ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN COMPAÑÍA INTERNACIONAL DE INTEGRACIÓN CI2

YESID ANDRES TORRES PIRE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2024

ETHICAL HACKING COMPAÑÍA INTERNACIONAL DE INTEGRACIÓN CI2

YESID ANDRES TORRES PIRE

Proyecto de grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Ing. Joel Carroll Vargas P.hD(c)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

DEDICATORIA

A mis hijos, mi esposa, mi familia, amigos y todas las personas que siempre han estado ahí para darme guía y consejo en cada uno de los procesos y etapas que a lo largo de mi vida me han acompañado y basado en su consejo, accionar, palabra, o muestra de amor, me han dado el insumo para seguir adelante con este proyecto de ser mejor cada día.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo y guía nos permiten ser mejores, a mi familia un agradecimiento especial por la paciencia, pero sobre todo por la fuerza que sobre mi infunden.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Pentesting: Penetración basada en pruebas con el objetivo de determinar vulnerabilidades

Reconocimiento pasivo: Fase donde se realizan procesos y métodos para obtención de información

Reconocimiento activo: también conocido como fingerprinting, es el proceso de interacción con el objetivo para obtención de información directa.

Escaneo de vulnerabilidades: Proceso de análisis de puntos débiles de un sistema a partir de metodologías o software.

Explotación: Fase de explotación de las vulnerabilidades detectadas mediante el uso de herramientas y códigos ya sean de desarrollo propios o públicos.

Vulnerabilidad: Debilidad o punto débil de un sistema de software que puede ser explotado por un atacante.

Payload: Se define como el proceso posterior al explotar una vulnerabilidad, buscando dar las entradas o accesos a códigos o inyecciones de ataque.

Write-Up: Informe el cual describe el proceso ejecutado por el atacante para posterior aprendizaje.

CTF: Pruebas o competiciones basados en ejercicios de hacking buscando el incremento de conocimiento.

Boot2root: Equipo preconfigurado con vulnerabilidades técnicas con el objetivo de mejorar el aprendizaje del atacante.

RESUMEN

Dentro de los modelos de infraestructura tecnológica actuales, se observan sistemas híbridos que combinan entornos On-Premise con la Nube, junto con sistemas físicos de última generación. Esto implica una constante necesidad de actualización, especialmente en entornos de producción aún no totalmente explorados.

Además de los sistemas físicos híbridos, se están implementando soluciones de aplicaciones mixtas, donde un solo sistema no se limita a una única estación de presentación, sino que se distribuye en múltiples modelos de aplicabilidad. Esto puede conllevar riesgos compartidos según los diferentes modelos de trabajo.

Es importante destacar que los desarrollos tecnológicos puestos en producción, así como los requerimientos técnicos de infraestructura, generalmente no incluyen evaluaciones actualizadas de capas de seguridad. Dado que las industrias de tecnología están en constante evolución, junto con las vulnerabilidades y riesgos emergentes, es crucial mantener actualizadas estas evaluaciones de seguridad.

Con el fin de abordar estas problemáticas, se debe determinar el nivel de riesgo de la compañía internacional de integración CI2 en sus sistemas productivos, con el fin de brindar un plan de remediación logrando un aseguramiento de su infraestructura tecnológica.

ABSTRACT

Within current technological infrastructure models, hybrid systems are observed that combine On-Premise environments with the Cloud, alongside state-of-the-art physical systems. This entails a constant need for updates, especially in production environments that are not yet fully explored.

In addition to hybrid physical systems, mixed application solutions are being implemented, where a single system is not limited to a single presentation station but is distributed across multiple applicability models. This can entail shared risks according to different working models.

It is important to note that technological developments put into production, as well as technical infrastructure requirements, generally do not include updated security layer evaluations. Given that technology industries are constantly evolving, alongside emerging vulnerabilities and risks, it is crucial to keep these security assessments updated.

In order to address these issues, it is necessary to determine the risk level of the international integration company CI2 in its productive systems, in order to provide a remediation plan achieving assurance of its technological infrastructure.

INTRODUCCIÓN

La compañía internacional de integración CI2 se dedica a proporcionar servicios de integración tecnológica en áreas como seguridad física y perimetral, movilidad, Oil & gas, y procesos de investigación, desarrollo e innovación. La infraestructura de servicios de comunicaciones, que incluye servidores, plataformas y software, es fundamental para respaldar la entrega de estos servicios. Dado el enfoque gubernamental de muchos de sus contratos y la naturaleza crítica de los servicios ofrecidos, la compañía se enfrenta a amenazas constantes en un entorno cada vez más sofisticado de ciberdelincuencia.

