UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROPUESTA DE METODOLOGÍA PARA EVALUAR LA SEGURIDAD INFORMÁTICA PERIMETRAL DE UNIDADES UNIVERSITARIAS.

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERA CIVIL EN COMPUTACIÓN

VALENTINA DANIELA RAMOS BUSTOS

PROFESOR GUÍA:
ALEJANDRO HEVIA ANGULO

MIEMBROS DE LA COMISIÓN:
FEDERICO OLMEDO BERÓN
IVANA BACHMANN ESPINOZA

SANTIAGO DE CHILE
2023

Resumen

La tecnología y la conectividad global están en constante crecimiento, lo que aumenta los riesgos de ser utilizados con intenciones maliciosas. Por eso, la ciberseguridad es fundamental para proteger nuestros datos y servicios. Las instituciones educativas son especialmente vulnerables a los ciberataques debido a su tendencia a mantener sistemas abiertos. Es importante que estas organizaciones adopten medidas proactivas en lugar de reactivas para fortalecer su seguridad. La concienciación y la educación en seguridad digital desde temprana edad son clave. En el caso de Chile, la educación superior es un objetivo atractivo para los ciberatacantes. Por esto, surge la idea de una herramienta que permita evaluar la seguridad de los establecimientos con el fin de aportar a una futura implementación de medidas de prevención de delitos informáticos en este sector.

Se propone una metodología que identifique y evalúe los riesgos de seguridad de la red dentro del contexto mencionado. Esto con el fin de brindar un mejor entendimiento de seguridad informática a las instituciones educacionales. Este trabajo busca además ser un aporte para el proceso de elaboración de un plan de acción que busque un mejoramiento en el sistema de seguridad informática existente. De igual forma, se busca promover la conciencia y educación en ciberseguridad entre el personal y los estudiantes.

La metodología propuesta consta de tres etapas: análisis pasivo, análisis activo y análisis de resultados. En el primer análisis, se recopila información sobre la infraestructura de red, como la topología, dispositivos utilizados y políticas. En el análisis activo, se evalúan las configuraciones de seguridad existentes, se identifican los dispositivos activos en la red, se analizan las posibles vulnerabilidades y se evalúan las políticas de seguridad. Durante el análisis de resultados, se relacionan y evalúan los resultados obtenidos de las etapas anteriores para determinar el estado general de la red. Esto permite a la entidad diseñar un plan de acción para mejorar la seguridad informática, priorizando la resolución de problemas identificados.

El trabajo realizado se considera satisfactorio, brindando un aprendizaje significativo y siendo percibido como una herramienta expansible y mejorable para fortalecer la ciberseguridad en el ámbito educativo. Se destaca la escasa información sobre seguridad informática en instituciones de educación superior, lo que podría ser un tema de investigación futuro. El trabajo en colaboración con el equipo encargado de la red fue una experiencia enriquecedora, generando nuevas preguntas y desafíos relacionados con la ciberseguridad en la institución. Este proyecto proporcionó valiosas lecciones sobre colaboración, trabajo en equipo y la complejidad de analizar redes con múltiples entidades, contribuyendo al desarrollo profesional de la estudiante.

A mi mamá, que sin todo su apoyo no sería ni un grano de arena de la persona que soy.

Agradecimientos

El desarrollo de esta memoria fue el resultado de largos 6 años y medio en la facultad, que quizás hubieran sido posibles de sobrellevar de forma solitaria, pero que ciertamente no hubieran sido tan geniales como lo fueron. Por esto me gustaría agradecerle a cada unx de mis amigxs que pude conocer a lo largo de esta carrera. Me acompañaron en tantas rabias, penas, frustraciones, trasnoches, pero por sobretodo alegrías, risas y la creación de recuerdos inolvidables.

Gracias al profesor Alejandro Hevia por apoyarme en el desarrollo de esta memoria y darme ánimo en mis momentos de casi-crisis que por suerte no llegaron tan lejos.

También quiero agradecer a Diego Vargas por guiarme en mis primeros pasos en la ciberseguridad, apoyarme en el desarrollo de mi memoria y ayudarme a encontrar mi motivación dentro de la computación.

Gracias también a lxs amigxs que conocí durante mi último año en la carrera, gracias a ustedes me motivé a escribir esta memoria e hicieron de mi último semestre uno de los mejores que tuve. Gracias por todas las risas y tardes en el toqui, fue genial compartir con ustedes.

Quiero hacer una mención especial a mis mejores amigas, que también conocí durante estos años. Amigas, estoy infinitamente agradecida con la vida de haberlas conocido, son lo más bello que existe e hicieron de mi paso por la universidad una experiencia que hasta me dan ganas de repetir. Las amo con todo mi corazón, gracias por todos estos años de amistad, no saben lo feliz que me hacen. Los agradecimientos en una memoria quedan cortísimos para expresarles todo, pero me encargaré de hacerlo durante todos los años de amistad que nos quedan por delante.

Y finalmente, gracias mi apoyo incondicional, mi mamá. Ni todas las palabras del mundo juntas podrían expresar lo agradecida que estoy contigo, pero aquí va una pequeña muestra. Gracias por apoyarme en absolutamente todo, por escucharme, por crecer junto a mí, por amarme con todo tu corazón, por acompañarme, por cuidarme, por ser la mejor mamá del mundo. Gracias por creer en mí cuando ni yo podía hacerlo. Te amo con todo mi corazón, nada de esto sería posible sin ti.

Gracias.

Tabla de Contenido

Índice de Ilustraciones

Capítulo 1

Introducción

La tecnología, la conectividad global y usos de servicios en la nube crecen y se desarrollan cada día, y de igual forma crecen los riesgos de utilizarse con intenciones maliciosas. Es por esto que la ciberseguridad toma un papel fundamental hoy en día para la protección de nuestros datos y servicios.

La ciberseguridad es el área de la tecnología que busca proteger y defender sistemas electrónicos, como computadores, servidores, dispositivos móviles, redes y los datos que ellos almacenan. También se conoce como seguridad de tecnología de la información, seguridad computacional o seguridad de la información electrónica.

Esta área es de gran importancia ya que abarca todo lo relacionado con la protección de datos personales, información de identificación personal, información de salud, propiedad intelectual, preferencias políticas, sistemas gubernamentales, educacionales y de la industria. Su acceso indebido por entes maliciosos puede implicar grandes daños a los titulares o dueños de dichos sistemas.

Dentro de las grandes entidades que corren grandes riesgos si no se adoptan las medidas cautelares necesarias, están las instituciones de educación.

Las organizaciones docentes o académicas son una opción atractiva para ciberdelincuentes debido a la natural tendencia de estas instituciones a mantener sistemas abiertos y/o con accesos más permisibles a sus usuarios dado la gran cantidad de estos. Así, en el sector de la educación, los ciberdelincuentes podrían obtener:

- Información sobre el personal y estudiantes.
- Bases de datos asociados a alumnos/as y exalumnos/as.
- Detalles de proveedores.
- Datos de investigación.

- Detalles sobre bienes materiales en los establecimientos educacionales.

Es imprescindible que las organizaciones asociadas a la educación mejoren su ciberseguridad, y la mejor estrategia para hacerlo es adoptando una mentalidad proactiva, en lugar de una reactiva. Los centros educativos no deben esperar a que suceda un ataque para comenzar a preparar sus defensas. Más bien, con antelación deben tener presente que los ciberataques son una realidad cada vez más recurrente. De no estar preparados, podrían sufrir grandes consecuencias.

La concientización, educación y capacitación en seguridad digital de forma temprana es muy importante para un correcto uso y mejor aprovechamiento en las tecnologías actuales en el área educacional. En particular, durante el año 2021 el Estado de Chile destinó un 47 % más de recursos a la educación superior que a la escolar, por lo que representa un objetivo más atractivo para ciberatacantes [1]. Es por esto que el desarrollo de esta memoria estará enfocado en este sector educacional superior y en la relevancia que representa un adecuado sistema y metodología de prevención de delitos informáticos.

1.1. Objetivos

1.1.1. Objetivo General

El objetivo general de este trabajo busca proponer una metodología para evaluar la seguridad informática perimetral de unidades académicas (facultades o similares) dentro de establecimientos de educación superior vía análisis de sus redes públicas o semi-públicas.

1.1.2. Objetivos Específicos

- Investigar posibles estrategias (incluyendo análisis pasivo y activo de redes) para realizar análisis de redes en redes inalámbricas.
- Aplicar algunas de estas estrategias dentro del establecimiento educacional local, incluyendo las distintas etapas de análisis de redes en un rol de interno (con credenciales de acceso).
- Identificar las consecuencias que podrían existir si la información obtenida con los análisis estuviera en manos de atacantes reales.
- Concientizar mediante los resultados obtenidos la importancia de la protección de datos pertenecientes a establecimientos educacionales.
- Explorar alternativas para validar la metodología propuesta (no incluye validarla).

1.2. Solución Propuesta

Para lograr los objetivos propuestos, antes de comenzar se deben conseguir las autorizaciones correspondientes para realizar el estudio e información clave de la red, como lo sería su respectiva segmentación, la existencia de segmentos protegidos y la relación usuarios-privilegios dentro de esta. Dentro de este proceso, se solicitan credenciales de acceso a la red Wi-Fi local, autorización de ingreso físico al lugar a estudiar y segmentación respectiva de la red, esto con el fin de simular ataques internos. Para esto, mediante contactos académicos del profesor guía, se hace llegar una solicitud formal a las autoridades correspondientes de la facultad en cuestión.

Además, se considerará una red "pública" si es de tipo inalámbrica y si conectarse a ella está permitido a cualquier persona físicamente presente en una instalación. Una red será "semi-pública" si una persona presente en la instalación pudiera tener la posibilidad de conectarse física o lógicamente, aún si la red tiene mecanismos de autenticación que buscan restringir el acceso a dicha red.

En cuanto al trabajo como tal, en primera instancia, se realizará un análisis pasivo de las redes y casa de estudio con el uso de credenciales de autenticación, las cuales deberían ser brindadas por la institución al momento de recibir las autorizaciones correspondientes.

El análisis pasivo de las redes consistirá en una investigación que busca obtener información sobre lugares donde sea posible conectarse a una red, métodos de acceso, características de las facultad a analizar, posibles ataques anteriores, políticas de seguridad, dispositivos y restricciones. Además, dentro de este análisis, se identificarán algunas características específicas de la red. Por ejemplo, tipo de seguridad, de cifrado y autenticación.

