



**UNIVERSIDAD TÉCNICA DE BABAHOYO**

**FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.**

**PROCESO DE TITULACIÓN**

**DICIEMBRE 2022 –MAYO 2023**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA**

**PRUEBA PRÁCTICA**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE:**

**INGENIERO EN SISTEMAS DE INFORMACIÓN**

**TEMA:**

**APLICACION DE HACKING ETICO PARA IDENTIFICAR  
AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED WIFI**

**ESTUDIANTE:**

**VIVAR FRANCO ITATY ANDREINA**

**TUTOR:**

**DIAZ CHONG MIGDALIA TERESA**

**AÑO 2023**

## Contenido

PLANTEAMIENTO DEL PROBLEMA.....	7
JUSTIFICACION.....	8
OBJETIVOS.....	9
LÍNEAS DE INVESTIGACIÓN.....	10
MARCO CONCEPTUAL.....	11
Sistema de Información.....	11
Funciones de un Sistema de Información.....	11
Seguridad Informática.....	12
Importancia de la seguridad informática.....	13
Redes inalámbricas.....	13
Tipos de Redes.....	14
Tipos de Hacker.....	15
Hackers.....	15
Carders.....	16
Cracker.....	16
Amenazas.....	16
Riesgos.....	17
Vulnerabilidades.....	18
Tipos de Vulnerabilidades informáticas.....	18
Física.....	19
Tipo Humano.....	19
Comunicaciones y del software.....	19

Hacking Ético .....	20
Modalidades de Hacking Ético .....	20
Prueba de Intrusión Externas .....	20
Prueba de Intrusión Internas. ....	21
Hacking Transparente .....	21
Seguridad Física .....	21
Ingeniería Social .....	22
Herramientas más Comunes para Identificar Vulnerabilidades .....	22
Nessus .....	23
OpenVAS .....	23
Nmap .....	24
MARCO METODOLÓGICO .....	25
RESULTADOS .....	26
Fase 1 Activo .....	26
Fase 2. Amenazas .....	27
Fase 3. Salvaguardas.....	34
Fase final. Impacto y riesgo residual .....	34
DISCUSIÓN DE RESULTADOS.....	35
CONCLUSIONES .....	36
RECOMENDACIONES .....	37
Referencias .....	38
ANEXOS .....	41

FIGURA 1 ANÁLISIS DE VULNERABILIDADES CON LA HERRAMIENTA NESSUS.....	27
FIGURA 2 DETALLES DEL ESCANEO .....	28
FIGURA 3 INICIO DE ESCANEO CON NESSUS .....	29
FIGURA 4 VULNERABILIDADES ENCONTRADAS.....	29
FIGURA 5 AMENAZAS SUPERIORES VPR.....	30
ILUSTRACIÓN 1 PROCESO DE UN SISTEMAS DE INFORMACIÓN.....	12
ILUSTRACIÓN 2 RELACIÓN ENTRE VULNERABILIDAD, AMENAZA Y RIESGO.....	18
<b>TABLA 1</b> TABLA DE ACTIVOS DE UNA RED WIFI.....	26
TABLA 2 RESULTADO DE ESCANEO EN NESSUS.....	30
TABLA 3 VULNERABILIDAD CRITICA.....	31
TABLA 4 VULNERABILIDAD ALTA .....	32
TABLA 5 VULNERABILIDAD MEDIA.....	32
TABLA 6 VULNERABILIDAD BAJA .....	33

## RESUMEN

El hacking ético es una práctica legítima y legal que permite identificar amenazas, riesgos y vulnerabilidades en sistemas informáticos y de redes. Cuando se aplica al análisis de la red WiFi, puede ayudar a descubrir vulnerabilidades y posibles debilidades en la seguridad. Los siguientes son cuatro puntos clave que se deben tener en cuenta al aplicar hacking ético para identificar amenazas y riesgos en la red Wi-Fi.

Primero, se debe obtener el permiso expreso del propietario de la red WiFi antes de realizar cualquier prueba de hacking ético. Segundo, se debe usar herramientas y técnicas de hacking ético para simular un ataque real, con el fin de identificar todas las vulnerabilidades posibles. Tercero, una vez encontradas las vulnerabilidades, se deben documentar y presentar recomendaciones específicas para solucionarlas a fin de mejorar la seguridad de la red WiFi. En cuarto lugar, se debe actualizar y reforzar continuamente la seguridad de la red WiFi, ya que las amenazas y vulnerabilidades siempre están en constante evolución y cambio.

Aplicar hacking ético para identificar amenazas, riesgos y vulnerabilidades en la red WiFi puede ayudar a mejorar la seguridad de la red y garantizar que la información y los datos de los usuarios estén protegidos. Es importante que esta actividad se realice de manera cuidadosa, ética y legal para garantizar la confidencialidad y privacidad de los datos de los usuarios.

**Palabras claves:** red wifi, vulnerabilidad, seguridad, hacking ético

## SUMMARY

Ethical hacking is a legitimate and legal practice that allows to identify threats, risks and vulnerabilities in computer systems and networks. When applied to WiFi network analysis, it can help uncover vulnerabilities and potential security weaknesses. The following are four key points to keep in mind when applying ethical hacking to identify threats and risks on the Wi-Fi network.

First, express permission must be obtained from the WiFi network owner before conducting any ethical hacking tests. Second, ethical hacking tools and techniques should be used to simulate a real attack, in order to identify all possible vulnerabilities. Third, once vulnerabilities are found, specific recommendations for addressing them should be documented and presented in order to improve WiFi network security. Fourth, WiFi network security must be continuously updated and strengthened, as threats and vulnerabilities are always evolving and changing.

Applying ethical hacking to identify threats, risks, and vulnerabilities in the WiFi network can help improve network security and ensure that user information and data are protected. It is important that this activity is carried out in a careful, ethical and legal manner to ensure the confidentiality and privacy of user data.

**Keywords: wifi network, vulnerability, security, ethical hacking**

## **PLANTEAMIENTO DEL PROBLEMA**

La razón por la que se realiza este estudio se debe a las muchas preocupaciones de los usuarios que utilizan redes como el Wi-fi, debido a las vulnerabilidades en la tecnología inalámbrica, que se utilizan como puertas de enlace para posibles ataques con diversos fines. La seguridad de una red inalámbrica depende de muchos factores, incluido el tipo de autenticación y cifrado utilizados.

Muchas de estas fallas son conocidas a nivel mundial, por lo que hoy en día existen una serie de alternativas entre hardware y software que permiten ataques a este tipo de redes de manera más efectiva. Por lo tanto, es importante tomar medidas de seguridad sólidas para evitar ser víctima de ataques que infrinjan la privacidad.

La falta de medidas de seguridad de la red, especialmente para los servicios de red, es un problema creciente el número de atacantes está aumentando. Muchos propietarios de redes WIFI desconocen la importancia del uso de técnicas de hacking ético para identificar vulnerabilidades en sus sistemas y redes. Debido a esto, no toman medidas preventivas para garantizar la seguridad de su red, lo que puede dejar su información vulnerable a ataques malintencionados.

En esta investigación se explorará la problemática asociada al uso de técnicas de hacking ético para identificar amenazas, riesgos y vulnerabilidades en la red WIFI. Además, se propondrán soluciones para abordar estos problemas y mejorar la seguridad de las redes y sistemas. Con la finalidad de proteger la información y garantizar el correcto uso de los recursos de conectividad en nuestra vida diaria.

## JUSTIFICACION

En la actualidad, la conectividad inalámbrica se ha vuelto esencial en nuestra vida cotidiana, tanto en el hogar como en el entorno empresarial, lo que hace que la seguridad de la red WIFI sea crucial para evitar posibles ataques y robos de información. La red wifi es una herramienta esencial para la conectividad de dispositivos en el entorno digital y, por tanto, es crucial garantizar su seguridad y protección.