La seguridad de la información y la protección cibernética son áreas de estudio críticas y en constante evolución, especialmente para empresas que prestan servicios tecnológicos sensibles a sectores gubernamentales. La integración de tecnologías en entornos críticos como seguridad física, movilidad y sectores de energía implica desafíos únicos en términos de protección de datos, resiliencia operativa y gestión de riesgos. En este contexto, el análisis y la mitigación de amenazas cibernéticas se vuelven esenciales para garantizar la continuidad del negocio y la protección de la información confidencial.

A pesar de la importancia estratégica de la infraestructura de servicios de comunicaciones de CI2 y la sensibilidad de los servicios que ofrece, existe una falta de evaluaciones actualizadas de seguridad y un enfoque integral para identificar y abordar las vulnerabilidades. Esto expone a la compañía a un alto riesgo de ataques cibernéticos, incluidos los dirigidos específicamente a sectores gubernamentales. La ausencia de evaluaciones adecuadas de capas de seguridad puede poner en peligro la integridad de los datos, la confidencialidad de la información y la reputación de la compañía.

El problema de la seguridad cibernética en entornos críticos como el de CI2 es de gran relevancia debido a las implicaciones potenciales de un compromiso de seguridad en los servicios prestados y la confianza del cliente. La protección contra amenazas cibernéticas es fundamental para mantener la competitividad y la operatividad de la compañía, especialmente frente a los crecientes desafíos de ciberseguridad en el contexto actual. Este trabajo contribuye al campo de estudio al proporcionar un enfoque estructurado y detallado para identificar, analizar, y mitigar amenazas cibernéticas en servicios críticos de integración tecnológica.

Este trabajo se centrará en el proceso de análisis, identificación, explotación y recomendaciones de remediación de amenazas para los servicios core de CI2. Se abordarán vulnerabilidades específicas en la infraestructura de servicios de comunicaciones utilizada para respaldar la prestación de servicios de integración tecnológica. Las recomendaciones de remediación estarán diseñadas para mejorar

la seguridad y la resiliencia operativa de la compañía frente a amenazas cibernéticas.

Se reconoce que este trabajo puede tener limitaciones en términos de alcance geográfico, tecnologías específicas cubiertas y acceso a información sensible de la compañía. Además, las recomendaciones de remediación propuestas pueden no abordar todas las posibles vulnerabilidades o escenarios de amenazas. La implementación efectiva de las recomendaciones requerirá coordinación y recursos adicionales por parte de CI2.

La ejecución de pruebas de ingeniería no solo proporcionará una evaluación crítica de la resiliencia del personal frente a las amenazas cibernéticas, sino que también servirá como punto de partida para iniciativas de concientización en seguridad. La capacitación del personal en la identificación y respuesta adecuada a los ataques de ingeniería social es fundamental para fortalecer la postura general de seguridad de CI2.

El análisis detallado de los sistemas productivos de la compañía permitirá una comprensión profunda de las vulnerabilidades existentes y sus posibles impactos en la prestación de servicios críticos. Esta identificación temprana de vulnerabilidades proporcionará a CI2 la oportunidad de implementar medidas proactivas para mitigar riesgos y fortalecer las defensas contra posibles amenazas.

La evaluación exhaustiva del nivel de exposición de los sistemas en producción proporcionará información esencial sobre las áreas de mayor riesgo y las vulnerabilidades más críticas que podrían ser explotadas. Esto permitirá a CI2 priorizar sus esfuerzos de seguridad y asignar recursos de manera eficiente para abordar las vulnerabilidades identificadas.

El desarrollo de un plan integral de recomendaciones de remediación garantizará que CI2 cuente con una hoja de ruta clara y efectiva para mejorar su postura de seguridad. Este plan será fundamental para la implementación de medidas correctivas necesarias y la mejora continua de las defensas cibernéticas de la compañía, contribuyendo así al campo de estudio de la seguridad de la información y la protección cibernética en entornos empresariales críticos como el de CI2.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La historia del "ethical hacking" o "hacking ético" se remonta a las primeras décadas de la historia de la informática. El término "hacker" originalmente se utilizaba para describir a personas apasionadas por la tecnología y la programación, que tenían habilidades técnicas avanzadas y eran capaces de explorar y comprender sistemas informáticos en profundidad.

En los años 60 y 70, los primeros hackers exploraban y descubrían vulnerabilidades en los sistemas informáticos con fines educativos y de aprendizaje. Muchos de ellos eran estudiantes universitarios y entusiastas de la tecnología que se dedicaban a la experimentación y la exploración de sistemas informáticos, sin intenciones maliciosas.

Sin embargo, a medida que la tecnología de la información se volvió más ampliamente utilizada en la década de 1980, también surgieron actividades de hacking con fines maliciosos, como robo de información, fraude, sabotaje y otros actos ilegales. Esto llevó a un aumento en la conciencia sobre la seguridad informática y a la necesidad de proteger los sistemas y datos de posibles amenazas.