En segundo lugar se procederá con el análisis de carácter activo, el cual consistirá en una evaluación de configuraciones y protección existente. Dentro de este, se llevará a cabo una serie de escaneos a la red con el fin de encontrar *hosts* activos, sus servicios asociados y un análisis de vulnerabilidades de estos. Para la ejecución de lo anterior, se hará uso de herramientas tipo escáner como *Nmap* [12] y *OpenVas* [8].

Finalmente, dentro de esta etapa, se procede a realizar una tercera evaluación del proceso de análisis. La cual, consiste en cuantificar el nivel de acceso a la información utilizando el sistema de puntuación *Common Vulnerability Scoring System* (CVSS) [4] como guía, información la cual posteriormente se debe analizar dentro de un contexto de establecimiento de educación superior.

Como adicional, en la parte final del estudio, se explorarían posibles estrategias que llevarse a cabo para validar la metodología. Este trabajo, sin embargo, no contempla realizar dicha validación.

Capítulo 2

Estado del Arte

2.1. Situación Actual

La pandemia de Covid-19 ha generado cambios profundos en muchos ámbitos, donde la educación no ha sido ajena. El aumento significativo del aprendizaje remoto y en línea ha obligado a la mayoría de establecimientos educacionales a una transición tecnológica donde la implementación de soluciones innovadoras es imprescindible.

Sin embargo, dichas soluciones se han realizado de forma rápida en pos de mantener activo el aprendizaje, lo cual hizo inevitable la aparición de nuevas vulnerabilidades y riesgos asociados.

Es importante señalar, que incluso antes de la pandemia el problema de la ciberseguridad en la educación ya estaba presente, pues en general ya existía una falta de fondos y/o personal capacitado para esta área específica. Desde hace años, las escuelas han evidenciado errores básicos de configuración del sistema, o simplemente mantienen problemas antiguos sin solucionar.

Actualmente el sistema educacional superior en Chile depende en grandes cantidades de la tecnología y conectividad, ya sea mediante su uso computacional como el almacenamiento de datos en la nube, material educativo online, clases virtuales, áreas administrativas y bases de datos. Como también su uso relacionado al acceso de personas a la diversas casas de estudio, facultades y laboratorios. En esto se incluyen también los distintos equipos a disposición de las personas pertenecientes a la comunidad universitaria, como computadores, impresoras, cámaras de seguridad, etc.

Los atacantes informáticos tienen una amplia gama de oportunidades para explotar la seguridad de estos centros educativos, ya que en general funcionan con sistemas antiguos u obsoletos los cuales no están preparados para hacer frente a ataques actuales más elaborados. Por ejemplo, en las universidades específicamente ya existe un historial de ataques de *malware* donde atacantes han robado o eliminado datos de los sistemas de los usuarios [6]. Además, también ataques de *ransomware* han provocado la inaccesibilidad a ordenadores pidiendo a cambio una suma de dinero para devolver el acceso a los datos [14].

Por otra parte, la seguridad física de los establecimientos también corre riesgo al momento de un ciberataque, ya que atacantes podrían ingresar a casas de estudio con acceso restringido, obtener información sobre la existencia de dispositivos tecnológicos de valor conectados a la red, manipular cámaras de seguridad, por ejemplo. Esto podría poner en riesgo la integridad de las personas presentes en el espacio educativo atacado.

Con la transición hacia un mundo digital, los efectos de la falta de seguridad pueden ser perjudiciales a mayor escala. Los centros educacionales necesitan conocimientos y una infraestructura tecnológica actualizada para ofrecer un aprendizaje virtual y presencial de manera segura a largo plazo.

Por lo anteriormente mencionado, un buen punto de inicio para que cualquier establecimiento educacional pueda tener una noción del estado de su seguridad es solicitar una prueba de penetración de sus sistemas para así tener la posibilidad de incrementar sus defensas y estar mejor preparados para un posible futuro incidente.

2.2. Técnicas

Para el desarrollo de esta memoria, se emplearán diversas técnicas previamente existentes relacionadas a las distintas etapas de lo que contempla un análisis de redes. Es importante mencionar que existe un gran número de herramientas, tecnologías y técnicas con las cuales se podría desarrollar un completo análisis perimetral de redes, su selección dependerá del criterio de la persona encargada de la realización de este análisis.

En este caso en particular, se presentan algunas técnicas relevantes que se podrían utilizar para el trabajo a realizar y las cuales representan un aporte importante en el ámbito de la ciberseguridad.

2.2.1. *Sniffing*

Corresponde a una técnica utilizada con el fin de monitorear lo que ocurre dentro de una red, lo cual se suele realizar en redes internas, aunque, también se puede emplear con paquetes en internet.

Este proceso es posible de realizar mediante el uso de algunas herramientas destinadas a la seguridad informática, las cuales son capaces de actuar sobre los sistemas que componen el tráfico de una red. Estas aplicaciones tienen la finalidad de capturar, interpretar y almacenar paquetes de datos que viajan por la red, para posteriormente ser analizados.

Los programas de *sniffing* hacen uso de la tarjeta de red de un equipo, para así obtener el tráfico que fluye por la red a que se esté conectado, ya sea una conexión mediante cable o inalámbrica.

Este tipo de software no solo captura los paquetes destinados a una tarjeta de red, sino

que recoge todos los paquetes destinados a todas las tarjetas de red que se encuentren en su área local, abriendo la posibilidad de encontrar información crucial sobre ésta.

Una de las herramientas de *sniffing* más utilizadas del mercado corresponde a *WireShark*, software de descarga gratuita disponible en internet [3].

2.2.2. Escaneo de red

Durante las etapas iniciales de un análisis de vulnerabilidades en una red, es importante detectar qué hosts se encuentran levantados y si existe algún puerto abierto asociado. Para esto, existen diversas herramientas de escaneo, una de las más conocidas corresponde a *Nmap*, la cual es completamente gratuita y de código abierto.

La primera etapa de esta técnica consiste en identificar qué hosts se encuentran activos en la red. Para esto, una herramienta de escaneo se encarga de buscarlos y mapearlos con sus direcciones IP respectivas.

Luego, con una lista de hosts activos, es posible realizar un segundo escaneo, pero asociado a los puertos. Esto consiste en el envío de paquetes a puertos específicos en un host y al análisis de respuestas para conocer detalles sobre los servicios en ejecución o identificar posibles vulnerabilidades.

Utilizar esta técnica permite obtener una gran cantidad de información sobre los equipos y servicios pertenecientes a una red. También permite averiguar si ciertos hosts específicos están conectados a Internet o a la red local, comprobar la existencia de puertos abiertos, verificar la presencia de un firewall e incluso podría entregar información sobre qué sistema operativo está utilizando un objetivo.

2.2.3. Análisis de vulnerabilidades

El proceso de identificación de potenciales vulnerabilidades de seguridades de una red corresponde a un análisis de vulnerabilidades. Dentro de los métodos más utilizados se encuentra el uso de software de tipo scan, los cuales se encargan de descubrir hosts activos, enumerar servicios dentro de estos, evaluar la presencia de vulnerabilidades y reportarlas.

Corresponde a una herramienta que permite obtener una visión preliminar del estado de la seguridad de la red analizada, pues existe la posible presencia de falsos positivos y/o complejidad insuficiente al momento de realizar el descubrimiento de hosts.

Sin embargo, se considera como un aporte dentro del proceso de análisis de redes pues aporta información útil para su posterior análisis dentro del contexto donde se esté llevando a cabo esto, permitiendo así una mejor priorización en cuanto a tomar medidas que busquen la mejora del sistema de seguridad que se tenga hasta el momento.

Dentro de las herramientas más utilizadas se encuentra la herramienta de scan pagada *Nessus* [5] y el software gratuito *OpenVas*.

2.3. Estudios y Comunidades Relacionadas

Existe una gran cantidad de lecturas relacionadas al impacto que han tenido distintos ataques cibernéticos al área educativa al rededor del mundo. Sin embargo, en cuanto a estudios y metodologías de prevención dedicadas específicamente a esta área, la cantidad de estos es considerablemente menor. De lo anterior, es posible analizar que existe una cultura reactiva en cuanto a incidentes de seguridad informática en el área educacional, cuando lo recomendable es una mirada preventiva de los posibles riesgos asociados a las tecnologías utilizadas en esta área.

En cuanto a estudios, el reporte de ciber impacto 2022 realizado por *Jisc* [10], una organización sin fines de lucro que proporciona servicios de red y TI a instituciones de educación superior e investigación en Reino Unido, sugiere que existe una mayor amenaza de ataques de *ransomware* contra la educación.

Según dicho reporte, docenas de universidades, colegios y escuelas del Reino Unido han sufrido ataques de *ransomware* desde 2020, causando interrupciones al personal y a los estudiantes, y costando a las instituciones cantidades sustanciales de dinero.

En algunos incidentes, *Jisc* afirma que los costos del impacto han superado los 2 millones de libras (2.255.818.000 pesos chilenos).

Durante los últimos años, se han diseñado diversas metodologías de evaluación de seguridad de redes o pasos a seguir para evaluar la seguridad informática perimetral [2], sin embargo, luego de la investigación llevada a cabo por la estudiante para el desarrollo del presente trabajo, es inevitable notar la escasez de estudios de estas técnicas enfocadas en el contexto educativo.

Por otra parte, en respuesta a la necesidad de compartir conocimiento y colaborar con información para así evitar ataques computacionales a instituciones de educación superior, es que surge la creación de comunidades como la Comunidad CISO (del inglés *Chief Information Security Officer* o bien el Jefe de Seguridad de la Información) Universitaria que agrupa a los responsables y especialistas en el tema. Esta comunidad cuenta agrupa hoy a más de 40 representantes de diferentes casas de estudios a nivel nacional y otros colaboradores. [13]

En mayo de 2019 se concretó la primera reunión en donde participaron instituciones de todo el país de manera presencial y por videoconferencia. En dicho encuentro se presentó la experiencia de la Casa de Bello, motivando al resto a intercambiar puntos de vista y animándolos a perder el miedo a compartir.