El hacking ético se refiere a la práctica de utilizar técnicas y herramientas de hacking con fines legítimos y éticos, con el objetivo de identificar vulnerabilidades y debilidades en sistemas y redes informáticas. En el caso específico de la red wifi, esto implica analizar la seguridad de la red inalámbrica y sus dispositivos, buscando debilidades que podrían ser explotadas por atacantes malintencionados.

En el presente caso de estudio se busca, identificar amenazas, riesgos y vulnerabilidades en la red wifi ya que es fundamental para prevenir ataques cibernéticos y proteger la información y los datos personales de los usuarios. Debido a que la información transmitida a través de la red wifi puede ser interceptada por terceros, por lo que es necesario tomar medidas para evitar que esto suceda.

Por lo tanto, se justifica la necesidad de detectar debilidades antes de que sean explotadas por hackers malintencionados y brinda la oportunidad de tomar medidas preventivas para evitar futuros ataques y proteger la información confidencial.



## **OBJETIVOS**

### **OBJETIVOS GENERAL**

- Analizar con la aplicación de hacking ético para identificar amenazas, riesgos y vulnerabilidades en la red wifi.

### **OBJETIVOS ESPECÍFICOS**

- Identificar los factores de amenaza, riesgos y las vulnerabilidades que se presentan en la red Wifi.
- Determinar los posibles puntos de accesos vulnerables dentro la red Wifi a través de hacking ético.
- Recomendar las mejores practicas para la seguridad de la red wifi.

## LÍNEAS DE INVESTIGACIÓN

El presente caso de estudio basa el desarrollo de su investigación bajo la orientación de la línea de investigación denominada “sistemas de información y comunicación, emprendimiento e innovación”; en conjunto con la sub-línea de investigación “redes y tecnologías inteligentes de software y hardware”. Comprendiendo así, el proceso de recolección y gestión de información con la finalidad de que la investigación efectúen datos importantes para el logro de este caso de estudio.

El estudio en cuestión está estrechamente ligado con las áreas de investigación que se centran en los sistemas de información, ya que estos implican la gestión y control de datos mediante el uso de dispositivos informáticos específicos. En particular, estos sistemas deben ser seguros y confiables, garantizando la disponibilidad y la integridad de la información. Para lograr este objetivo, se deben implementar medidas de protección y salvaguardias adicionales, especialmente en lo que respecta a la prevención de vulnerabilidades en la red Wi-Fi.

## MARCO CONCEPTUAL

### **Sistema de Información**

Un sistema de información es un conjunto de elementos y datos que interactúan entre sí con un propósito específico, que generalmente está relacionado con satisfacer una necesidad específica. Un ejemplo común de un SI es el manejo de la base de datos de una biblioteca.

Para que los sistemas de información sean efectivos, deben ser eficientes y fáciles de usar, ya que procesan y almacenan grandes cantidades de datos. Estos datos se cargan en un soporte físico o digital, ya sea de forma automática o manual, y se utilizan para producir información útil para llevar a cabo una actividad o alcanzar un objetivo en particular. Cualquier organización, ya sea en el campo de la medicina, los negocios, la química o las ciencias sociales, requiere un sistema de información para operar de manera efectiva. (Equipo editorial, 2018)

Un sistema de información se compone de elementos y datos que trabajan juntos con el fin de cumplir un propósito específico. Su principal tarea es el procesamiento y almacenamiento de información, que posteriormente es utilizada para generar datos útiles que contribuyen en la ejecución de actividades y la consecución de objetivos en diferentes áreas, como empresas, organizaciones y ciencias.

### **Funciones de un Sistema de Información**

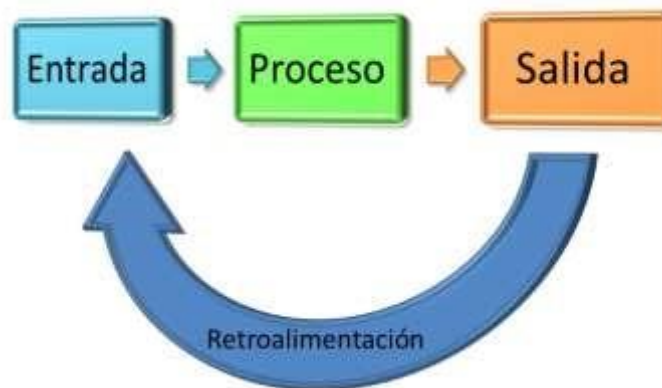
Tres tipos de sistemas de información la cual facilita información que la organización necesita para tomar decisiones, monitorear el desempeño, analizar problemas y crear nuevos productos y servicios. Estos pasos son:

- ✓ Recopilar y almacenar datos: el sistema de información recopila datos de diversas fuentes y los almacena en una base de datos centralizada.
- ✓ Procesamiento es convertir la entrada en una forma que los humanos puedan entender con lo que tenga más sentido.

- ✓ El producto o resultado transmite información procesada a la persona o actividad para la cual se va utilizar.

Los sistemas de información también necesitan la retroalimentación, la cual brinda ayuda a los miembros relevantes de la institución para ayudarlos a calcular o concordar las etapas de alimentación. (Laudon, 2018)

*Ilustración 1 Proceso de un sistemas de información*



### **Seguridad Informática**

Según los autores (Romero Castro, y otros, 2018) la seguridad informática es una disciplina que se enfoca en garantizar la protección del entorno informático. Según varios expertos, la informática se dedica a los procesos, técnicas y métodos que buscan el procesamiento, almacenamiento y transmisión de la información. Por otro lado, la seguridad de la información no se limita al ámbito informático, sino que abarca todo aquello que pueda contener datos sensibles. La seguridad de la información se ocupa de prácticamente todo, lo que implica que hay varias diferencias entre ambas disciplinas. Sin embargo, la distinción más significativa radica en el universo que cada una maneja dentro del entorno informático.

La seguridad informática y la seguridad de la información son disciplinas complementarias, pero con diferencias importantes en cuanto al alcance de su universo de aplicación. Ambas son fundamentales para garantizar la protección de los datos y la privacidad en el mundo digital actual.

Existen diversas herramientas y técnicas que pueden emplearse para salvaguardar tanto la información digital como la analógica. La seguridad informática (InfoSec) abarca distintos ámbitos de la tecnología de la información, tales como la seguridad de la red y la infraestructura, así como también la auditoría y las pruebas de seguridad. Para evitar que usuarios no autorizados accedan a información confidencial, se utilizan herramientas como la autenticación y los permisos. De esta forma, se previenen daños como el robo, la alteración o la pérdida de información.

### **Importancia de la seguridad informática**

Según lo que redacta (Gamboa Suarez, 2020) Resulta de vital importancia conocer los diferentes riesgos que existen en el ámbito de la seguridad informática, tales como ataques cibernéticos, espionajes y actos delictivos que pueden perjudicar a empresas, organizaciones e individuos. Es fundamental estar informado acerca de las herramientas disponibles para detectar, prevenir y contrarrestar estos riesgos, con el fin de proteger adecuadamente los sistemas y la información que manejan. La necesidad de proteger los sistemas y datos críticos de empresas, organizaciones e individuos es el principal motivo que hace de la seguridad informática un aspecto clave en la era digital actual.

### **Redes inalámbricas**

Las redes inalámbricas (WiFi) son una tecnología que permite a los usuarios conectarse a Internet sin necesidad de cables. Esto proporciona movilidad al usuario dentro de un área y ahorros en costos para el administrador de la red, ya que no se requiere un sistema de cableado estructurado para conectar a los usuarios a Internet. Para determinar la cobertura de WiFi en una zona, es necesario realizar una prueba llamada "walk test", en la cual se camina por el área evaluada y se obtiene un mapa de calor que indica la calidad de la señal en diferentes puntos. El objetivo de esta prueba es asegurar que los servicios que los usuarios necesiten, tanto internos como externos, estén disponibles, como el acceso a Internet y a repositorios internos. (Gomez, 2019)

La tecnología inalámbrica permite a los usuarios conectarse a una red local e Internet sin utilizar cables o datos móviles. También se le conoce como redes WLAN (Wireless Local Area Network), y permite la comunicación entre varios dispositivos mediante la transmisión de información a través de ondas, eliminando la necesidad de cables y proporcionando mayor libertad al usuario mientras evita la utilización de puntos de red.

