05336037 y domiciliado en la calle Manaos N° 28 – Iquitos, asesor del presente proyecto de tesis.

DELCARO BAJO JURAMENTO LO SIGUIENTE:

DE NO HABER REALIZADO PLAGIO PARA EL DESARROLLO DEL PROYECTO DE TESIS TITULADO “EFECTO DEL HACKING ETICO EN LA INFRAESTRUCTURA INFORMATICA DE LA NOTARÍA CAVIDES LUNA – PUNCHANA 2021”.

Iquitos, 06 de setiembre del 2021

Manuel Tuesta Moreno
DNI: 05336037

ANEXO 07. Base de datos.

N° DE EQUIPOS	**EQUIPOS**	**CONFIDENCIALIDAD** ¿El usuario autorizado o no autorizado tiene acceso a la información almacenada?		**INTEGRIDAD** ¿El usuario autorizado o no autorizado puede modificar la información almacenada?		**DISPONIBILIDAD** ¿La información almacenada no está disponible en el momento oportuno para el usuario autorizado?	
		Antes	Después	Antes	Después	Antes	Después
1	EQUIPO 1	0	1	0	1	0	1
2	EQUIPO 2	0	1	0	1	0	1
3	EQUIPO 3	0	0	0	0	0	0
4	EQUIPO 4	0	1	0	1	0	1
5	EQUIPO 5	0	1	0	1	0	1
6	EQUIPO 6	0	1	0	1	0	1
7	EQUIPO 7	0	0	0	0	0	0
8	EQUIPO 8	0	1	0	1	0	1
9	EQUIPO 9	0	0	0	0	0	0
10	EQUIPO 10	0	1	0	1	0	1
11	EQUIPO 11	0	1	0	1	0	1
12	EQUIPO 12	0	0	0	0	0	0
13	EQUIPO 13	0	1	0	1	0	1
14	EQUIPO 14	0	1	0	1	0	1
15	EQUIPO 15	0	0	0	0	0	0
16	EQUIPO 16	0	1	0	1	0	1
17	EQUIPO 17	0	1	0	1	0	1
18	EQUIPO 18	0	1	0	1	0	1
19	EQUIPO 19	0	0	0	0	0	1
20	EQUIPO 20	0	0	0	0	0	0
21	EQUIPO 21	0	0	0	0	0	0
22	EQUIPO 22	0	0	0	0	0	0
23	EQUIPO 23	0	0	0	0	0	0
24	EQUIPO 24	0	0	0	0	0	0
25	EQUIPO 25	0	0	0	0	0	0
26	EQUIPO 26	0	0	0	0	0	0
27	EQUIPO 27	0	0	0	0	0	0