Además, se elaboró una encuesta entre la comunidad, de modo de conocer con más detalle la realidad en las instituciones de educación superior; la que reveló, entre otros datos, que un 43,5 % de las universidades no cuenta con una Política General de Seguridad de la Información, mientras que un 34,8 % comentó que contaban con un lineamiento base, el que no estaba oficializado; y sólo un 21,7 por ciento refirió contar con una Política General de Seguridad de la Información.

Capítulo 3

Problema

La falta de seguridad en redes inalámbricas dentro de un establecimiento de educación superior puede ser un problema serio, ya que las redes no seguras son vulnerables a ataques cibernéticos y pueden exponer información confidencial a posibles hackers. Algunos de los problemas que pueden surgir incluyen:

- Acceso no autorizado: Si la red inalámbrica no está protegida con un sistema de autentificación, cualquier persona podría conectarse a ella sin autorización y acceder a los recursos compartidos, como archivos y carpetas compartidas. Lo cual podría exponer información confidencial o incluso permitir que un atacante instale software malicioso en la red.
- Intercepción de datos: En caso de que la red no esté encriptada, cualquier persona cercana a la red podría capturar los datos que se transmiten por ella, incluyendo contraseñas, nombres de usuario, información financiera y otra información confidencial. La falta de encriptación puede ser particularmente problemática en entornos educativos donde los estudiantes y el personal pueden estar accediendo a información confidencial en línea.
- Riesgo de malware: Cuando una red inalámbrica no está protegida con un software antivirus, puede ser vulnerable a ataques de malware. Los virus y otros tipos de malware pueden propagarse rápidamente a través de una red sin protección y pueden causar daños importantes en los sistemas conectados a ella.

Teniendo en cuenta los posibles problemas que puede traer una deficiencia en la seguridad de la redes en el contexto planteado, resulta imperante tener una solución a esta problemática.

En el caso de esta memoria, esta solución se plantea como una metodología, la cual tiene como fin principal ser una herramienta que permita identificar y evaluar los posibles riesgos de la seguridad actual de la red. Tener esta información en conocimiento, trae múltiples beneficios para los establecimientos de educación, tales cómo:

- Facilita tomar medidas para proteger la información confidencial de los estudiantes, profesores y personal administrativo, como datos personales, registros académicos y financieros.
- Previene interrupciones no deseadas en las operaciones educativas. Identificar las vulnerabilidades permite implementar medidas de mitigación para evitar interrupciones en el acceso a servicios y recursos en línea.
- Muchos establecimientos de educación superior están sujetos a regulaciones y leyes relacionadas con la protección de datos, como el Reglamento General de Protección de Datos (GDPR) [15] en la Unión Europea. Conocer los riesgos ayuda a asegurar el cumplimiento de estas normativas y evitar posibles sanciones.
- Permite asignar recursos adecuados para implementar medidas de seguridad eficientes. Esto ayuda a priorizar las inversiones y acciones necesarias para proteger las redes y sistemas de manera más efectiva.

Por otra parte, como complemento a la implementación de esta metodología, cada casa de estudio debería promover la conciencia y la educación en ciberseguridad entre el personal y los estudiantes, fomentando una cultura de seguridad cibernética en toda la comunidad educativa.

3.1. Requisitos a considerar

Antes de comenzar con el desarrollo de la solución se considera como requisito previo la autorización por parte del establecimiento educacional, que en este caso corresponde al Campus Beauchef de la Universidad de Chile, para realizar una serie de pruebas necesarias para el diseño de la metodología a plantear. Esto incluye accesibilidad al campus, credenciales para ingresar a la red a analizar, permiso de ejecución de los distintos tests sobre esta y establecer cuáles serían los límites de al momento de implementarlos.

Con los requisitos de autorización obtenidos, se plantean los siguientes requisitos para la implementación de la metodología como tal:

- Información de la infraestructura de red: Es fundamental comprender la infraestructura de la red del establecimiento, incluyendo la segmentación de la red, la configuración de los dispositivos de red, los puntos de acceso inalámbrico y cableado, etc. Lo cual ayudará a identificar posibles puntos débiles y áreas de enfoque en el análisis de seguridad. Para obtener esta información, se considera una reunión previa con el equipo a cargo de las redes del establecimiento.
- Identificación de activos críticos: Obtener información sobre los activos críticos con acceso restringido, como servidores de datos, sistemas de información estudiantil, registros académicos y financieros, sistemas de gestión administrativa, sistemas de seguridad, etc. Cada entidad a cargo está encargada de definirlos y permite enfocar los esfuerzos de análisis en aquellos activos que son más valiosos y sensibles.

- Análisis de riesgos: Evaluación de los riesgos potenciales que pueden afectar la seguridad de la red. Puede incluir amenazas internas y externas, vulnerabilidades conocidas, análisis de malware y posibles escenarios de ataques. El análisis de riesgos ayudará a establecer prioridades y guiar las acciones de seguridad.
- Políticas y normativas: Considerar las políticas y normativas específicas que se aplican al establecimiento de educación superior, como las políticas de seguridad de la información y las regulaciones de privacidad de datos. Estas servirán como marco para desarrollar medidas de seguridad y garantizar el cumplimiento normativo.
- Herramientas y tecnologías: Identificar las herramientas y tecnologías necesarias para realizar el análisis de redes, como escáneres de vulnerabilidades, distintos softwares de código abierto comúnmente utilizados en ciberseguridad y herramientas de monitoreo de red. Es esencial contar con las herramientas adecuadas para realizar un análisis eficiente.
- Proceso de revisión y mejora continua: La metodología a plantear, se considera como un paso inicial al proceso de protección de redes, por lo que es recomendable establecer un proceso de revisión y mejora continua de esta. Es recomendable evaluar regularmente la eficacia de las medidas de seguridad implementadas, actualizar las políticas y procedimientos según sea necesario y estar al tanto de las nuevas amenazas y vulnerabilidades emergentes.

3.2. Características de calidad deseadas

En cuanto a características de calidad deseadas para la metodología a plantear, se consideran las siguientes:

1. Integridad: Debe abarcar todos los aspectos relevantes del análisis de redes, desde la identificación de activos y riesgos hasta la implementación de un análisis de vulnerabilidades básico. Proporcionando un enfoque simple y sistemático para evaluar la seguridad básica de la red.
2. Escalabilidad: Capacidad de adaptarse a diferentes tamaños y complejidades de redes. Esto con el fin de ser aplicable tanto a pequeños establecimientos de educación superior como a grandes universidades, y ser flexible para acomodar futuros cambios y expansiones de la red.
3. Repetibilidad: Posibilidad de aplicar de manera consistente y obtener resultados similares en diferentes ocasiones, asegurando que los análisis de redes se realicen de manera sistemática y confiable.
4. Enfoque basado en riesgos: Adoptar un enfoque basado en riesgos, centrándose en la identificación de las amenazas y vulnerabilidades más relevantes y críticas para la seguridad de la red. Lo cual permite priorizar acciones y recursos según el nivel de riesgo asociado.

5. Claridad y sencillez: La metodología debe ser clara y comprensible, evitando términos técnicos excesivamente complejos. Proporcionando instrucciones claras y paso a paso para llevar a cabo el análisis de redes, facilitando su implementación por parte de personal técnico y no técnico.

Capítulo 4

Solución

Se plantea una metodología básica de análisis de redes, la cual se divide en 3 etapas principales, análisis pasivo, activo y de resultados. Estas abarcan los pasos mencionados a continuación:

Análisis pasivo:

- Recopilación de información: Consiste en obtener información sobre la infraestructura de red, como la topología de la red, dispositivos de red utilizados, segmentación, restricciones y políticas.

Análisis activo:

1. Evaluación de configuraciones y protección existente: Consiste en la revisión de las configuraciones de seguridad preventivas existentes en la red, con el fin de evaluar la presencia de configuraciones incorrectas y/o la falta de estas.
2. Identificación de *hosts* activos: Identificar dispositivos o *hosts* que estén actualmente activos y accesibles dentro de la red utilizando herramientas de escaneo de red.
3. Análisis de vulnerabilidades: Realizar un análisis de vulnerabilidades en los *hosts* identificados para evaluar la existencia de posibles vulnerabilidades.
4. Evaluación de políticas de seguridad: Revisar y evaluar las políticas y procedimientos de seguridad existentes en la red para asegurar el cumplimiento de los estándares mínimos de seguridad.

Análisis de resultados:

Una vez obtenidos los resultados tanto del análisis pasivo como activo, es posible relacionarlos y evaluar el estado general de la red. Esto con el objetivo de que la entidad a cargo

pueda diseñar un plan de acción en cuanto a mejoramiento de su seguridad informática, guiándose en los resultados y permitiéndoles así definir cierta prioridad para la resolución de sus problemáticas.

4.1. Metodología

4.1.1. Antes de comenzar

A modo de precaución, se sugiere dar aviso de la ejecución de la metodología a la entidad correspondiente, ya que esta implica un tráfico inusual de paquetes dentro de la red. Este podría ser visto como una amenaza, provocando un posible bloqueo de dirección IP del equipo utilizado para esta ejecución.

A continuación, se define el paso a paso de la metodología planteada.

4.1.2. Análisis Pasivo

El análisis pasivo, se plantea como la etapa del análisis de redes en donde se recopila información y se realizan evaluaciones sin interactuar directamente con la red.

El objetivo principal es obtener una visión general de la red y su estado actual sin realizar acciones que puedan afectar su funcionamiento.

Recopilación de información

Esta primera fase consiste en la obtención de información relevante sobre la infraestructura de la red que se va a analizar. Para esto, es necesario consultar al equipo encargado sobre ciertos elementos claves mencionado a continuación:

- Topología de red: Corresponde a cómo se estructura y conecta la red, identificando sus diferentes componentes y cómo se comunican entre sí. Puede incluir la ubicación física de los dispositivos de red y la forma en que están interconectados.
- Dispositivos: Para comprender la infraestructura y los puntos de acceso que deben ser considerados en el análisis de seguridad, es necesario identificar los dispositivos de red presentes. Estos pueden incluir routers, switches, firewalls, puntos de acceso inalámbrico, etc.
- Segmentación: Consiste en la separación lógica de las partes de una red en función de diferentes criterios, como la función, el departamento, la ubicación geográfica o los niveles de seguridad requeridos. Cada segmento o subred puede tener sus propias políticas de seguridad, configuraciones de red y controles de acceso.

- Restricciones y políticas: Para evaluar posibles prácticas inseguras, se necesita información sobre los ajustes de seguridad, restricciones y las políticas de acceso de los dispositivos de red.