## **Tipos de Redes**

Existen varias formas de clasificar las redes, y una de ellas es según el medio de propagación utilizado. En este sentido, podemos encontrar dos tipos de redes: las alámbricas y las inalámbricas. En las redes alámbricas, la comunicación entre los dispositivos de la red se realiza a través de cables. Por otro lado, en las redes inalámbricas, la comunicación se realiza a través de ondas de señal en lugar de cables.

Existen diferentes tipos de redes según su alcance y su topología, aquí te presento algunas de las más comunes:

- ✓ **PAN** (Personal Area Network) es un tipo de red que se utiliza para conectar dispositivos de comunicación y computación que se encuentran dentro del espacio físico de una persona, como por ejemplo un teléfono móvil, una computadora portátil, una tablet, una smartwatch, entre otros dispositivos.
- ✓ **LAN** (Local Area Network): es una red de área local que se limita a un área geográfica pequeña, como una oficina, un edificio o un campus universitario.
- ✓ **WAN** (Wide Area Network): es una red de área amplia que se extiende sobre una gran área geográfica, como una ciudad, un estado o incluso un país. Se utiliza para conectar redes LAN separadas entre sí.
- ✓ **MAN** (Metropolitan Area Network): es una red de área metropolitana que abarca una ciudad o una región geográfica específica. Se utiliza comúnmente para conectar diferentes sucursales de una empresa en una ciudad.
- ✓ **WLAN** (Wireless Local Area Network): es una red de área local inalámbrica que utiliza tecnología de radiofrecuencia en lugar de cables para conectar dispositivos.

- ✓ **VPN (Virtual Private Network):** es una red privada virtual que utiliza internet para conectar dispositivos remotos como si estuvieran en la misma red local. (Lederkremer, 2019)

### **Tipos de Hacker**

Como indica (Cristancho, 2022) Los hackers son generalmente reconocidos como personas sin identidad definida, quienes suelen llevar a cabo actividades ilegales en el mundo virtual. Sin embargo, es importante destacar que existen distintas categorías de hackers, que son clasificadas según su perfil o propósito. Dado que las ciencias informáticas abarcan una amplia gama de disciplinas, los hackers pueden ser catalogados en diversos tipos, en función de su especialidad y motivación.

Por consiguiente, existen múltiples criterios de clasificación para los'/ hackers, lo que permite establecer una variedad de categorías para estos individuos se clasificación de los más comunes.

### **Hackers**

Teniendo en cuenta a (LLamas, 2022) Un hacker es una persona que se especializa en el uso de lenguajes y técnicas a nivel tecnológico, enfocándose principalmente en los relacionados con Internet y los sistemas en red. Es decir, este tipo de especialistas suelen ser personas con conocimientos muy profundos, que no es necesario adquirirlos científicamente, pero el autoaprendizaje está muy extendido.

Un hacker es un individuo experto en informática que tiene habilidades avanzadas en el manejo de sistemas y redes, y que utiliza sus conocimientos para analizar, modificar o crear software y hardware. Aunque se asocia con frecuencia a los hackers con actividades ilegales, hay diferentes tipos de hackers, y muchos utilizan su conocimiento para mejorar la seguridad de los sistemas.

**Carders**

Los carders son individuos que utilizan habilidades y técnicas fraudulentas para obtener información de tarjetas de crédito, tales como números y códigos de seguridad, con el objetivo de realizar transacciones no autorizadas en línea. Estos delincuentes pueden vender esta información en el mercado negro o usarla para comprar productos o servicios fraudulentamente. Los carders también pueden fabricar tarjetas falsas o clonar tarjetas reales para su uso indebido.

**Cracker.**

Según (Marker, 2019) El término "cracker" se refiere a una persona que utiliza sus habilidades informáticas para llevar a cabo acciones ilegales en línea. Estas acciones pueden incluir la invasión de sistemas, la decodificación de contraseñas y algoritmos de encriptación, y la obtención de acceso no autorizado a software y datos personales. Los crackers a menudo buscan beneficios personales, como poder jugar juegos sin un CD-ROM o generar claves de registro falsas para programas específicos. En resumen, los crackers son considerados como delincuentes virtuales que aprovechan sus conocimientos para llevar a cabo actividades ilegales en línea.

**Amenazas**

Según (Ponce Larreategui, 2021) Las amenazas cibernéticas están en constante evolución y cada vez más sofisticadas, siendo el Malware el método más común empleado para lograr no autorizado al objetivo deseado.

Se considera una amenaza informática a cualquier tipo de actividad que se aprovecha de una debilidad en un sistema informático para atacarlo o invadirlo. En el caso de las



empresas, las amenazas informáticas suelen provenir mayormente de ataques externos, aunque también hay que tener en cuenta las amenazas internas.

Las amenazas informáticas son cualquier acción o evento que tenga el potencial de comprometer la seguridad de los sistemas de información o de la tecnología de la información (TI) de una organización. Las amenazas informáticas pueden tener un gran impacto en la confidencialidad, integridad y disponibilidad de los sistemas de información y de la tecnología de la información (TI), y pueden resultar en la pérdida de datos, la interrupción de los servicios, la exposición de información confidencial y otros riesgos importantes para la seguridad de la información. Es importante que las organizaciones adopten medidas de seguridad adecuadas para mitigar estas amenazas y proteger sus sistemas y datos críticos.

### **Riesgos**

Riesgo a la seguridad de nuestra información son cada vez más sofisticados y cambian constantemente para adaptarse a los intereses de aquellos que buscan obtener beneficios de manera ilegítima. Incluso un correo electrónico aparentemente inofensivo puede desencadenar un ataque de ransomware, donde nuestros datos quedan secuestrados y solo pueden recuperarse a cambio de un rescate. La falta de precaución al compartir información personal o financiera puede resultar en pérdidas económicas significativas y a veces irreparables. (Tamayo, 2019)

Además, la falta de cuidado en el lugar de trabajo puede llevar al robo de información valiosa y confidencial, lo que puede ser especialmente dañino para empresas y organizaciones. A pesar de contar con herramientas de seguridad informática, no siempre es posible evitar estos riesgos, ya que los atacantes están en constante evolución y buscan formas cada vez más ingeniosas de acceder a nuestra información.

## Vulnerabilidades

Con base a (Coronel & Quirumbay, 2022) Cualquier fallo o punto débil presente en un activo que pueda afectar negativamente el desempeño del sistema informático se considera una debilidad o "agujero de seguridad". Estas debilidades pueden ser el resultado de una implementación inadecuada de las aplicaciones, una configuración incorrecta del sistema operativo o un uso descuidado de los sistemas, entre otros factores.

Las vulnerabilidades son puntos débiles o fallos presentes en un sistema o aplicación que pueden ser explotados por atacantes con el fin de comprometer su seguridad. Estos defectos pueden ser causados por errores en el diseño, la programación, la implementación o la configuración del sistema, y pueden ser aprovechados para llevar a cabo ataques como la ejecución remota de código, el robo de información o la denegación de servicio.

*Ilustración 2 Relación entre Vulnerabilidad, Amenaza y Riesgo*



## Tipos de Vulnerabilidades informáticas

Como dice (Restrepo, 2019) Son muchas las vulnerabilidades informáticas a las que están expuestas las empresas en la actualidad. Por eso la inversión en ciberseguridad y sistema de protección ha experimentado un gran aumento en los últimos años, siendo los profesionales en ciberseguridad uno de los perfiles más buscados en el sector de la informática.