LEYENDA	
SI	0
NO	1

ANEXO 08

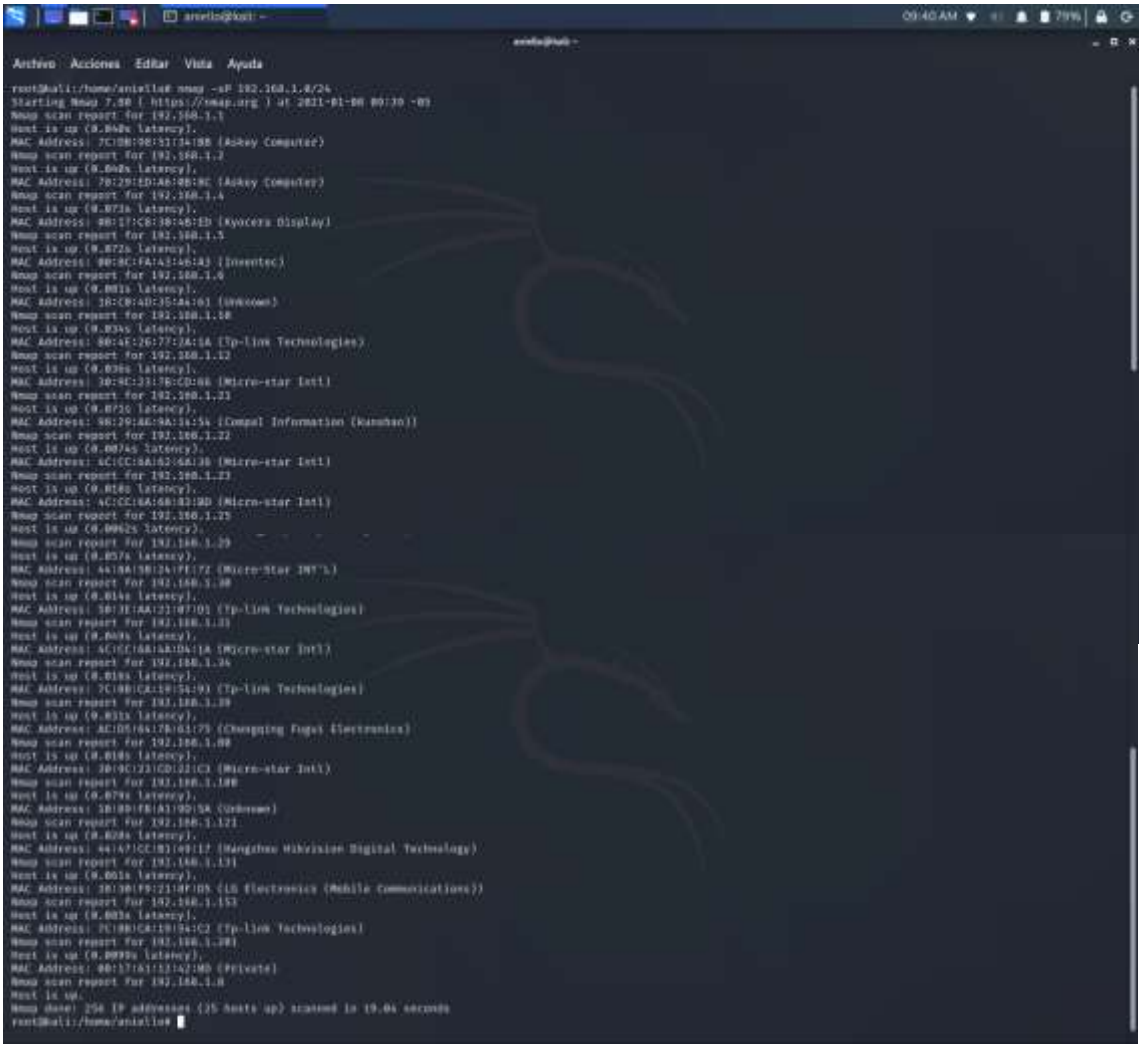
APLICACIÓN DE HAKING ETICO

FRANCO ANIELLO DAVILA LAGE

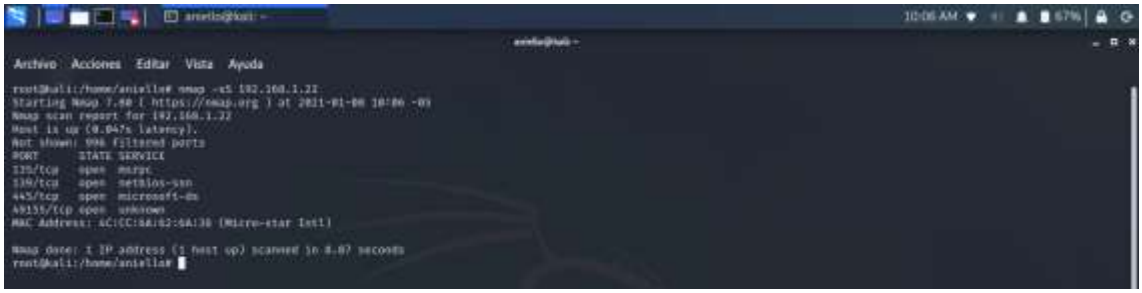
JORGE MIGUEL JOSSEMAIR BRAYN ICOMEDES GARCÍA

Escaneo y enumeración.