4.1.3. Análisis Activo

El análisis activo se refiere a un análisis donde existe interacción directa con la red, ya sea mediante la generación de tráfico dentro de esta, o el envío de solicitudes a dispositivos específicos que se encuentren conectados.

Este tipo de análisis permite realizar pruebas controladas y obtener información sobre dispositivos conectados, puertos abiertos, posibles brechas de seguridad y debilidades en la infraestructura de la red.

Evaluación de configuraciones y protección existente

Uno de los primeros pasos para proteger una red y a los usuarios que la utilizan, es mantener una correcta y actualizada configuración de seguridad. Esta puede constar de diversos factores, se ejemplifican algunos a continuación:

- Cifrado: Corresponde al proceso de codificación de los datos transmitidos entre dispositivos, con el fin de proteger la confidencialidad e integridad de estos.
- Autenticación: La presencia de un sistema de autenticación en la red, corresponde a una medida básica imprescindible para evitar que cualquier dispositivo se conecte a esta. De no estar implementada esta medida, un atacante podría conectarse fácilmente y comprometer los datos existentes.
- Firmware actualizado: Consta de mantener el firmware de los routers presentes en la red actualizado. Esto evita la vulnerabilidad a brechas de seguridad conocidas asociadas a versiones anteriores de estos.
- Cifrado obsoleto: Evitar la utilización de un cifrado obsoleto como WEP (Wired Equivalent Privacy). Ya que probablemente han sido ampliamente comprometidos y no ofrecen una protección adecuada.
- Antivirus: El uso de un antivirus dentro de la red puede ayudar a protegerla de diversas amenazas, tales como virus, malware,ransomware, phishing, entre otros. Su funcionamiento consiste en escanear archivos y tráfico de datos en busca de contenido malicioso, bloquear archivos y sitios web malignos y mantener en cuarentena dispositivos infectados.
- Firewall: La implementación de un firewall dentro del sistema de seguridad de una red puede ser utilizada para bloquear dispositivos no autorizados que intenten establecer una conexión, prevenir el acceso indebido a recursos, proteger a usuarios de ataques maliciosos, entre otras utilidades.

Considerar los métodos y herramientas recién mencionadas, es una técnica efectiva de aumentar el nivel de seguridad preventiva dentro de una red, por lo que se considera altamente recomendable de aplicar.

Identificación de *hosts* activos

La información obtenida en la primera fase, facilita el siguiente paso, la identificación de *hosts* activos dentro de la red.

Consiste en el proceso de descubrir distintos dispositivos conectados a la red, con el fin de analizarlos y verificar si se encuentran correctamente protegidos.

Existen diversos métodos para realizar descubrimiento de *hosts*. Uno de los métodos más comunes, corresponde al uso de herramientas de scan de redes, por ejemplo la herramienta de código abierto *Nmap*. Estas, envían paquetes de datos a posibles dispositivos presentes en la red y esperan por una respuesta. Dichas respuestas pueden ser utilizadas para identificar dispositivos conectados, sus direcciones IP, sistema operativo, etc.

El proceso de identificación de *hosts* activos, se puede dividir en los siguientes pasos a seguir:

1. Definir rango de scan: En este caso, corresponde al uso de la información sobre la segmentación que se obtuvo en la fase anterior. De esta forma, los escaneos que se realicen pueden enfocarse en segmentos específicos. También, es posible evaluar el uso de algunas técnicas exhaustivas para los segmentos restringidos (en caso de existir).
2. Envío de paquetes: Las herramientas de scan permiten el envío de diversos paquetes de datos, los cuales pueden ser de diferentes tipos como ICMP, UDP o TCP.
3. Esperar respuesta: Una vez que los paquetes de datos han sido enviados, se necesita esperar por una respuesta a estos. Estas últimas permiten identificar dispositivos conectados en la red.
4. Análisis de resultados: Al momento de tener las respuestas, es necesario analizarlas para identificar los *hosts* activos. Lo cual puede realizarse mediante la inspección de las direcciones IP, sistemas operativos y cualquier otra información que entregue la respuesta.

La aplicación de esta fase es de gran importancia al momento de continuar, ya que permite enfocar los tests de las siguientes etapas exclusivamente a los dispositivos identificados y no al segmento completo, optimizando el análisis en general.

Análisis de vulnerabilidades

Corresponde al proceso sistemático de identificar potenciales vulnerabilidades de seguridad en una red. Uno de los métodos más utilizados, es el uso de herramientas de escaneo de

vulnerabilidades, las cuales abarcan una amplia gama de vulnerabilidades a analizar, como configuraciones incorrectas, o software desactualizado que podría presentar vulnerabilidades conocidas. Dentro de las herramientas más utilizadas que cuentan con esta funcionalidad se encuentran *Nessus* y *OpenVas*.

El funcionamiento de una herramienta de scan de vulnerabilidades suele consistir en algunos pasos generales:

1. Descubrimiento: El scan en primer lugar envía paquetes al *host* objetivo y analiza las respuestas recibidas, esto con el fin de descubrir *hosts* activos. Este paso no es obligatorio, ya que existe la opción de entregar manualmente una lista de *hosts* objetivo que se asuman activos para los pasos siguientes.
2. Enumeración: La herramienta aplica técnicas de enumeración de servicios activos para cada *host* activo, es decir, envía solicitudes a posibles servicios presentes y luego analiza las respuestas obtenidas.
3. Evaluación de vulnerabilidades: Corresponde a evaluar las vulnerabilidades de cada servicio detectado, para lo cual se compara la configuración de este con una base de datos de vulnerabilidades conocidas.
4. Reporte: Aplicaciones de tipo scan de vulnerabilidades recopilan las respuestas obtenidas durante el análisis para posteriormente emitir un reporte donde se presente cada una de estas. Dichos reportes incluyen la vulnerabilidad, su severidad y en algunos casos opciones de mitigación.

Una desventaja de las herramientas de escaneo de vulnerabilidades, es la presencia de falsos positivos, es decir, reportes de vulnerabilidades que no están presentes realmente. Sin embargo, estas herramientas se consideran como un aporte, ya que permiten obtener una noción del estado de seguridad en el cual se encuentra la red, con la cual un establecimiento puede desarrollar un plan de acción para que su red cumpla con los estándares que se definan.

Adicionalmente, herramientas de este tipo, suelen acompañar las vulnerabilidades encontradas con posibles mitigaciones, lo que permite que algunas vulnerabilidades sean fácil y rápidamente solucionadas.

Evaluación de políticas de seguridad

Una vez obtenidos los resultados del análisis de vulnerabilidades y la evaluación de configuraciones y protección existente, es necesario chequear si el estado de la seguridad de la red cumple con los requisitos estipulados en las políticas de seguridad del establecimiento.

El caso particular de los establecimientos de educación, es que suelen utilizar redes con acceso bastante abierto, es decir, que los usuarios en la red suelen tener visibilidad a la mayoría de los dispositivos presentes en esta. Esto debido a la posible necesidad de interconectar servicios de forma simple.

Lo anterior, podría implicar que algunas posibles vulnerabilidades identificadas en la etapa anterior, no se interpreten como tal, ya que para efectos del establecimiento, la red cumpliría con un comportamiento esperado.

Además, los establecimientos como Campus o facultades, también suelen estar regidos por las normas de la Universidad o Instituto del cual son parte. Por lo que también es importante la revisión del cumplimiento de las normativas a esa escala.

Por otra parte, en caso de no poseer políticas de seguridad, ninguna vulnerabilidad encontrada se considerará dentro de un comportamiento esperado de la red. Por consiguiente, la severidad de las vulnerabilidades se cuantificará como tal.

4.1.4. Análisis de Resultados

En cuanto al análisis de resultados, este se divide en pasos. En primer lugar, se evalúan en cuanto a la recopilación de configuraciones y protección existente. Esto implica el chequeo del uso de las herramientas y técnicas de seguridad mencionadas en la subsección. "Evaluación de configuraciones y protección existentes", la cuales abarcan una lista de factores que conllevan a una buena práctica de seguridad preventiva y que son altamente recomendables para proteger una red en cualquier contexto.

En segundo lugar, se evalúa el análisis de vulnerabilidades ejecutado previamente, con el objetivo de contextualizar las vulnerabilidades detectadas al contexto educacional en el cual fueron detectadas. Esta etapa del análisis se enfoca en dar a entender que el puntaje CVSS de cada vulnerabilidad detectada se enfoca en un contexto universal, el cual carece del enfoque particular que se busca en el presente trabajo de memoria. Lo recién mencionado es debido a que el puntaje CVSS está diseñado para capturar la severidad de una vulnerabilidad y no el riesgo asociado a ella. Por lo cual es necesario analizarlas en el contexto que corresponde para evitar una priorización incorrecta de cada una al momento de definir un plan de acción para su mitigación.

Por ejemplo, en una tienda en línea, se asigna un puntaje CVSS de 6,5 a una vulnerabilidad que expone los números de tarjetas de crédito de los clientes a cada usuario que inicie sesión en el portal. Por otra parte, un puntaje de 10 se le asigna a un hallazgo de ejecución remota de código (RCE) no autenticado dentro de un servidor interno de control de calidad que no está conectado a Internet. Ambos hallazgos deben corregirse, pero la puntuación por sí sola implica que la vulnerabilidad RCE debería tener prioridad, cuando en realidad es la primera vulnerabilidad mencionada la que tendría el mayor impacto en caso de ser explotada [9].

Por casos como el mencionado anteriormente, es que se debe considerar el puntaje CVSS como una referencia, pero no como un factor definitivo al momento de priorizar mitigaciones en el plan de acción. La evaluación de vulnerabilidades no se considera dentro del alcance de este trabajo de memoria, ya que implica una mirada subjetiva del equipo encargado de la red y su análisis de políticas de seguridad en caso de existir.

Finalmente, se agrega el resultado de la evaluación de políticas de seguridad también realizado previamente y se concluye con un análisis general del conjunto de resultados el cual

se espera contribuya para el diseño de las acciones a tomar para proteger la red en la cual se trabaja la presente metodología.

Interpretación de resultados

Con el fin de entender más claramente el significado de los resultados obtenidos, se intentaron diversas ideas para interpretarlos, las cuales no tuvieron éxito debido a razones relacionadas al alcance del trabajo de título o a su dificultad como tal.