Existen diferentes tipos de vulnerabilidades en el ámbito de la seguridad informática. Algunos de los principales tipos de vulnerabilidades son:

**Física**

La vulnerabilidad física se refiere a la posibilidad de acceder físicamente al dispositivo, lo que permitiría tomar el control del mismo y llevar a cabo acciones que eventualmente podrían resultar en una amenaza o ataque.

Son debilidades en la seguridad física de un sistema que permiten a un atacante obtener acceso no autorizado a los recursos del sistema.

**Tipo Humano**

Las vulnerabilidades humanas se relacionan con errores de configuración de los administradores de red, lo que puede ser aprovechado por ciberdelincuentes. Estos errores incluyen dejar configuraciones predeterminadas en las cuentas de usuarios, establecer permisos incorrectamente, mantener servicios inactivos y ejecutar rutinas peligrosas. Los usuarios comunes también pueden cometer errores al ejecutar rutinas o comandos inapropiados en las máquinas.

**Comunicaciones y del software**

Las debilidades que pueden surgir en el software y hardware son susceptibles de generar riesgos para el correcto funcionamiento de los sistemas y procesos globales de transacciones. Estas vulnerabilidades pueden surgir debido a diversas causas, lo que hace necesario implementar medidas preventivas y de seguridad para minimizar su impacto y asegurar la integridad y confidencialidad de la información y los recursos involucrados en estas transacciones.

Son fallos en el código de un programa que pueden ser explotados por un atacante para obtener acceso no autorizado a un sistema o para causar daño.

## **Hacking Ético**

Como dice (Gauthier & Mendez, 2020) Es interesante notar que, en los cursos de seguridad, se presta poca atención a la importancia de los fundamentos matemáticos, éticos y legales. A pesar de que la criptografía es considerada de gran importancia y requiere un conocimiento sólido de matemáticas, y que el hacking ético depende de una base sólida en ética y legalidad.

La práctica del hacking ético implica llevar a cabo pruebas de seguridad en la red de datos y en los sistemas de información para detectar riesgos, amenazas y vulnerabilidades. Su objetivo es evaluar el estado actual de la organización con el fin de aplicar medidas correctivas necesarias para garantizar la seguridad y protección de los activos y datos de la empresa.

## **Modalidades de Hacking Ético**

Existen múltiples maneras de analizar o evaluar la infraestructura tecnológica de una organización de forma ética y legal. Entre las técnicas más frecuentes de hacking ético se encuentran:

- Prueba de intrusión externas.
- Prueba de intrusión internas.
- Hacking transparente.
- Seguridad física.

## **Prueba de Intrusión Externas**

Esta técnica de hacking ético es conocida como "blind testing" o prueba a ciegas, ya que el consultor solo recibe el nombre de la empresa a auditar y no tiene acceso a la infraestructura de la organización. Este enfoque se considera más realista porque es común que los atacantes solo tengan información limitada sobre su víctima, como el nombre de la organización a atacar.

### **Prueba de Intrusión Internas.**

En el caso de pruebas de auditoría de red pública, el cliente proporciona información limitada sobre los elementos a auditar, como direcciones IP y la función del equipo en la red, como router, web-server o firewall. Por otro lado, cuando se realizan pruebas internas, se conoce como auditoría de caja gris, ya que el auditor solo recibe los mismos accesos que un empleado de la empresa, con los mismos privilegios. Esto incluye un punto de red para la estación de auditoría y datos de configuración de red, como dirección IP, máscara de subred, gateway y servidor DNS. Sin embargo, el cliente no revela información adicional, como las credenciales de usuario para unirse a un dominio o la existencia de subredes, entre otros detalles.

### **Hacking Transparente**

La auditoría de caja blanca se refiere a cuando una empresa cliente proporciona al hacker información completa de sus redes y sistemas para auditar. Además de conceder acceso a la red y la información de configuración para el equipo del auditor, como en la auditoría de caja gris, el auditor también recibe información adicional, como diagramas de red, una lista detallada de equipos a auditar con nombres, plataformas, servicios ofrecidos, direcciones IP, información de subredes remotas, entre otros detalles.

Debido a que el consultor no tiene que extraer esta información por su cuenta, la auditoría de caja blanca requiere menos tiempo y tiene un costo más bajo. Es común que se le solicite al consultor probar varios escenarios en la auditoría de caja blanca.

### **Seguridad Física**

La seguridad física es vista como un tema separado de las auditorías de hacking ético por muchos expertos. No obstante, hay empresas especializadas que pueden incluir la seguridad física como parte de sus servicios de auditoría. (Tecnolgia, 2022)

La seguridad física es una parte fundamental del hacking ético, ya que permite evaluar la resistencia de los controles físicos de una organización frente a posibles ataques. En el contexto del hacking ético, el objetivo de la evaluación de la seguridad física es determinar si las medidas de seguridad implementadas son efectivas para proteger los activos y recursos críticos de la organización.

### **Ingeniería Social**

La Ingeniería Social implica el uso de engaños para obtener información confidencial de las personas, lo que puede poner en riesgo su seguridad. En la actualidad, su uso ha aumentado debido al crecimiento significativo de usuarios en redes sociales, correos electrónicos y otras formas de comunicación en línea. (Benavides, 2020)

La ingeniería social es una técnica de manipulación psicológica utilizada para engañar a las personas y obtener información confidencial o acceso a sistemas y redes. Esta técnica se basa en la explotación de la confianza, la curiosidad y la falta de atención, y puede incluir el uso de pretextos, phishing, malware y otras tácticas engañosas para lograr sus objetivos. La ingeniería social es un riesgo importante para la seguridad de la información y la privacidad, y es importante que los individuos y las organizaciones estén conscientes de los riesgos y tomen medidas para protegerse.

### **Herramientas más Comunes para Identificar Vulnerabilidades**

Para llevar a cabo dicha tarea, es necesario contar con un escáner de vulnerabilidades, el cual se encarga de examinar tu red y sistemas para detectar posibles debilidades y proporcionar información acerca de los riesgos asociados con ellas. Aunque existen diversas herramientas de análisis de vulnerabilidades en el mercado, es importante considerar que la elección de la mejor opción dependerá de las necesidades específicas de cada organización.

En este contexto, se pueden mencionar los tres escáneres de vulnerabilidades más destacados.

## **Nessus**

Nessus es una herramienta de gran alcance para escanear vulnerabilidades en la mayoría de los sistemas operativos más comunes. Realiza escaneos de puertos y emplea diversas técnicas de explotación para buscar y penetrar vulnerabilidades detectadas. Nessus cuenta con una amplia gama de plugins que le otorgan gran potencia y escalabilidad para realizar análisis complejos. (Postigo Palacios, 2020)

Nessus es un programa de escaneo de vulnerabilidades de red desarrollado por Tenable Network Security. Es ampliamente utilizado por profesionales de seguridad de la información para identificar y evaluar las vulnerabilidades de los sistemas de red y aplicaciones en busca de posibles brechas de seguridad.

Nessus funciona mediante la realización de escaneos automáticos en los sistemas y aplicaciones, utilizando una base de datos de vulnerabilidades conocidas para identificar posibles problemas de seguridad. Los resultados del escaneo se presentan en un informe detallado, que incluye información sobre las vulnerabilidades encontradas, así como recomendaciones para corregir o mitigar los problemas.

## **OpenVAS**

OpenVAS (Open Vulnerability Assessment System) es una plataforma de evaluación de vulnerabilidades de código abierto que proporciona múltiples opciones para analizar y detectar posibles amenazas en una red. Los resultados obtenidos por OpenVAS permiten a los usuarios tomar medidas para mejorar la seguridad de los sistemas mediante la realización de operaciones específicas. (Altube, 2020)

Es una herramienta de escaneo de vulnerabilidades de red de código abierto. Utiliza una base de datos de pruebas de seguridad conocidas para buscar vulnerabilidades en los sistemas y servicios de red. OpenVAS puede ser utilizado para identificar posibles brechas de seguridad en los sistemas, así como para realizar auditorías de seguridad.