Descubrimiento de equipos: en ella se encontraron visible 25 equipos, y 02 equipos se encontraron desconectados a la red. Contabilizándose con ello 27 equipos informáticos.



Escaneo de puertos para conocer los puertos abiertos y los servicios que están ejecutándose en cada equipo de la red.

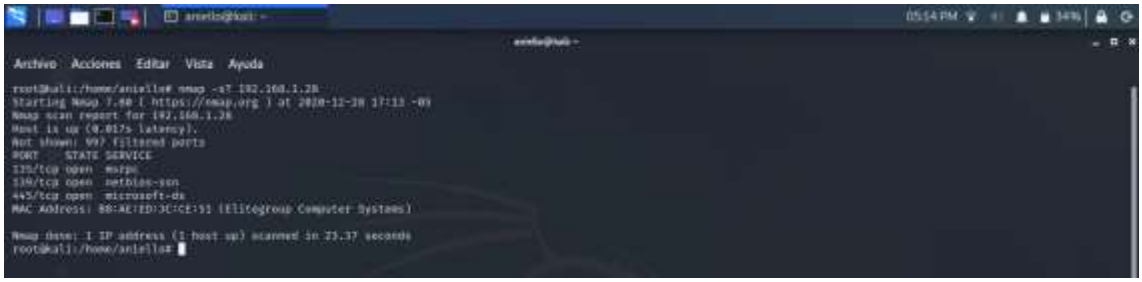



Archivo Acciones Editar Vista Ayuda
root@kali:/home/aniella# nmap -sS 192.168.1.1
Starting Nmap 7.80 (https://nmap.org) at 2021-01-08 09:50 -05
Nmap scan report for 192.168.1.1
Host is up (0.047s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
5431/tcp open park-agent
MAC Address: 7C:5B:98:31:34:88 (Askey Computer)
Nmap done: 1 IP address (1 host up) scanned in 14.26 seconds
root@kali:/home/aniella#


Archivo Acciones Editar Vista Ayuda
root@kali:/home/aniella# nmap -sT 192.168.1.21
Starting Nmap 7.80 (https://nmap.org) at 2020-12-28 17:01 -05
Nmap scan report for 192.168.1.21
Host is up (0.0085s latency).
Not shown: 988 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown
49158/tcp open unknown
MAC Address: 7C:8B:CA:0B:21:E8 (Tp-link Technologies)
Nmap done: 1 IP address (1 host up) scanned in 42.00 seconds
root@kali:/home/aniella#


Archivo Acciones Editar Vista Ayuda
root@kali:/home/aniella# nmap -sT 192.168.1.26
Starting Nmap 7.80 (https://nmap.org) at 2020-12-28 17:10 -05
Nmap scan report for 192.168.1.26
Host is up (0.0035s latency).
Not shown: 987 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
554/tcp open rtsp
1688/tcp open nsjtp-data
1801/tcp open msmq
2968/tcp open enpp
10243/tcp open unknown
49152/tcp open unknown
49153/tcp open unknown
49155/tcp open unknown
49158/tcp open unknown
49161/tcp open unknown
MAC Address: 44:8A:5B:2A:FE:88 (Micro-Star INT'L)
Nmap done: 1 IP address (1 host up) scanned in 14.36 seconds
root@kali:/home/aniella#


Archivo Acciones Editar Vista Ayuda
root@kali:/home/aniella# nmap -sT 192.168.1.27
Starting Nmap 7.80 (https://nmap.org) at 2020-12-28 17:11 -05
Nmap scan report for 192.168.1.27
Host is up (0.0069s latency).
Not shown: 988 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
2968/tcp open enpp
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49159/tcp open unknown
49160/tcp open unknown
MAC Address: B0:6E:BF:ED:3C:24:8E (Elitegroup Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 16.36 seconds
root@kali:/home/aniella#


Archivo Acciones Editar Vista Ayuda
root@kali:/home/aniellar# nmap -sT 192.168.1.28
Starting Nmap 7.80 (https://nmap.org) at 2020-12-30 17:13 -03
Nmap scan report for 192.168.1.28
Host is up (0.017s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: B8:AE:ED:3C:CE:51 (Elitegroup Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 23.37 seconds
root@kali:/home/aniellar#