A medida que la tecnología de la información se volvió más ampliamente utilizada en la década de 1980, también surgieron actividades de hacking con fines maliciosos, como robo de información, fraude, sabotaje y otros actos ilegales. Este período vio la proliferación de virus informáticos y el surgimiento de figuras icónicas en el ámbito del hacking malicioso, como Kevin Mitnick, quien se hizo famoso por sus intrusiones en sistemas informáticos de alto perfil.

Durante las décadas de 1960 y 1970, los primeros hackers se dedicaban a la exploración y al aprendizaje, motivados por una profunda curiosidad y una pasión por la tecnología. Sin embargo, con el tiempo, el acceso y el conocimiento de sistemas informáticos avanzados empezaron a atraer a individuos con intenciones menos nobles. La transición hacia el hacking malicioso comenzó a tomar forma cuando ciertos individuos se dieron cuenta del potencial de sus habilidades para obtener beneficios personales o causar daño.

En los años 80, la tecnología informática se expandió rápidamente, y con ella, surgieron las primeras manifestaciones de hacking malicioso. Figuras como Kevin Mitnick se convirtieron en íconos del hacking criminal, llevando a cabo intrusiones en sistemas gubernamentales y corporativos. Mitnick, en particular, fue famoso por su habilidad para eludir la seguridad informática y acceder a información confidencial, lo que generó un gran revuelo mediático y un interés creciente en la

ciberseguridad. Estos primeros hackers maliciosos demostraron que los sistemas informáticos, aunque avanzados, eran vulnerables a las intrusiones.

La década de 1980 también vio la creación y difusión de los primeros virus informáticos. Programas como el "Brain Virus", creado en 1986 por dos hermanos paquistaníes, marcó el inicio de la era del malware. Este virus infectaba el sector de arranque de los disquetes y se propagaba de una computadora a otra. La aparición de estos programas maliciosos hizo evidente que las intenciones detrás del hacking habían cambiado, y que las nuevas amenazas podían causar daños significativos tanto a individuos como a organizaciones.

A medida que el hacking malicioso se expandía, también lo hacían las motivaciones y las técnicas empleadas por los atacantes. Algunos buscaban notoriedad y reconocimiento en la comunidad hacker, mientras que otros estaban motivados por ganancias financieras, espionaje corporativo o incluso terrorismo cibernético. Las técnicas empleadas se volvieron más sofisticadas, incluyendo la explotación de vulnerabilidades de día cero, la ingeniería social para manipular a los usuarios y el desarrollo de rootkits y troyanos para mantener acceso persistente a los sistemas comprometidos.

El impacto del hacking malicioso fue significativo y multifacético. Empresas y gobiernos comenzaron a enfrentar pérdidas financieras y de reputación debido a los ataques cibernéticos. En respuesta, la industria de la ciberseguridad empezó a desarrollarse de manera más formal, con la creación de nuevas tecnologías y prácticas para defenderse de estas amenazas. Las agencias gubernamentales también empezaron a establecer leyes y regulaciones más estrictas para perseguir y castigar a los hackers maliciosos. Este período marcó un punto de inflexión, donde la ciberseguridad pasó de ser un campo de interés académico a convertirse en una prioridad crítica para la protección de la infraestructura digital global.

En respuesta a este aumento de actividades de hacking malintencionado, algunos hackers con habilidades técnicas avanzadas comenzaron a utilizar sus conocimientos para ayudar a proteger los sistemas informáticos en lugar de atacarlos. Estos hackers éticos, también conocidos como "hackers éticos" o "expertos en seguridad", comenzaron a emplear sus habilidades para identificar vulnerabilidades en sistemas y redes, y trabajar en estrecha colaboración con los propietarios de los sistemas para corregir las debilidades antes de que fueran explotadas por hackers malintencionados.

El término "ethical hacking" o "hacking ético" comenzó a utilizarse en la década de 1990 para describir esta práctica de utilizar habilidades de hacking con fines legales y éticos, con el objetivo de proteger los sistemas y datos de las organizaciones. Con el tiempo, el hacking ético se ha convertido en una práctica reconocida y aceptada en la industria de la seguridad informática, con profesionales especializados que realizan pruebas de penetración, auditorías de seguridad y otras actividades para

identificar y corregir vulnerabilidades en sistemas y redes, con el consentimiento y la autorización de los propietarios de los sistemas.