## **Nmap**

Nmap ( Network Mapper ) es una herramienta de auditoría de seguridad y exploración de red gratuita y de código abierto. Está diseñado para descubrir hosts y servicios en una red informática, creando así un mapa de la red. Nmap utiliza una variedad de técnicas para lograr esto, incluido el escaneo de puertos y la detección de versiones. Se puede usar para identificar hosts y servicios, así como para identificar vulnerabilidades de seguridad y posibles exploits.



## MARCO METODOLÓGICO

En muchos casos, se utiliza la técnica de investigación conocida como la metodología MAGERIT para analizar la gestión de riesgos en los sistemas informáticos. Esta metodología fue desarrollada e implementada por el Consejo Superior de Administración Electrónica con el objetivo de minimizar los riesgos asociados al manejo de información en una organización y mejorar la utilización de los recursos tecnológicos. La metodología MAGERIT se divide en cinco fases:

- ✓ **Fase 1 Activos:** Se identifican los activos relevantes para la organización.
- ✓ **Fase 2 Amenazas:** Se determinan las amenazas a las que están expuestos estos activos.
- ✓ **Fase 3 Salvaguardas:** Se evalúan las existentes y su eficacia frente a los riesgos.
- ✓ **Fase 4 Impacto residual:** Se refiere al daño que sufriría el activo en caso de que la amenaza se materialice.
- ✓ **Fase 5 Riesgo residual:** Se evalúa el riesgo residual, que se calcula aprobando el impacto con la tasa de ocurrencia de la amenaza.

Para obtener información precisa y confidencial sobre las características de la red informática, se mantuvo un diálogo con 10 individuos. También se utilizaron fuentes de gramática para recopilar documentos y crear un flujo continuo y establecido de datos relacionados con las vulnerabilidades de la red wifi. Estas fuentes consisten en una variedad de fuentes de información, incluidos libros digitales, tesis, artículos, revistas y sitios web confiables, todos respondiendo a publicaciones de los últimos cinco años. Para analizar las razones y consecuencias del hacking ético en la red wifi, se pretende examinar cómo esta práctica puede impactar en la seguridad y el funcionamiento de la misma.

Además, se ha empleado el método de investigación correlacional para evaluar la relación entre la variable independiente de hacking ético y la variable dependiente de vulnerabilidad en los servicios de red wifi.

## RESULTADOS

Se llevó a cabo la exploración de debilidades con el soporte de la herramienta Nessus, la cual es ampliamente utilizada a nivel global en el campo de hacking ético para detectar y comprobar vulnerabilidades de una red wifi.

### Fase 1 Activo

En esta etapa, se llevarán a cabo pruebas de penetración en la red inalámbrica wifi local. Este proceso se divide en varias sub-fases enfocadas en la red WLAN, que incluyen la recopilación de información, el escaneo y la auditoría, el análisis y la búsqueda, la explotación y el ataque, y finalmente el reporte y la presentación.

*Tabla 1 Tabla de Activos de una red wifi*

<b>Activo Tecnológico</b>	<b>Descripción</b>
<b>Router inalámbrico</b>	El dispositivo que proporciona la conexión a Internet a través de la red WiFi.
<b>Dispositivos móviles</b>	Smartphones, tablets, laptops, etc.
<b>Televisores inteligentes, dispositivos de streaming y videojuegos</b>	Se conectan a la red WiFi para acceder a contenido en línea.
<b>Dispositivos de domótica</b>	Cámaras de seguridad, termostatos inteligentes, asistentes virtuales, entre otros
<b>Tarjetas inalámbricas</b>	Permiten a los dispositivos conectarse a la red WiFi de forma inalámbrica.
<b>Antenas</b>	Mejoran la calidad de la señal y la cobertura de la red WiFi.
<b>Cableado</b>	Los cables que conectan el router inalámbrico a la red de datos.
<b>Software de gestión de la red</b>	Los programas que permiten configurar y administrar la red WiFi.

## Fase 2. Amenazas

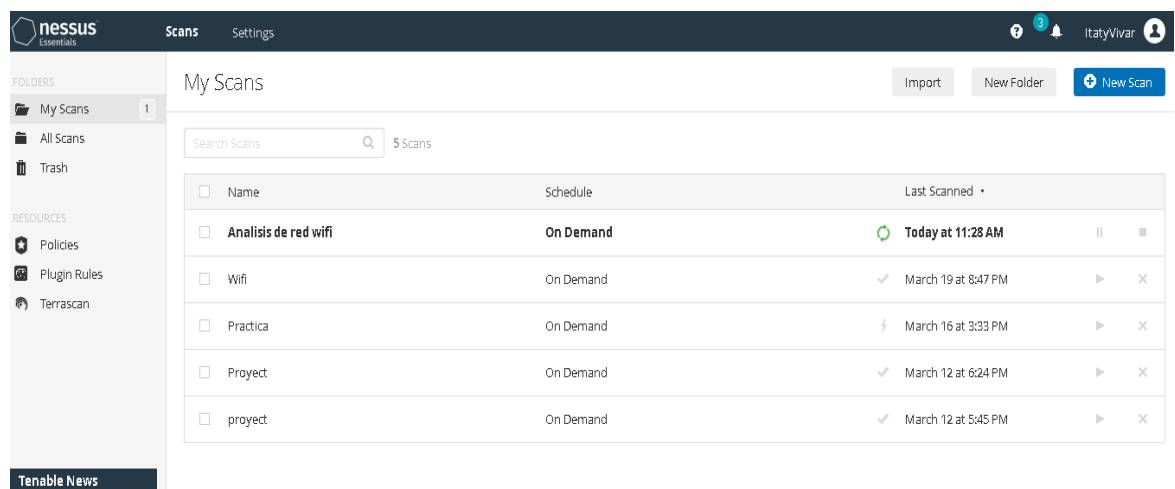
En este período se está llevando a cabo la identificación de las amenazas y vulnerabilidades que podrían poner en riesgo los activos tecnológicos de la red wifi. Para realizar esta tarea, se ha utilizado la herramienta Nessus, la cual cuenta con una interfaz sencilla que permite buscar posibles brechas de seguridad en los sistemas informáticos.

### Determinación de amenazas y vulnerabilidades

En esta fase, se está iniciando el escaneo de la red informática para detectar vulnerabilidades, utilizando la herramienta Nessus, la cual nos permite escanear toda la red y mostrar las posibles vulnerabilidades para prevenir posibles ataques informáticos. Después de haber completado la configuración necesaria, procedimos con la siguiente etapa que consistió en llevar a cabo la labor de escanear la red, tal y como se indica en el procedimiento.

En la Figura 3. Se afirma que el sistema de computación evaluado presenta debilidades que pueden ser aprovechadas por un hacker para obtener información que luego será utilizada como base para ataques más elaborados. Además, si se utilizan comunicaciones sin cifrar o con cifrado débil, existe el riesgo de que se produzca una fuga de datos, ya que la información transmitida a través de formularios puede ser interceptada o capturada.

Figura 1 Análisis de Vulnerabilidades con la herramienta Nessus



The screenshot shows the Nessus Essentials interface. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main area is titled 'My Scans' and contains a table of scan results. The table has columns for Name, Schedule, and Last Scanned. The scans listed are: 'Analisis de red wifi' (On Demand, Today at 11:28 AM), 'Wifi' (On Demand, March 19 at 8:47 PM), 'Practica' (On Demand, March 16 at 3:33 PM), 'Proyect' (On Demand, March 12 at 6:24 PM), and 'proyect' (On Demand, March 12 at 5:45 PM). Each row includes a checkbox, a status icon, and a 'Last Scanned' timestamp.