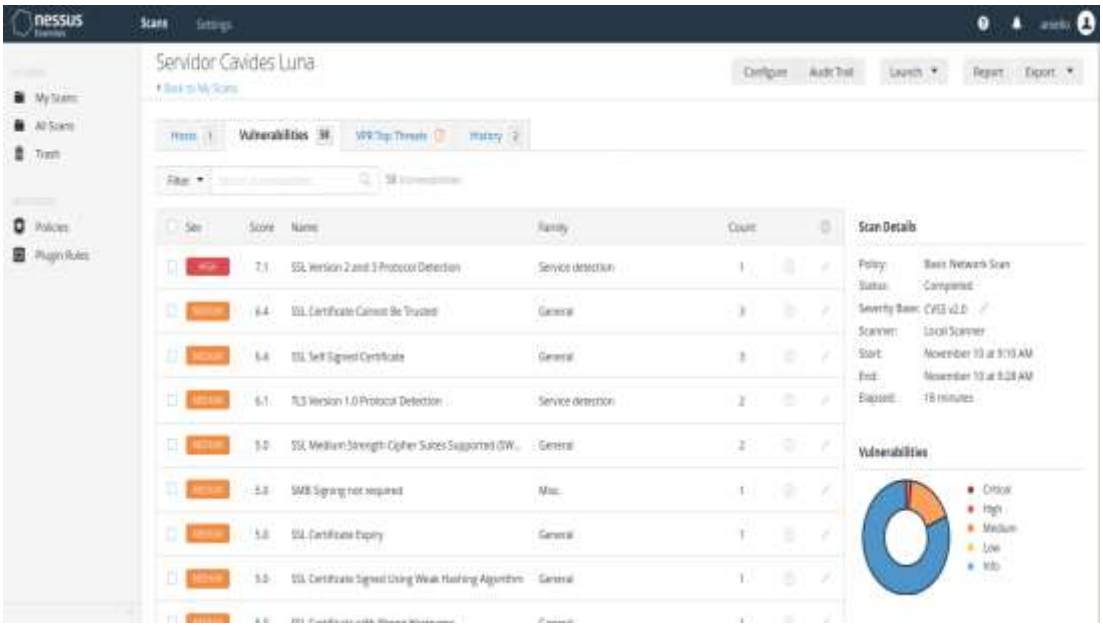

Archivo Acciones Editar Vista Ayuda
root@kali:/home/aniellar# nmap -sT 192.168.1.29
Starting Nmap 7.80 (https://nmap.org) at 2020-12-30 17:15 -03
Nmap scan report for 192.168.1.29
Host is up (0.0020s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE
3968/tcp open mqqp
5357/tcp open wsdapi
MAC Address: 44:8A:5B:24:FE:72 (Micro-Star INT'L)
Nmap done: 1 IP address (1 host up) scanned in 23.17 seconds
root@kali:/home/aniellar#