En particular, por el alcance y duración de la presente memoria, no es posible medir el riesgo de las vulnerabilidades encontradas por lo mencionado anteriormente relacionado a "la mirada subjetiva del equipo encargado de la red y su análisis de políticas de seguridad en caso de existir". Sin esta información no es posible categorizar las vulnerabilidades de la forma necesaria para concretar las siguientes ideas:

- Semáforo: Se pensó en reflejar el estado general de la seguridad de la red como un semáforo, asignando una luz verde, amarilla, o roja en caso de que el estado de la seguridad se considerara seguro, medianamente seguro o inseguro. El estado sería definido dependiendo de los resultados de la evaluación de configuraciones y protección existente, el resultado de análisis de vulnerabilidades y la evaluación de políticas de seguridad. No fue posible concretar debido a la falta de categorización por riesgo de las vulnerabilidades encontradas durante el análisis de vulnerabilidades.
- Gráfico vulnerabilidades por prioridad: Surgió la idea de ilustrar de forma gráfica las vulnerabilidades encontradas asignándoles una prioridad, la cual serviría de guía para definir qué vulnerabilidades mitigar en primer lugar. No fue posible concretar debido a la falta de categorización por riesgo de las vulnerabilidades encontradas durante el análisis de vulnerabilidades, la cual estaría directamente relacionada con la prioridad a asignar.
- Definir gravedad de vulnerabilidades encontradas relacionando cantidad de *hosts* encontrados y cantidad de vulnerabilidades encontradas: Se plantea la idea de obtener la proporción de vulnerabilidades encontradas sobre la cantidad de *hosts* activos descubiertos, mas se concluye que no es posible debido a que un *host* puede presentar múltiples vulnerabilidades. Por ejemplo, dentro de una red con 100 *hosts* activos descubiertos se encuentran 50 vulnerabilidades críticas (máxima severidad). Esto no significa que la mitad de la red se encuentre afectada críticamente, esto también podría corresponder a un *host* el cual presente las 50 vulnerabilidades. Por lo tanto, esta proporción no necesariamente reflejaría de forma correcta el estado de la seguridad de la red.

Por otra parte, también se busca asignar un valor numérico o "nota" al resultado de la evaluación de configuraciones y protección existente, sin embargo, no fue posible ya que definir la cantidad de puntos que se deben cumplir para considerarse una red en un estado preventivo "bueno", corresponde a un análisis subjetivo fuera del alcance del presente trabajo. Por lo cual, se decide que un resultado positivo es cuando se apunta a cumplir la mayoría de los puntos propuestos en esa sección.

Finalmente, se concluye que el análisis de resultados busca entregar algunos resultados de la forma más clara posible, sin establecer una escala o métrica, mas sí busca entregar recomendaciones y algunas conclusiones parciales las cuales se consideran un aporte para el futuro trabajo que se sugiere realizar con el fin de completar la evaluación de la seguridad de la red en cuestión.

Capítulo 5

Validación

En el caso de la presente memoria, la validación de la solución planteada consiste en una aplicación de la metodología dentro de una red inalámbrica perteneciente a la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile. Esto con el fin de realizar una prueba de la metodología planteada.

A continuación, se desarrollan las etapas que constituyen la metodología dentro del contexto de prueba que se mencionó anteriormente.

5.1. Aplicación de la metodología

5.1.1. Antes de comenzar

Como paso previo de la simulación, se coordina una reunión con el equipo de redes encargado de la red a analizar, con el fin de solicitar las autorizaciones y credenciales correspondientes (en caso de ser necesario).

5.1.2. Análisis Pasivo

Recopilación de información

Para el desarrollo de la recopilación de información, se aprovecha la instancia de reunión mencionada en la subsección anterior para consultar por la información necesaria para el comienzo del análisis.

Dentro de la información recopilada, se resumen la más relevante a continuación:

- Topología de red: Corresponde a una red conformada por una gran cantidad de dispositivos de red, que busca una conexión simple entre dispositivos, con el fin de mantener

una interconectividad sencilla y directa. Esto ya que, según se explica en la reunión, la Facultad tiene la necesidad de mantener una serie de servicios dentro de la red, los cuales deben tener la capacidad de conectarse entre sí para una correcta funcionalidad dentro de esta.

- Dispositivos: Dentro de los dispositivos de red que se pueden encontrar se incluyen equipos clientes como computadores y teléfonos, y también *access points.*
- Segmentación: Con el fin de la ejecución del caso de prueba, se entregan tres segmentos relevantes dentro de la red. Sin embargo, se menciona la existencia de segmentos adicionales. Debido al tiempo que conllevan las pruebas para el desarrollo de la metodología, se decide trabajar en uno de los segmentos. Este se considera relevante ya que contempla un subsegmento restringido y la presencia de diversos dispositivos y servicios.
- Restricciones y políticas: Se comunica que dentro de los usuarios de la red inalámbrica no existen roles diferenciados, mas los administradores de la red sí poseen sus respectivas credenciales para el acceso a equipos y servicios que la manejan. Por otra parte, en cuanto a políticas a nivel de la universidad, se menciona que no existen políticas autorizadas por la Vicerrectoría de Tecnologías de la Información de la Universidad de Chile. Y en cuanto a nivel de la facultad, existe un reglamento de uso de la cuenta asociada a cada estudiante, mas no existen políticas de uso de la red.

5.1.3. Análisis Activo

Evaluación de configuraciones y protección existente

Esta etapa se desarrolla en conjunto con la recopilación de información, es decir, algunos puntos de la información obtenida que se menciona a continuación fueron obtenidos gracias a los datos consultados al equipo encargado de la red durante la reunión inicial.

En concreto, se obtienen los siguientes resultados:

- Cifrado: En cuanto al cifrado de la red, se logra identificar la presencia de este. Para lo anterior, se utiliza la herramienta gratuita de análisis de tráfico de red *Wireshark* con el fin de interceptar un paquete de datos que transite en la red y analizar su contenido. Dentro del paquete capturado se identifica un campo relacionado al tipo de cifrado que se utiliza, confirmando la presencia de este. Además, al momento de establecer una conexión con la red, es posible identificar su cifrado dentro de la configuración de esta, la cual es visible en la ventana de ajustes de red del computador utilizado para el análisis.

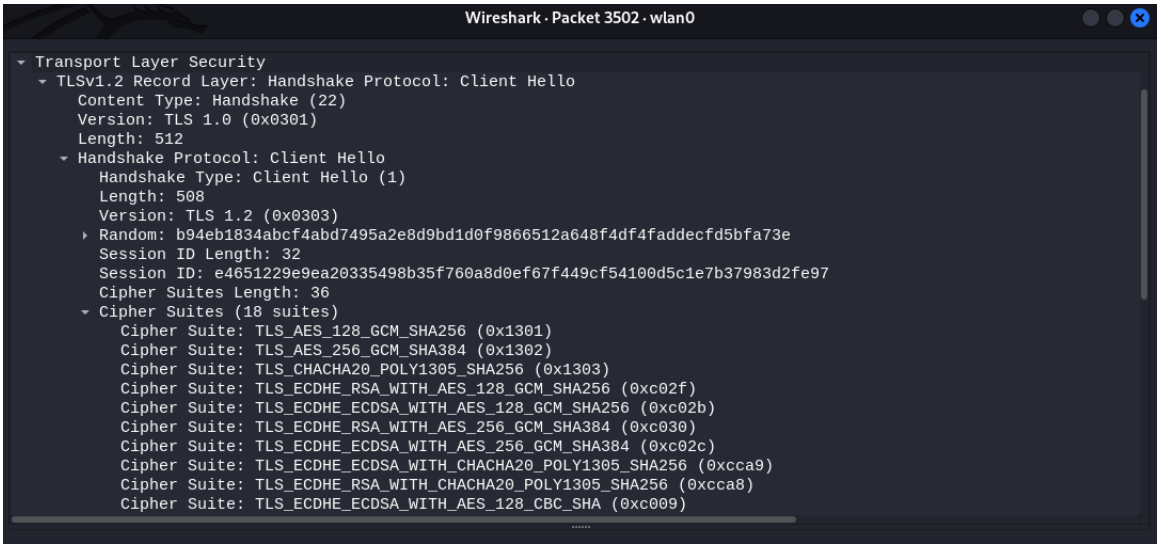


Figura 5.1: Información sobre cifrado utilizado dentro de paquete capturado.

- Autenticación: Se identifica la presencia de un sistema de autenticación en la red, ya que al momento de establecer la conexión, se solicitan credenciales para hacer uso de esta. Este sistema también se puede visualizar dentro de la ventana de ajustes de red del computador.
- Firmware actualizado: Según lo informado por el equipo encargado de la red, los routers adhieren a políticas de actualización de firmware permanente.
- Cifrado obsoleto: Al igual que lo que se menciona en el punto referente al cifrado, es posible analizar un paquete de datos en la red e identificar qué cifrado se utiliza. En el caso de la red analizada, se identifica el protocolo de seguridad WPA2, el cual se considera medianamente seguro ya que corresponde a uno de los últimos protocolos universalmente implementados. Sin embargo, en caso de que los routers presentes sean compatibles, se recomienda el uso del protocolo WPA3, ya que este incluye correcciones a las brechas de seguridad que presenta WPA2.

Figura 5.2: Información sobre tipo de cifrado en configuración de la red.

- Antivirus: Se informa que solo existe la presencia de antivirus dentro de equipos clientes y que no existe política que obligue a mantener activo dicho software.
- Firewall: Según la información recibida, existen firewalls a nivel de enlace hacia Internet. Sin embargo, aún no existen firewalls en la red interna.

Identificación de *hosts* activos

El proceso de identificación de *hosts* activos, se desarrolla utilizando la herramienta de código *Nmap*, ya que se destaca por su rendimiento y funcionalidades.

En pocas palabras, *Nmap* utiliza diversas técnicas de bajo nivel, como lo son el envío y recepción de paquetes de red a posibles dispositivos en la red a analizar. En caso de recibir respuesta, *Nmap* registra dicha respuesta y se considera como un indicador de que un *host* o dispositivo está activo.