<input type="checkbox"/>	Name	Schedule	Last Scanned		
<input type="checkbox"/>	Analisis de red wifi	On Demand	Today at 11:28 AM	II	■
<input type="checkbox"/>	Wifi	On Demand	March 19 at 8:47 PM	▶	✕
<input type="checkbox"/>	Practica	On Demand	March 16 at 3:33 PM	▶	✕
<input type="checkbox"/>	Proyect	On Demand	March 12 at 6:24 PM	▶	✕
<input type="checkbox"/>	proyect	On Demand	March 12 at 5:45 PM	▶	✕

En esta fase observamos en la Figura 4. Nos detalla el día que se ejecutó el análisis de vulnerabilidades el cual fue el 21 de marzo a las 11:27 a.m. y finalizó a las 11:40 a.m. El cual fue total de 12 minutos que tardó en escanear.

*Figura 2 Detalles del Escaneo*

#### **Escanear detalles**

---

Política:	Escaneo avanzado
Estado:	Completado
Base de gravedad:	CVSS v3.0 
Escáner:	Escáner local
Comienzo:	Hoy a las 11:27 a.m.
Fin:	Hoy a las 11:40 a.m.
Elapso:	12 minutos

Una vez finalizada la fase de exploración, se pudieron detectar y evidenciar las debilidades y amenazas. Nessus presenta gráficos en forma de barras y de pastel, como se muestra en la Figura 5, para proporcionar una vista general de estas vulnerabilidades y amenazas.

Figura 3 Inicio de Escaneo con Nessus

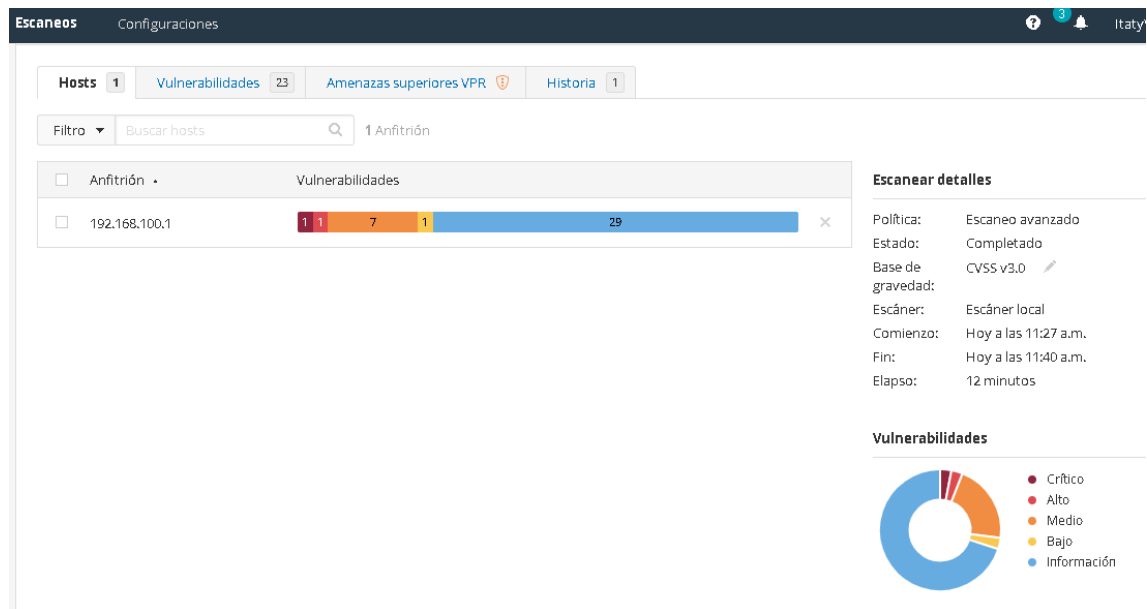


Figura 4 Vulnerabilidades encontradas

Sev	Puntuac...	Nombre	Familia	Contar	
CRÍTICO	9,8	Detección de protocolo S...	Detección de servicio	1	
MIXTO	...	9 SSL ( Problemas múl...	General	9	
MEDIO	6,5	Servidor Telnet sin cifrar	Misceláneo.	1	
MEDIO	4,3 *	OpenSSL SSL_OP_NETSC...	General	1	
MIXTO	...	3 TLS ( Problemas múl...	Detección de servicio	3	
BAJO	3,3 *	Detección del servidor D...	Detección de servicio	1	
INFORMACIÓN	...	2 TLS ( Problemas múl...	General	2	
INFORMACIÓN		Escáner Nessus SYN	Escáneres de puerto	3	
INFORMACIÓN		Detección de servicio	Detección de servicio	3	

La figura 4 muestra de algunas las vulnerabilidades que son critica, mixto, medio, bajo y como última información que se ha encontrado en nuestra red wifi esta herramienta que utilizamos, nos proporciona un listado exhaustivo de las debilidades detectadas durante el análisis. Además, estas debilidades se encuentran organizadas según su nivel de riesgo, como se puede observar en las ilustraciones que acompañan al informe.

Figura 5 Amenazas superiores VPR

Hosts 1 Vulnerabilidades 23 Amenazas superiores VPR Historia 1

Nivel de amenaza evaluado: **Medio**

Las siguientes vulnerabilidades están clasificadas por el sistema patentado de calificación de prioridad de vulnerabilidad de Tenable (VPR). Los hallazgos enumerados a continuación detallan las diez vulnerabilidades principales, proporcionando una vista priorizada para ayudar a guiar remediación para reducir efectivamente el riesgo. Haga clic en cada hallazgo para mostrar más detalles junto con los hosts impactados. Para obtener más información sobre el sistema de puntuación VPR de Tenable, consulte [Priorización predictiva](#).

**Escaneo detalles**

Política: Escaneo avanzado  
 Estado: Completado  
 Base de gravedad: CVSS v3.0  
 Escáner: Escáner local  
 Comienzo: Hoy a las 11:27 a.m.  
 Fin: Hoy a las 11:40 a.m.  
 Elapso: 12 minutos

Gravedad VPR	Nombre	Razones	Puntuación VP...	Hosts
MEDIO	Oráculo de relleno SSLv3 sobre vulnerabilidad de cif...	No hay eventos grabados	5.3	1
MEDIO	SSL Suites cifradas de resistencia media compatible...	No hay eventos grabados	5.1	1
BAJO	SSL RC4 Cipher Suites Compatible ( Bar Mitzvah )	No hay eventos grabados	3.6	1
BAJO	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHAN...	No hay eventos grabados	2,7	1

A continuación, se presenta una tabla que resume el análisis realizado mediante Nessus, lo cual nos permite identificar la cantidad de vulnerabilidades presentes en la red wifi.