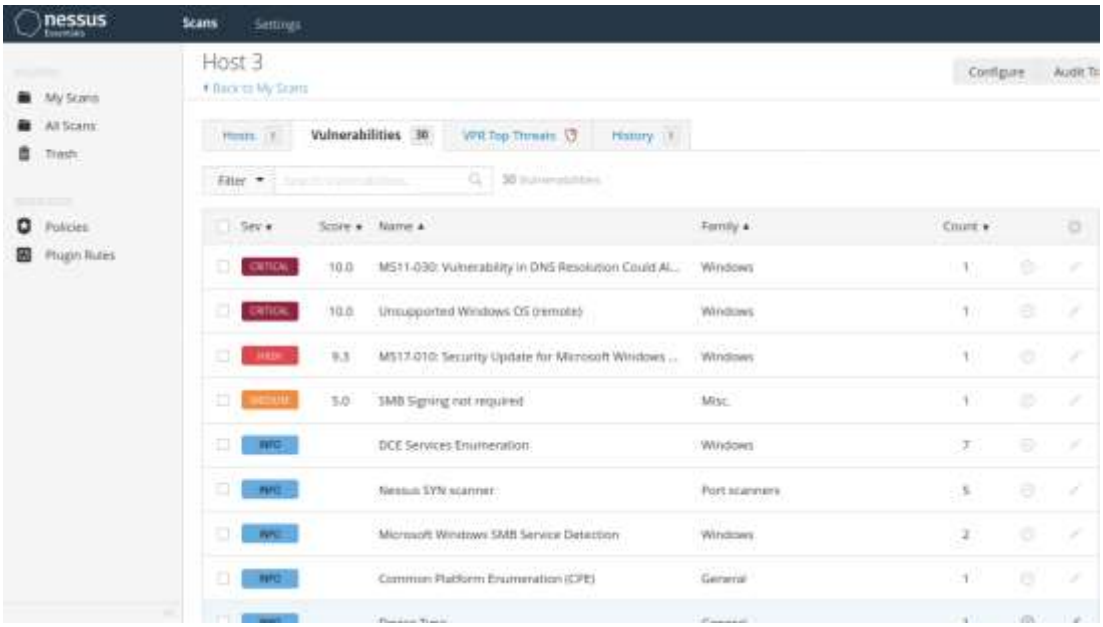

Archivo Acciones Editar Vista Ayuda
root@kali:/home/aniellar# nmap -sT 192.168.1.30
Starting Nmap 7.80 (https://nmap.org) at 2020-12-30 17:16 -03
Nmap scan report for 192.168.1.30
Host is up (0.030s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1688/tcp open nsjtp-data
3968/tcp open mqqp
MAC Address: 50:3E:AA:21:07:01 (Tp-link Technologies)
Nmap done: 1 IP address (1 host up) scanned in 18.65 seconds
root@kali:/home/aniellar#