Dentro del portal de *Nmap*, se encuentra una recopilación de las mejores combinaciones de opciones presentes en esta herramienta para el descubrimiento de *hosts* [11]. Las cuales se mencionan junto al porcentaje de efectividad en la siguiente tabla:

N°	Efectividad	Comandos utilizados
1	62.47 %	-PE
2	77.61 %	-PE -PA80
3	83.83 %	-PE -PA80 -PS443
4	88.64 %	-PE -PA80 -PS443 -PP
5	91.12 %	-PE -PA80 -PS443 -PP -PU40125 –source-port 53
6	92.42 %	-PE -PS80 -PS443 -PP -PU40125 -PA3389 –source-port 53
7	93.10 %	-PE -PS80 -PS443 -PP -PU40125 -PS3389 -PA21 –source-port 53
8	93.69 %	-PE -PS80 -PS443 -PP -PU40125 -PS3389 -PA21 -PU161 –source-port 53

Tabla 5.1: Mejores combinaciones para descubrimiento de *hosts*

Luego de algunas pruebas dentro de la red local, se seleccionan algunas de las mejores técnicas planteadas anteriormente, pero también agregando un scan de tipo ping, el cual identifica *hosts* activos sin realizar un escaneo exhaustivo de todos los puertos y servicios en cada *host*.

Los comandos a utilizar se resumen a continuación:

N°	Comando
1	sudo nmap -sn -v
2	sudo nmap -sn -PE -PA80 -PS443 -PP -PU40125 –source-port 53 -v
3	sudo nmap -sn -PE -PS80,443 -PP -PU40125 -PA3389 –source-port 53 -v
4	sudo nmap -sn -PE -PS80,443,3389 -PP -PU40125 -PA21 –source-port 53 -v
5	sudo nmap -sn -PE -PS80,443,3389 -PP -PU40125,161 -PA21 –source-port 53 -v

Tabla 5.2: Comandos seleccionados.

Al momento de ejecutar los comandos seleccionados, se agrega la opción de guardar el resultado del scan en un archivo de texto, con la opción "$-oN$ [*nombrearchivo*].*txt*" con el fin de realizar un análisis posterior de los resultados.

Una vez obtenidos los resultados, se limpian los archivos obtenidos y se resumen en uno. Este contiene la lista de direcciones IP obtenidas luego de ejecutar todos los comandos.

Para facilitar la limpieza de los resultados se programa el código *listandclean* [A.1], el cual se encarga de limpiar, filtrar y ordenar las direcciones IP obtenidas.

Por otra parte, en caso de existir un segmento restringido dentro de la red, es altamente recomendable chequear si las direcciones que lo componen se encuentran dentro de los resultados de los scans que se realicen, ya que existe la posibilidad de que se espere que estas direcciones no sean fácilmente identificables. En el caso de la red de prueba, ninguna dirección IP del subsegmento restringido es identificada, lo cual corresponde al comportamiento esperado.

El segmento analizado se define con una máscara de 16 bits, es decir, consta de 65536 posibles direcciones IP. De las cuales se logran identificar 1520 *hosts* activos luego de la

ejecución del proceso de descubrimiento de estos.

Con la información obtenida en esta etapa, es posible focalizar el próximo análisis de vulnerabilidades exclusivamente a las direcciones recopiladas, reduciendo así el tiempo de ejecución de este considerablemente.

Análisis de vulnerabilidades

Para la ejecución del análisis de vulnerabilidades, se utiliza la herramienta *OpenVas*, ya que corresponde a la herramienta gratuita más utilizada y recomendada. Esta herramienta contiene la funcionalidad de ejecutar análisis de vulnerabilidades, identificándolas junto a su puntaje de severidad CVSS (Common Vulnerability Scoring System), solución (que en la mayoría de los casos corresponde a una mitigación), técnica de detección utilizada, entre otras características.

En primer lugar, se define el objetivo a escanear, configurando sus respectivos *hosts*, los puertos a analizar y posibles credenciales para algunos servicios.

En el caso del análisis ejecutado, el objetivo se define utilizando la lista de *hosts* activos obtenida en la etapa anterior. Además, se establecen los puertos a analizar como todos los puertos TCP y los 100 principales recomendados por *Nmap* y no se agregan credenciales adicionales de servicios:

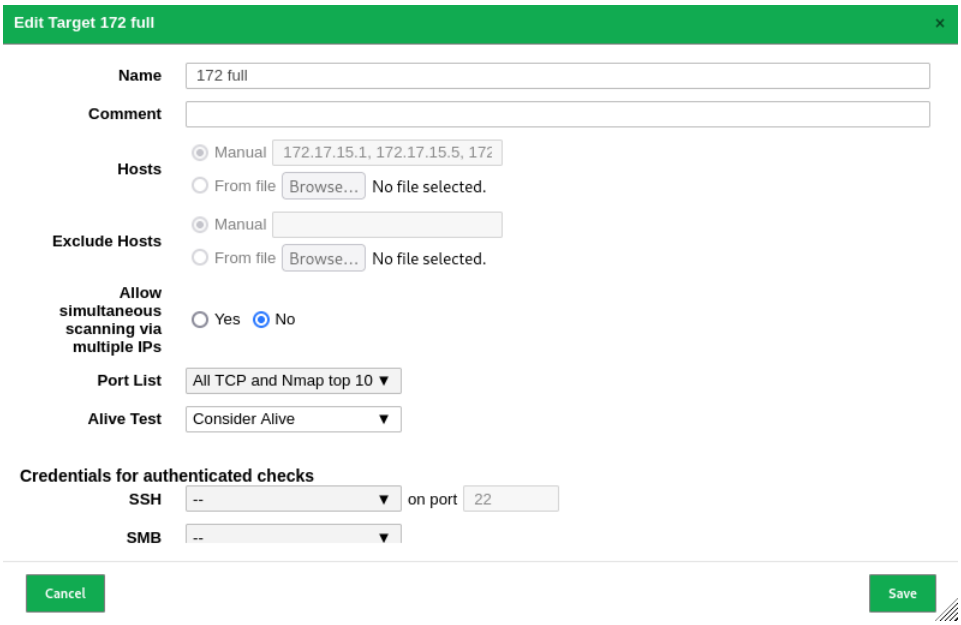


Figura 5.3: Configuración de objetivo dentro de software *OpenVas*

Luego, se define la tarea que ejecutará el scan. En donde es posible establecer el objetivo, agendar repeticiones del scan, tipo de scan, entre otros factores.

Para este caso, se establece el objetivo definido previamente y sin repeticiones. También, se define el tipo de scan como *"Full and fast"*, el cual en primer lugar ejecuta un scan de puertos y

sus servicios, para luego chequear la presencia de vulnerabilidades asociadas a dichos servicios. En el portal de la herramienta se menciona que las vulnerabilidades analizadas durante el proceso, corresponden exclusivamente a las cuales no dañarían el sistema del objetivo [7]. Esto cumple con lo solicitado por el equipo encargado de la red, por lo que se considera factible llevarlo a cabo.

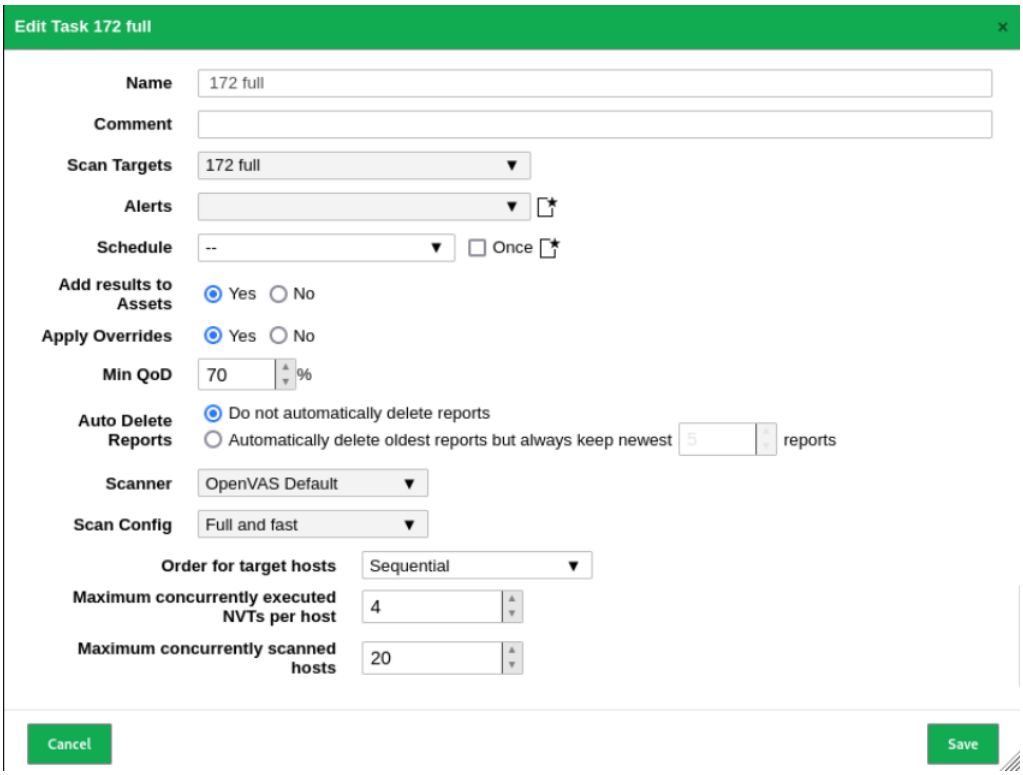


Figura 5.4: Configuración de tarea dentro de software *OpenVas*

Con la tarea definida, se procede a ejecutar el scan. Este demora 4 días en finalizar, obteniendo un total de 2895 vulnerabilidades asociadas a 758 *hosts* diferentes.