Tabla 2 Resultado de escaneo en Nessus

Escaneo usando Nessus	
Vulnerabilidades encontradas:	6
Información adicional:	17
Total	23
Tipo de Análisis:	Análisis Avanzado
Tiempo de inicio:	11:27 a.m.
Tiempo final:	11:40 a.m.
Duración Total	12 minutos
Vulnerabilidades Criticas	1
Vulnerabilidades Altas	2
Vulnerabilidades Medias	2

Vulnerabilidades Bajas	1
------------------------	---

### Detalle de las Vulnerabilidades encontradas

Tabla 3 Vulnerabilidad Critica

Detalle de Vulnerabilidades	
<b>Fecha de Publicación:</b>	12/10/2005
<b>Fecha de Modificación:</b>	04/04/2022
<b>Nombre:</b>	CVSS v3.0 Base Score 9.8 CVSS v3.0 Vector: CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: H / I: H / A: H  Puntaje base CVSS v2.0: 10.0 CVSS v2.0 Vector: CVSS2 # AV: N / AC: L / Au: N / C: C / I: C / A: C
<b>Importancia:</b>	Critica
<b>Recursos Afectados:</b>	Detección de protocolo SSL Versión 2 y 3
<b>Detalle:</b>	<p>El servicio remoto acepta conexiones cifradas usando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos, que incluyen:</p> <ul style="list-style-type: none"> <li>- Un esquema de relleno inseguro con cifrados CBC.</li> <li>- Renegociación insegura de la sesión y esquemas de reanudación.</li> </ul> <p>Un atacante puede explotar estos defectos para realizar ataques de hombre en el medio o para descifrar las comunicaciones entre el servicio afectado y los clientes.</p>
<b>Recomendación:</b>	Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Use TLS 1.2

Tabla 4 Vulnerabilidad Alta

<b>Detalle de Vulnerabilidades</b>	
<b>Fecha de Publicación:</b>	23/11/2009
<b>Fecha de Modificación:</b>	03/02/2021
<b>Nombre:</b>	CVSS v3.0 Vector: CVSS: 3.0 / AV: N / <u>CVE-2016-2183</u>
<b>Importancia:</b>	Alta
<b>Recursos Afectados:</b>	SSL Suites cifradas de resistencia media compatibles (SWEET32)
<b>Detalle:</b>	El host remoto admite el uso de cifrados SSL que ofrecen cifrado de resistencia media. Nessus considera la resistencia media como cualquier cifrado que use longitudes de clave de al menos 64 bits y menos de 112 bits, o que use el conjunto de cifrado 3DES. Tenga en cuenta que es considerablemente más fácil eludir el cifrado de fuerza media si el atacante está en la misma red física.
<b>Recomendación:</b>	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

Tabla 5 Vulnerabilidad Media

<b>Detalle de Vulnerabilidades</b>	
<b>Fecha de Publicación:</b>	27/10/2009
<b>Fecha de Modificación:</b>	12/062020
<b>Nombre:</b>	CVSS v3.0 Base Score 6.5
<b>Importancia:</b>	MEDIA
<b>Recursos Afectados:</b>	Servidor Telnet sin cifrar



<b>Detalle:</b>	<p>El host remoto está ejecutando un servidor Telnet a través de un canal sin cifrar. No se recomienda usar Telnet sobre un canal sin cifrar, ya que los inicios de sesión, las contraseñas y los comandos se transfieren en texto sin cifrar.</p> <p>Esto permite que un atacante remoto y hombre en el medio escuche una sesión de Telnet para obtener credenciales u otra información confidencial y modificar el tráfico intercambiado entre un cliente y un servidor.</p> <p>SSH es preferido sobre Telnet ya que protege las credenciales de las escuchas y puede hacer un túnel de flujos</p>
<b>Recomendación:</b>	Deshabilite el servicio Telnet y use SSH en su lugar.

*Tabla 6 Vulnerabilidad Baja*

<b>Detalle de Vulnerabilidades</b>	
<b>Fecha de Publicación:</b>	05/05/2001
<b>Fecha de Modificación:</b>	06/03/2019
<b>Nombre:</b>	Detección del servidor DHCP
<b>Importancia:</b>	Baja
<b>Recursos Afectados:</b>	CVSS v2.0: 3.3 CVSS v2.0 Vector: CVSS2 # AV: A / AC: L / Au: N / C: P / I: N / A: N

<b>Detalle:</b>	Este script hace contacto con el servidor DHCP remoto ( si lo hay ) e intenta recuperar información sobre el diseño de la red. Algunos servidores DHCP proporcionan información confidencial, como el nombre de dominio NIS o la información de diseño de red, como la lista de servidores web de red, etc. No demuestra ninguna vulnerabilidad, pero un atacante local puede usar DHCP para familiarizarse íntimamente con la red asociada.
<b>Recomendación:</b>	Aplique filtrado para mantener esta información fuera de la red y elimine cualquier opción que no esté en uso.

### **Fase 3. Salvaguardas**

Se toman en cuenta las amenazas y vulnerabilidades identificadas en la red de wifi y se recopila la información relevante. Se destaca la importancia de proteger la información y reducir las amenazas para disminuir los riesgos asociados con la empresa.

### **Fase final. Impacto y riesgo residual**

Se evalúa el impacto potencial y el riesgo residual de los riesgos identificados durante el análisis. Estos riesgos podrían causar la pérdida significativa de información y poner en peligro los activos y la infraestructura de nuestra red wifi, por lo que se deben tomar medidas correctivas para minimizar su impacto.

## DISCUSIÓN DE RESULTADOS

Como se puede observar en las imágenes que muestran los resultados, el escaneo realizado con la herramienta NESSUS detectó vulnerabilidades de diferentes niveles de impacto, ya sea alto, medio o bajo. Fue posible identificar un total de 23 vulnerabilidades, de las cuales la mayoría se encontraban relacionadas con SSL se trata de un procedimiento diseñado para navegadores y servidores web, que permite asegurar la autenticidad, cifrado y descifrado de la información que se envía por medio de Internet.

Se ha comprobado que la versión de OpenSSL en el servidor remoto permite que la sesión se reanude con un cifrado menos seguro que el utilizado en la sesión original. Esto implica que un atacante, al interceptar el inicio de una conexión SSL, puede manipular el caché de sesión OpenSSL para que las siguientes reanudaciones de dicha sesión utilicen un cifrado menos seguro elegido por el atacante.

Otra de las debilidades identificadas fue una mala configuración, que se refleja como una configuración defectuosa de la tunelización, con un impacto considerado medio. Esto implica que, al existir solicitudes consecutivas a una misma conexión, algunas de ellas podrían ser autenticadas o validadas correctamente mientras que otras no, debido a esta mala configuración.

Encontramos una vulnerabilidad media la cual se llama TLS Versión 1.1 Protocolo deprecado, este servicio remoto acepta conexiones cifradas con TLS, la cual carece de soporte para suites cifradas actuales y recomendadas. Los cifrados que admiten cifrado antes del cálculo MAC y los modos de cifrados autenticados como GCM no se pueden usar con TLS 1.1. Al 31 de marzo de 2020, los puntos finales que no están habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web y proveedores principales.

## CONCLUSIONES

Es importante tener en cuenta los factores de amenaza, riesgos y vulnerabilidades que se presentan en la red Wifi para poder determinar y fortalecer los posibles puntos de acceso vulnerables mediante una prueba de hacking ético. A partir de esto, las recomendaciones de las mejores prácticas de seguridad de la red Wifi deben ser implementadas para mejorar la privacidad y confidencialidad de los datos que compartimos a través de ella, garantizando así la integridad y protección de nuestro entorno digital.

Al establecer políticas de seguridad claras, capacitar a los usuarios, implementar soluciones de seguridad, y mantener actualizado el sistema, se minimiza el riesgo de ataques cibernéticos y se asegura la confidencialidad, integridad y disponibilidad de los datos transmitidos a través de la red Wifi. Es fundamental para protegerla de posibles ataques informáticos. Conociendo los puntos débiles, se pueden establecer medidas de seguridad más efectivas y evitar que los datos sean comprometidos

A pesar de que el hacking ético puede ser muy útil, no es la única forma de mejorar la seguridad de la red wifi. Es importante implementar otras medidas de seguridad, como el uso de contraseñas seguras, la configuración correcta del router y la instalación de software de seguridad. el hacking ético puede ser una herramienta útil para identificar vulnerabilidades en la red wifi y tomar medidas para protegerla. Las mejores prácticas de seguridad, como emplear contraseñas seguras, actualizar regularmente el firmware y limitar el acceso al router, también son importantes para garantizar la seguridad de la red. Al implementar estas medidas, los usuarios pueden minimizar el riesgo de sufrir un ataque malicioso y mantener la privacidad y la integridad de su información en línea.