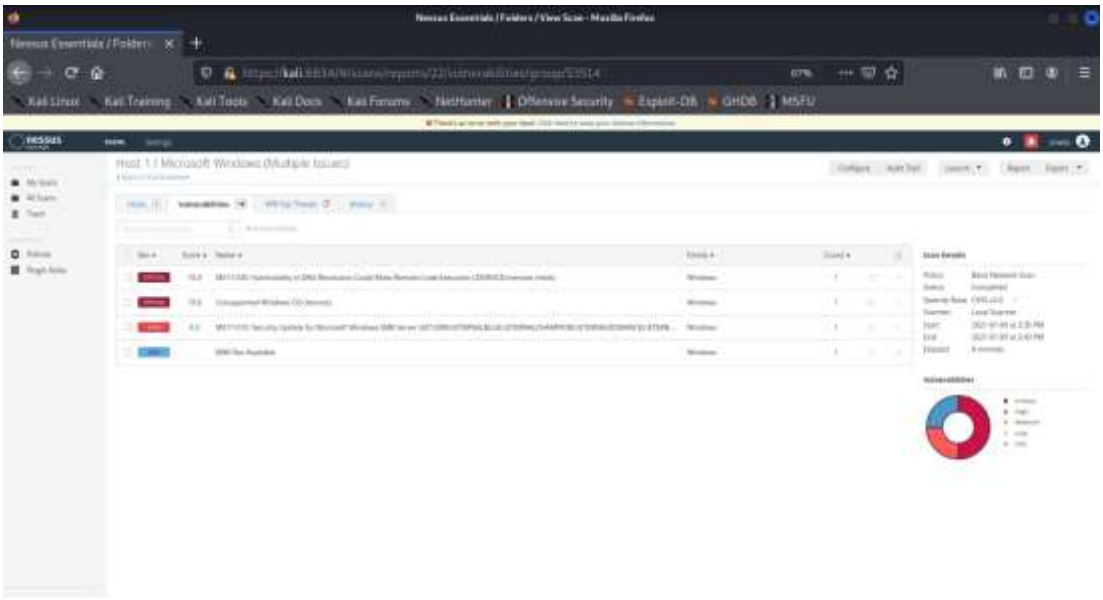

Archivo Acciones Editar Vista Ayuda
root@kali:/home/aniellar# nmap -sT 192.168.1.40
Starting Nmap 7.80 (https://nmap.org) at 2020-12-30 17:19 -03
Nmap scan report for 192.168.1.40
Host is up (0.0033s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3968/tcp open mqqp
3389/tcp open ms-wbt-server
7070/tcp open realserver
MAC Address: 38:9C:23:CD:22:C3 (Micro-star Intl)
Nmap done: 1 IP address (1 host up) scanned in 17.66 seconds
root@kali:/home/aniellar#

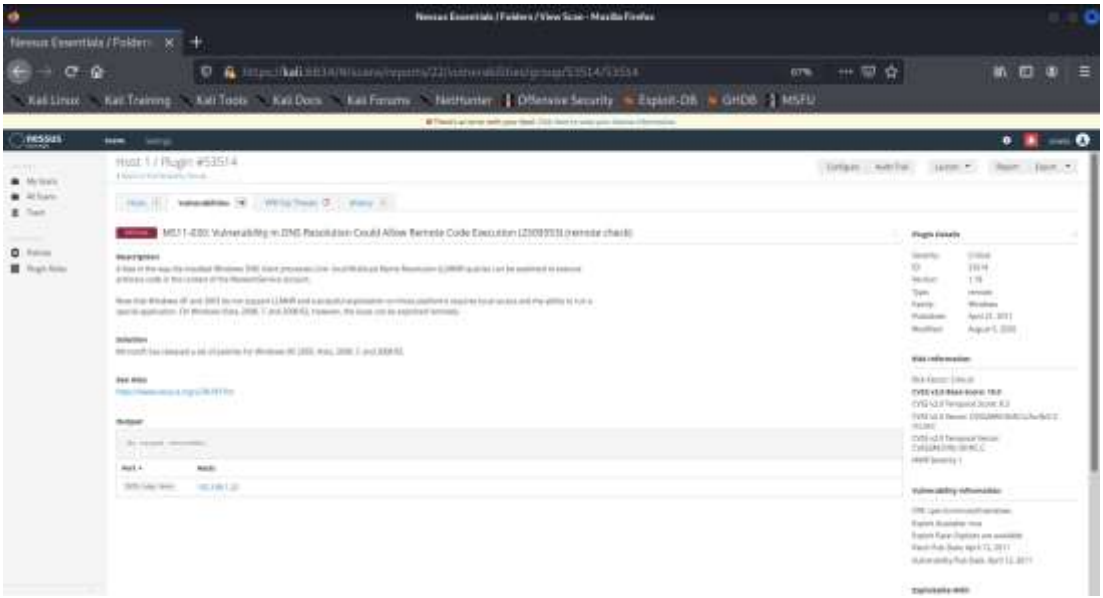

Archivo Acciones Editar Vista Ayuda
root@kali:/home/aniellar# nmap -sT 192.168.1.121
Starting Nmap 7.80 (https://nmap.org) at 2020-12-30 17:21 -03
Nmap scan report for 192.168.1.121
Host is up (0.003s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
80/tcp open http
554/tcp open rtsp
8000/tcp open http-proxy
9010/tcp open sdr
MAC Address: 44:47:CC:81:6B:17 (Hangzhou Hikvision Digital Technology)
Nmap done: 1 IP address (1 host up) scanned in 11.25 seconds
root@kali:/home/aniellar#