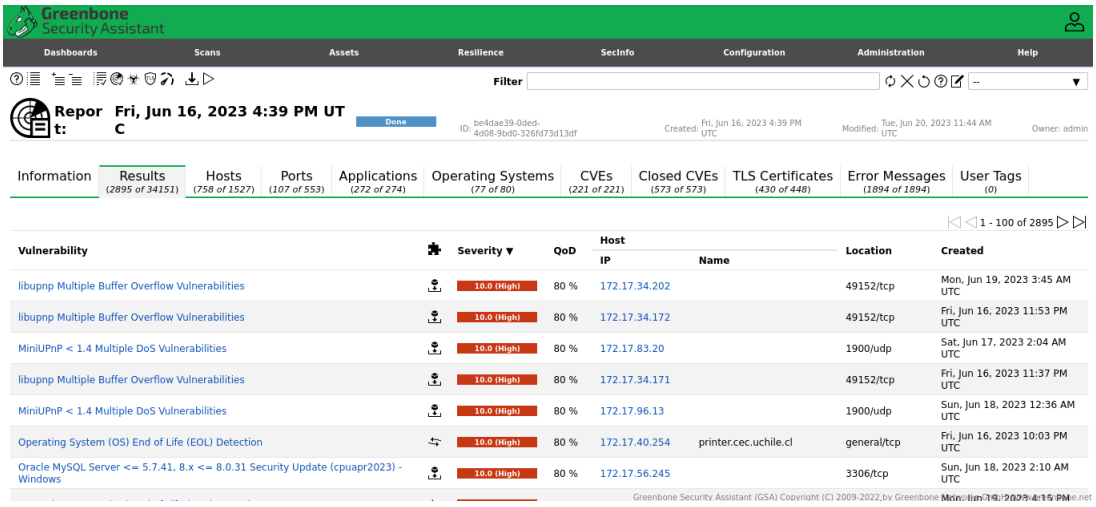
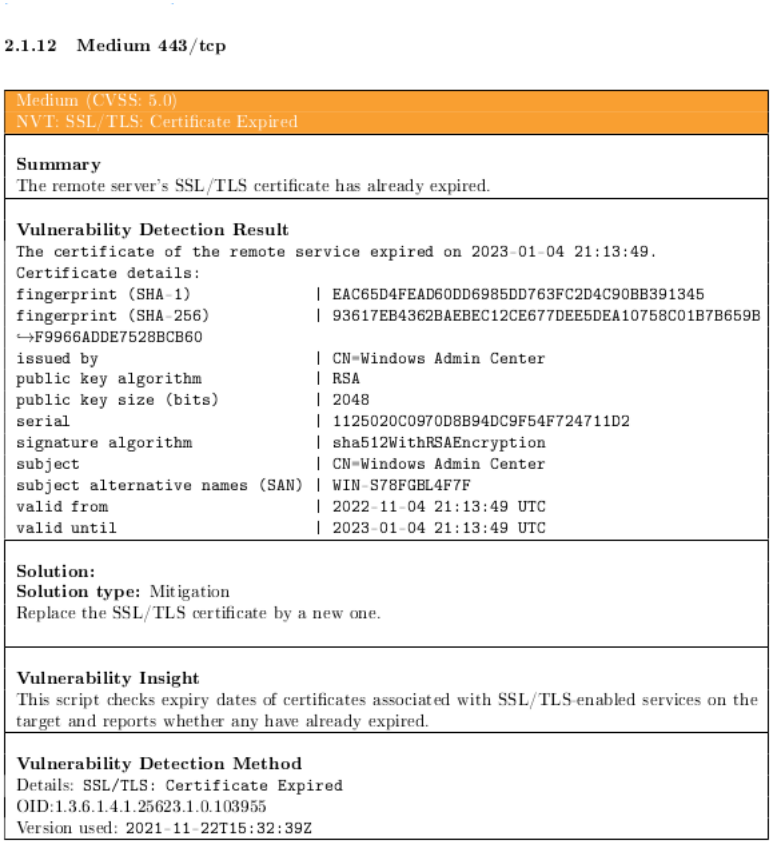


Figura 5.5: Página principal de reporte con resultados.

Finalmente, es posible generar un reporte con la información obtenida, el cuál será utilizado en el posterior análisis de resultados y además se envía al equipo encargado con el fin de mantenerlos en conocimiento de las vulnerabilidades identificadas.



2.1.12 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result
The certificate of the remote service expired on 2023-01-04 21:13:49.
Certificate details:

fingerprint (SHA-1)	EAC65D4FEAD60DD6985DD763FC2D4C90BB391345
fingerprint (SHA-256)	93617EB4362BAEBEC12CE677DEE5DEA10758C01B7B659B ↪F9966ADDE7528BCB60
issued by	CN=Windows Admin Center
public key algorithm	RSA
public key size (bits)	2048
serial	1125020C0970D8B94DC9F54F724711D2
signature algorithm	sha512WithRSAEncryption
subject	CN=Windows Admin Center
subject alternative names (SAN)	WIN-S78FGBL4F7F
valid from	2022-11-04 21:13:49 UTC
valid until	2023-01-04 21:13:49 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2021-11-22T15:32:39Z

Figura 5.6: Formato de vulnerabilidad detectada.

Evaluación de políticas de seguridad

En cuanto a políticas de seguridad, debido a la falta de estas, se considera que ninguna vulnerabilidad identificada corresponde a un comportamiento esperado dentro de la red, ya que de ser así, esto debería estar oficialmente declarado en un reglamento.

Por otra forma, no es posible evaluar si la red cumple con los requisitos de la Facultad y Universidad, debido a que dichos requisitos no se encuentran estipulados oficialmente.

5.1.4. Análisis de Resultados

En primer lugar, con respecto a configuraciones y protección existente:

1. Cifrado: Presente.
2. Autenticación: Presente.

3. Firware actualizado: Presente.
4. Cifrado no-obsoleto: Presente, con posibilidad de mejora.
5. Antivirus: Parcialmente presente, con posibilidad de mejora en caso de existir política que lo solicite.
6. Firewall: Parcialmente presente, con posibilidad de mejora.

En cuanto a los factores mencionados, se aprecian resultados positivos, ya que se cumplen en su mayoría. Se recomienda mejorar los puntos con posibilidad de mejora y evaluar una extensión de cobertura en cuanto a los puntos parcialmente presentes.

Por otra parte, en lo que a análisis de vulnerabilidades respecta, se identificaron 359 vulnerabilidades de severidad alta, 1508 de severidad media y 1028 de severidad baja, lo que se puede apreciar gráficamente en el gráfico a continuación.

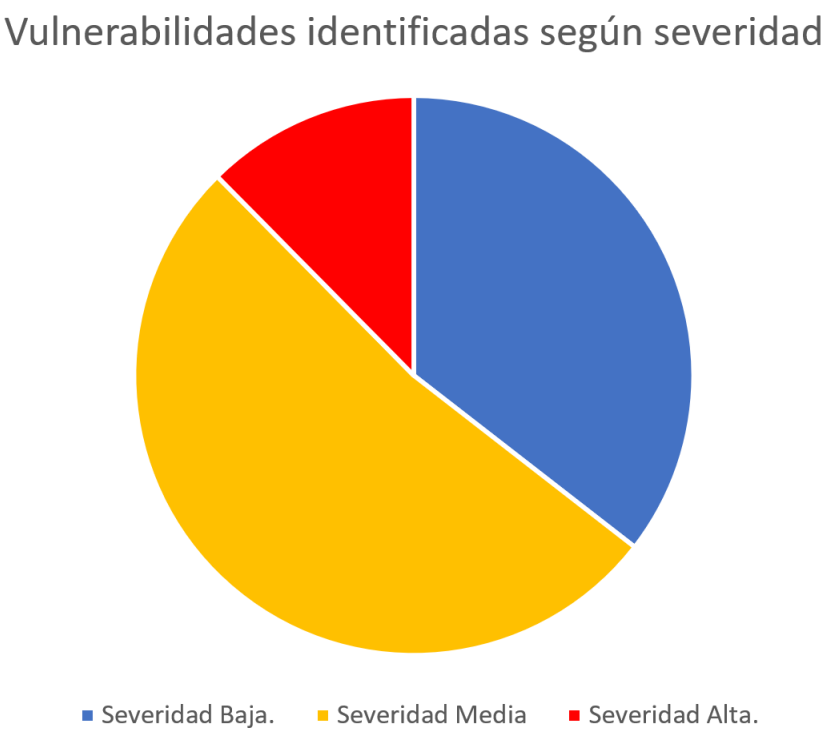


Figura 5.7: Vulnerabilidades identificadas según severidad.

A partir del reporte emitido por el software utilizado (en este caso, *OpenVas*), es posible analizar cada vulnerabilidad detectada, donde se sugiere abarcarlas desde mayor a menor severidad, con el fin de evaluarlas en el contexto educacional en el que se encuentran y asignarles una prioridad según posible impacto. Tarea la cual no contempla el presente trabajo de título, ya que la importancia que tiene cada posible impacto debe definirse por el equipo encargado de la red y las políticas de la red en caso de existir. Con el objetivo de que este paso pueda ser realizado para su consideración en un posible plan de acción a futuro, el reporte obtenido durante el análisis fue enviado a la brevedad al equipo encargado de la red.

En tercer lugar, como se mencionó en la sección anterior, no existe política de seguridad establecida. Esto conlleva una ambigüedad riesgosa en cuánto a qué comportamiento está contemplado dentro de lo esperado en la red y qué comportamiento refleja un falla en la seguridad de esta. Además, en el caso de que un atacante intentara ejecutar un ataque a la red, no sería posible aplicar la ley de delito informático. Tampoco queda definida la posibilidad de aplicar sanción alguna.

Finalmente, a modo resumen del análisis de resultados, la red analizada contiene una positiva (pero mejorable) protección existente preventiva. Sin embargo, se sugiere fuertemente realizar la evaluación de riesgo por vulnerabilidad encontrada relativa al análisis de vulnerabilidades realizado, utilizando el reporte de vulnerabilidades encontradas, el cual fue entregado al equipo encargado correspondiente. Ya que, si bien no fue posible realizar el mencionado análisis en el presente trabajo, el número de vulnerabilidades detectadas de severidad alta y media no son despreciables y se recomienda que sean consideradas lo antes posible. Y como último punto, se recomienda definir y establecer una política de seguridad, tanto a nivel Facultad como Universidad. esto permitiría una correcta evaluación de posibles brechas de seguridad en el sistema y la aplicación de la correspondiente sanción a un posible atacante.

Capítulo 6

Conclusión

El objetivo general de este trabajo corresponde a proponer una metodología para evaluar la seguridad informática perimetral de unidades académicas (facultades o similares) dentro de establecimientos de educación superior. Con el fin de que esta sirva como una herramienta que permita identificar de forma sencilla, una visión del estado de la seguridad de la red del establecimiento. Lo cual permita al equipo encargado de esta, desarrollar un plan de acción de mejora y su sistema de seguridad existente y también, asista en la identificación de vulnerabilidades con el objetivo de ser mitigadas lo antes posible.