## RECOMENDACIONES

Implementar, control y monitoreo constante de las actividades en el sistema informático para detectar y eliminar posibles amenazas y vulnerabilidades. Algunas de las vulnerabilidades identificadas incluyen problemas en la configuración de DDs en Apache, la detección de versiones 2 y 3 del protocolo SSL, métodos HTTP TRACE/TRACK permitidos en Apache HTTP y certificados SSL no confiables. Es importante tomar medidas para reducir el riesgo de futuros ataques a la seguridad en la red de wifi y garantizar la integridad y confidencialidad de los datos. Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

Utilizar herramientas de detección de vulnerabilidades de renombre y reconocidas en el mercado tecnológico para identificar y remediar las vulnerabilidades identificadas. Es importante también llevar a cabo un monitoreo constante de la red y establecer políticas de seguridad adecuadas que permitan la detección temprana de cualquier posible amenaza o vulnerabilidad. Además, es importante mantenerse actualizado sobre las últimas tendencias y amenazas en el mundo de la ciberseguridad, para poder tomar medidas preventivas eficaces.

Se deben realizar pruebas de seguridad regularmente para asegurarse de que la red wifi está protegida contra posibles ataques. Esto puede incluir pruebas de penetración, evaluaciones de vulnerabilidades y auditorías de seguridad. Se deben implementar medidas de seguridad adicionales en la red wifi, como la actualización regular del firmware del router, el uso de un software de seguridad actualizado y la configuración correcta del firewall.

## Referencias

- Altube, V. R. (11 de Noviembre de 2020). *OpenWebinars*. Obtenido de OpenWebinars: <https://openwebinars.net/blog/que-es-openvas/>
- Benavides, E. F. (2020). Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social. *CIENCIA UNEMI*, 13(32), 27-40. doi:<https://doi.org/10.29076/issn.2528-7737vol13iss32.2020pp27-40p>
- Coronel, I. A., & Quirumbay, D. I. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Universidad Estatal Península de Santa Elena, UPSE | La Libertad - Ecuador*, 97-109. doi:<https://doi.org/10.26423/rctu.v9i2.672>
- Cristancho, F. (13 de Enero de 2022). *Talently* . Obtenido de <https://books.google.com.mx/books?id=7frADwAAQBAJ&printsec=frontcover&hl%20%20=es#v=onepage&q&f=false>
- Equipo editorial, E. (6 de Septiembre de 2018). *Enciclopedia Humanidades*. Obtenido de Enciclopedia Humanidades.: <https://humanidades.com/sistema-de-informacion/>
- Gamboa Suarez, J. L. (2020). Importancia de la seguridad informatica y ciberseguridad en el mundo actual. *Universidad Piloto de Colombia*, 1-12. Obtenido de <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y>
- Gauthier, V., & Mendez, R. A. (2020). *Seguridad Informática*. Bogotá D. C: Editorial Universidad del Rosario. doi:<https://doi.org/10.12804/si9789587844337>
- Gomez, S. (2019). IMPLEMENTACIÓN DE UN APLICATIVO MÓVIL WALK. *MAGÍSTER EN TELECOMUNICACIONES. ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL*, Guayaquil. Obtenido de

<https://www.dspace.espol.edu.ec/bitstream/123456789/52649/1/D-CD109530%20-%20G%c3%b3mez%20Romero.pdf>

Laudon, K. . (2018). Administración de los Sistemas de Información Capítulo 1-El reto de los sistemas de Información Qué es un sistema de información? *Tecnología Laudon & Laudon*, 1-65. Obtenido de [https://www.emagister.com/uploads\\_user\\_home/Comunidad\\_Emagister\\_8601\\_laudon.pdf](https://www.emagister.com/uploads_user_home/Comunidad_Emagister_8601_laudon.pdf)

Lederkremer, M. (2019). *Redes informaticas*. Buenos Aires: Six Ediciones. doi:<https://books.google.com.mx/books?id=7frADwAAQBAJ&printsec=frontcover&hl%20%20=es#v=onepage&q&f=false>

LLamas, J. (1 de Agosto de 2022). *Economipedia*. Obtenido de <https://economipedia.com/definiciones/hacker.html>

Marker, G. (2019). *Tecnologia-informatica.com*. Obtenido de <https://www.tecnologia-informatica.com/que-es-un-cracker/>

Ponce Larreategui, J. G. (2021). INDICADORES DE COMPROMISO (IOC) PARA DETECCIÓN DE AMENAZAS EN LA SEGURIDAD INFORMÁTICA CON ENFOQUE EN EL CÓDIGO MALICIOSO. (*Titulo de Ingeniero de sistemas*). Universidad Politecnica Salesiana Ecuador, Guayaquil.

Postigo Palacios, A. (2020). *Seguridad informática*. Paraninfo.

Restrepo, Z. A. (25 de Julio de 2019). Vulnerabilidades en redes de internet alámbricas e inalámbricas. *Universidad Nacional Abierta y a Distancia UNAD*, 1-117. Obtenido de <https://repository.unad.edu.co/handle/10596/27729>

Romero Castro, M. I., Vera Navarrete, D. S., Alava Cruzatty, J. E., Parrales Anzules, G. R., Alava Mero, C., Murillo Quimiz, A. L., & Y Castillo Merino, M. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMATICA Y EL ANALISIS DE VULNERABILIDADES*. C/ Els Alzamora, 17 - 03802 - ALCOY (ALICANTE):

3ciencias Área de Innovación y Desarrollo,S.L.  
doi:ttp://dx.doi.org/10.17993/IngyTec.2018.46

Tamayo, S. (2019). *UHemisferios IMF*. Obtenido de  
<https://globalimf.com.ec/uhemisferios/blog/gestion-de-riesgos-informaticos/>

Tecnolgia, T. (29 de Julio de 2022). *TECH Ecuador - Blog TECH*. Obtenido de Universidad  
Tecnologica: <https://www.techtitute.com/ec/escuela-de-negocios/blog/hacking-etico>



## ANEXOS

## Ejecucion de Nessus

**nessus** Scans Settings ItatyVivar

**My Scans** Import New Folder New Scan

Search Scans 5 Scans

Name	Schedule	Last Scanned
Analisis de red wifi	On Demand	Today at 11:28 AM
Wifi	On Demand	March 19 at 8:47 PM
Practica	On Demand	March 16 at 3:33 PM
Proyect	On Demand	March 12 at 6:24 PM
proyect	On Demand	March 12 at 5:45 PM

Tenable News

**Escaneos** Configuraciones Itaty

Hosts 1 Vulnerabilidades 23 Amenazas superiores VPR Historia 1

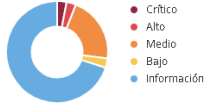
Filtro Buscar hosts 1 Anfitrión

Anfitrión	Vulnerabilidades
192.168.100.1	1 1 7 1 29

**Escaneos detalles**

Política: Escaneo avanzado  
 Estado: Completado  
 Base de gravedad: CVSS v3.0  
 Escáner: Escáner local  
 Comienzo: Hoy a las 11:27 a.m.  
 Fin: Hoy a las 11:40 a.m.  
 Elapso: 12 minutos

**Vulnerabilidades**



- Crítico
- Alto
- Medio
- Bajo
- Información

**Vulnerabilidades** 23

Filtro Buscar vulnerabilidades 23 Vulnerabilidades

Sev	Puntuac...	Nombre	Familia	Contar
CRÍTICO	9,8	Detección de protocolo S...	Detección de servicio	1
MIXTO	...	SSL ( Problemas múl...	General	9
MEDIO	6,5	Servidor Telnet sin cifrar	Misceláneo.	1
MEDIO	4,3 *	OpenSSL SSL_OP_NETSC...	General	1
MIXTO	...	TLS ( Problemas múl...	Detección de servicio	3
BAJO	3,3 *	Detección del servidor D...	Detección de servicio	1
INFORMACIÓN	...	TLS ( Problemas múl...	General	2
INFORMACIÓN		Escáner Nessus SYN	Escáneres de puerto	3
INFORMACIÓN		Detección de servicio	Detección de servicio	3