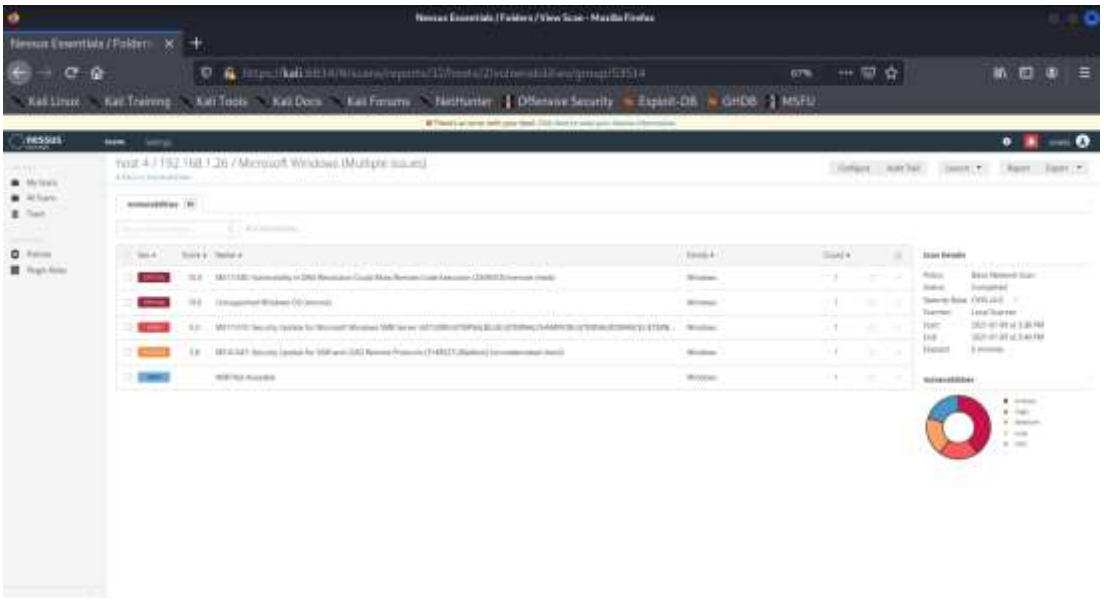
Escaneo de vulnerabilidades por medio de Nessus.

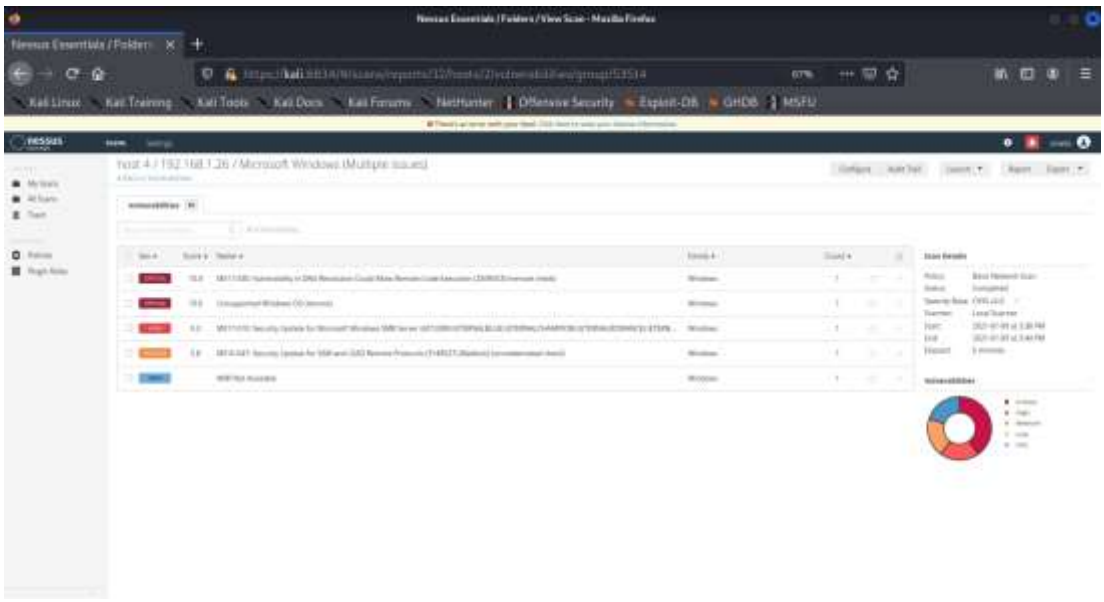












Se aplico la técnica hombre en medio para interceptar el tráfico de red y obtener usuario y contraseña del sistema informático notarial.