La solución se enfocó en una metodología compuesta por 3 etapas principales: análisis pasivo, análisis activo y análisis de resultados. La cual logra parcialmente los objetivos que se proponen.

En primer lugar, se cumple con la investigación de posibles estrategias, herramientas y técnicas para realizar los distintos análisis, ya la solución contempla recursos que en su gran mayoría no habían sido puestos en práctica por la estudiante.

También, se logra aplicar parcialmente las estrategias planteadas dentro del establecimiento educacional que se define como escenario de prueba al momento de ejecutar la simulación de aplicación de la metodología. Esto se realiza dentro de un rol de usuario con acceso a la red. Se considera un cumplimiento parcial de este objetivo, debido a la dificultad de interpretación de resultados que se mencionó anteriormente, lo cual no permitió realizar en su completitud el análisis de vulnerabilidades deseado.

Dentro del proceso de análisis activo de la metodología se identifica un proceso de concientización en conjunto al equipo encargado de la red, planteando la importancia de las estrategias utilizadas y su posterior análisis de resultados, lo cual se complementa cumpliendo con el objetivo de exploración de alternativas de validación de la solución, ejecutando así una simulación exitosa.

Se considera que el resultado del trabajo es satisfactorio, pues implica un gran aprendizaje para la estudiante y se considera una herramienta expansible y mejorable que puede significar un aporte para el acercamiento de la ciberseguridad dentro del contexto educacional.

Por otra parte, durante el desarrollo de la solución fue posible identificar la escasa in-

formación de seguridad informática enfocada en establecimientos superior, lo cual podría implicar una rama de investigación a desarrollar a futuro. Además, el trabajo en conjunto con el equipo encargado significó un aprendizaje para la estudiante, pues corresponde al desarrollo de trabajo en equipo dentro de un grupo de personas establecido previamente y significó un desafío en cuanto a exposición de visiones y creencias relacionadas a la ciberseguridad y su manejo en el establecimiento, permitiendo así la aparición de nuevas interrogantes y planteamientos que no se habían presentado previamente.

Dentro de las lecciones aprendidas, se comprende de mejor forma el significado de la colaboración y trabajo en equipo indirecto, conciencia sobre la duración de un concreto análisis de redes y su dificultad al implicar distintas entidades que de igual forma utilizan la red analizada. Además, el presente trabajo de título significó un aporte en cuanto a enfrentar nuevos desafíos y superar las dificultades que se presentaron en su desarrollo. Se considera como una experiencia que brinda un positivo desarrollo como futura profesional a la estudiante.

A partir de esta memoria, se identifican posibles mejoras e ideas complementarias, como lo son las mencionadas a continuación:

- Agregar la opción de obtener credenciales de acceso a la red mediante un *access point* falso, con el fin de simular un ataque real y analizar su respuesta por parte de la red.
- Realizar los análisis sin utilizar credenciales, obteniendo así la visión de un atacante externo.
- Desarrollo de un producto que analice políticas de uso y las relacione con las vulnerabilidades detectadas, facilitando así un mejor entendimiento de qué respuestas por parte de la red constituyen un comportamiento esperado de esta.
- Desarrollo de herramienta que analice las vulnerabilidades encontradas durante el análisis y modifique su puntaje CVSS de acuerdo al contexto educacional en el que se encuentra.
- Trabajo a largo plazo que implique la medición de riesgo asociado a vulnerabilidades encontradas en el contexto particular que representan los establecimientos de educación superior. Por ejemplo, se sugiere un estudio de largo plazo que correlaccione y/o contraste los ataques documentados a varias instituciones educacionales, su nivel de compromiso y severidad, con los datos recolectados en las fases de análisis pasivo y activo de la metodología propuesta en el presente trabajo. Tal estudio podría dar pie a una validación de la metodología empleada, así como la elaboración de variantes más precisas de ésta. Podría corresponder a una línea de investigación interesante.

Bibliografía

[1] Francisco Alessandri. Comparación gasto público por nivel educativo. *acciónEducar*, 2021.

[2] Elena Canorea. Qué es el pentesting — procesos y metodologías. In *https://www.plainconcepts.com/es/pentesting/*, 2021.

[3] Gerald Combs. Wireshark. In *https://www.wireshark.org/download.html*, 2006.

[4] Consejo Consultivo Nacional de Infraestructuras de EE.UU. (NIAC). Commor vulnerability scoring system (cvss). In *https://www.first.org/cvss/specification-document*, 2003.

[5] Renaud Deraison. Nessus. In *https://www.tenable.com/products/nessus*, 1998.

[6] Noelia García. Ciberseguridad: Las universidades son las terceras instituciones más atacadas. *El Economista*, 2019.

[7] Greenbone Networks GMBH. Scanning a system. In *https://docs.greenbone.net/GSM-Manual/gos-22.04/en/scanning.html*.

[8] Greenbone Networks GMBH. Openvas. In *https://openvas.org/*, 2006.

[9] Antti Tuomi Lari Lehtomäki Jason Johnson, Weiming Theh. Keeping score: hhow to get the most from cvss. In *https://www.withsecure.com/en/expertise/resources/keeping-score-how-to-get-the-most-from-cvss*, 2021.

[10] Jisc. Cyber impact 2022. In *The impact of cyber security incidents on the UK's further and higher education and research sectors*, 2022.

[11] Nmap Software LLC. Putting it all together: Host discovery strategies. In *https://nmap.org/book/host-discovery-strategies.html*.

[12] Gordon Lyon. Nmap. In *https://nmap.org/*, 1997.

[13] Andrés Peñailillo. Ciberseguridad en instituciones de educación. *trendTIC*, 23:32, 2019.

[14] Matías Vega. Universidad santo tomás sufre ataque informático y suspende actividades virtuales. *BioBio Chile*, 2020.

[15] Parlamento Europeo y Consejo de la Unión Europea. Reglamento general de protección de datos de la unión europea (gdpr). In *https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu*$_e$*s*, 2016.

Anexo

Listing A.1: Código python encargado de limpiar y ordenar resultados de scans *Nmap* y resumirlos en archivo único.

```
import re, os, ipaddress

# Este c digo debe ser ejecutado con permisos de root

# Crea archivos _list y _clean en base a archivos existentes
# de distintos scans
def crear_list_y_clean(archivos_names):

    for archivo in archivos_names:

        archivo_txt = "./Original/"+archivo+".txt"



        with open(archivo_txt, "r") as f:
            content = f.read()

        # Busca y reemplaza en el texto
        content_new = re.sub(r".*\[host down\]\n", r"", content)
        content_new1 = re.sub(r"Host is up.*\n", r"", content_new)
        content_new2 = re.sub(r"Increasing .*\n", r"", content_new1)
        content_new3 = re.sub(r"adjust_timeout.*\n", r"", content_new2)
        content_new4 = re.sub(r"Nmap scan report for ", r"", content_new3)

        # Ruta y nombre del archivo de salida de
        ruta_list = './List/'+ archivo +'_list.txt'

        # Verificar si la ruta existe, si no, crearla
        directorio_salida = os.path.dirname(ruta_list)
        if not os.path.exists(directorio_salida):
```

```
                os.makedirs(directorio_salida)

        #Escribe archivo de direcciones ip listas junto con
        # algunos dominios encontrados
        with open(ruta_list, "w") as f:
            f.write(content_new4)

        content_new5 = re.sub(r"^# Nmap.*\n", r"", content_new4)
        content_new6 = re.sub(r".*seconds", r"", content_new5)
        content_new7 = re.sub(r".* \(", r"", content_new6)
        content_new8 = re.sub(r"\).*", r"", content_new7)
        content_new9 = re.sub(r".*decreasing.*\n", r"", content_new8)
        cleans = re.sub(r'\s$', r"",content_new9)

        # Ruta y nombre del archivo de salida de
        ruta_clean = './Clean/'+ archivo +'_clean.txt'

        # Verificar si la ruta existe, si no, crearla
        directorio_salida2 = os.path.dirname(ruta_clean)
        if not os.path.exists(directorio_salida2):
                os.makedirs(directorio_salida2)

        # Escribe archivo que contiene exclusivamente
        # las direcciones ip encontradas
        with open(ruta_clean, "w") as f:
                f.write(cleans)

# Lee archivos de carpeta Clean
def leer_archivos(archivos):
    contenido = []
    for archivo in archivos:
        txt = "./Clean/"+archivo
        with open(txt, 'r') as f:
                contenido.extend(f.readlines())
    return contenido

# Elimina l neas repetidas en formato de direcci n ip
def eliminar_lineas_repetidas(contenido):
    contenido_sin_repetir = list(set(contenido))
    sin_jumps = [sub.replace('\n', '') for sub in contenido_sin_repetir]
    sin_jumps.sort()
    aux=sorted(sin_jumps, key = ipaddress.IPv4Address)
    contenido_final = [i + "\n" for i in aux]
    return contenido_final

# Escribe contenido (por fila) en un archivo
def escribir_archivo(contenido, nombre_archivo):
```

```
    with open(nombre_archivo, 'w') as f:
        f.writelines(contenido)

# Une archivos clean en uno general, sin repetir ips repetidas
def merge_clean(archivos_txt,input_name):

        # Leer los archivos y agrupar el contenido
        contenido = leer_archivos(archivos_txt)

        # Eliminar l neas repetidas
        contenido_sin_repetir = eliminar_lineas_repetidas(contenido)

        # Ruta y nombre del archivo de salida
        ruta_salida = './'+ input_name +'_clean.txt'

        # Verificar si la ruta existe, si no, crearla
        directorio_salida = os.path.dirname(ruta_salida)
        if not os.path.exists(directorio_salida):
            os.makedirs(directorio_salida)

        # Escribir el contenido sin l neas repetidas
    # en el archivo de salida
        escribir_archivo(contenido_sin_repetir, ruta_salida)

# Lista de archivos a leer
input_name = '172'
aux = ["_sn", "_pro5", "_pro6", "_pro7", "_pro8"]
archivos_names = []
archivos_clean_txt = []
for a in aux:
    archivos_names.append(input_name+a)
    archivos_clean_txt.append(input_name+a+"_clean.txt")


# Crea archivos list y clean en sus respectivas carpetas
crear_list_y_clean(archivos_names)

# Crea un archivo  nico  que resume todos los hosts
# activos encontrados con las distintas t cnicas
merge_clean(archivos_clean_txt, input_name)
```