El nacimiento del hacking ético se produjo como respuesta directa al aumento de las actividades de hacking malicioso durante la década de 1980. Con la proliferación de ataques informáticos y la creciente dependencia de la tecnología digital, las organizaciones comenzaron a darse cuenta de la necesidad de proteger sus sistemas de información. La seguridad informática pasó a ser una prioridad, y la industria buscó maneras de anticipar y mitigar las amenazas antes de que causaran daño significativo. Este contexto preparó el terreno para que los hackers con conocimientos avanzados en tecnología comenzaran a utilizar sus habilidades de manera constructiva y legal.

Algunos de los primeros hackers que inicialmente estaban involucrados en actividades de exploración y aprendizaje comenzaron a ver el valor en utilizar sus habilidades para el bien. Esta transición no siempre fue fácil, ya que muchos enfrentaban la percepción negativa asociada con el término "hacker". Sin embargo, al enfocarse en la protección de sistemas y datos, estos individuos comenzaron a establecerse como consultores de seguridad. Utilizando sus conocimientos para identificar vulnerabilidades y trabajar con las organizaciones para corregirlas, sentaron las bases del hacking ético.

La formalización del hacking ético se produjo a través de la creación de programas y certificaciones que establecían estándares y prácticas éticas para los profesionales de seguridad. Uno de los hitos más significativos en este proceso fue la creación de la certificación de Ethical Hacker Certificado (Certified Ethical Hacker - CEH) por el Consejo Internacional de Consultores de Comercio Electrónico (EC-Council) en 2003. Esta certificación proporcionó un marco formal para la formación y evaluación de hackers éticos, asegurando que los profesionales no solo tuvieran habilidades técnicas, sino también un compromiso con la ética y la legalidad.

Los hackers éticos comenzaron a desarrollar y utilizar una variedad de herramientas y técnicas para llevar a cabo su trabajo de manera efectiva. Estas herramientas, que incluyen escáneres de vulnerabilidades como Nessus, frameworks de pruebas de penetración como Metasploit, y herramientas de análisis de seguridad como OWASP ZAP, permitieron a los hackers éticos realizar evaluaciones exhaustivas de la seguridad de los sistemas. Además, técnicas como la ingeniería social, el phishing ético y el análisis forense digital se volvieron fundamentales en la identificación y mitigación de riesgos de seguridad.

Con el tiempo, el hacking ético ganó aceptación y reconocimiento en la industria de la seguridad informática. Las organizaciones comenzaron a ver el valor en contratar hackers éticos para realizar pruebas de penetración, auditorías de seguridad y otras evaluaciones proactivas de sus sistemas. Este cambio de perspectiva permitió a los hackers éticos desempeñar un papel crucial en la defensa contra ciberataques. La

colaboración entre hackers éticos y organizaciones contribuyó a la creación de prácticas de seguridad más robustas y efectivas, fortaleciendo la protección de la infraestructura digital global.

Los escáneres de vulnerabilidades son herramientas esenciales en el arsenal de un hacker ético. Estas herramientas automatizadas permiten a los profesionales de seguridad identificar debilidades en sistemas y aplicaciones de manera eficiente. Ejemplos destacados incluyen Nessus y OpenVAS. Nessus, desarrollado por Tenable Network Security, es conocido por su capacidad de realizar escaneos profundos y generar informes detallados sobre las vulnerabilidades detectadas. OpenVAS, un proyecto de código abierto, ofrece funcionalidades similares y es altamente valorado por su flexibilidad y capacidad de personalización. Estas herramientas ayudan a los hackers éticos a identificar puntos débiles antes de que puedan ser explotados por atacantes maliciosos.

Los frameworks de pruebas de penetración, como Metasploit, son fundamentales para realizar pruebas más intrusivas y detalladas en sistemas y redes. Metasploit, desarrollado originalmente por H.D. Moore y ahora mantenido por Rapid7, permite a los hackers éticos simular ataques reales para evaluar la seguridad de un entorno. Este framework incluye una amplia gama de exploits y payloads que pueden ser utilizados para comprometer sistemas de prueba. Al emplear Metasploit, los hackers éticos pueden demostrar cómo un atacante podría explotar vulnerabilidades específicas y proporcionar recomendaciones precisas para mitigarlas.

Herramientas de análisis de seguridad como OWASP ZAP (Zed Attack Proxy) son cruciales para la evaluación de la seguridad de aplicaciones web. OWASP ZAP es un proyecto de código abierto patrocinado por la Open Web Application Security Project (OWASP), y se utiliza ampliamente para identificar vulnerabilidades comunes en aplicaciones web, como inyecciones SQL, cross-site scripting (XSS) y problemas de configuración de seguridad. La herramienta permite a los hackers éticos realizar escaneos automatizados y pruebas manuales, proporcionando una visión integral de la seguridad de una aplicación web y ayudando a los desarrolladores a corregir las debilidades identificadas.

La ingeniería social es una técnica que explota la psicología humana para obtener acceso no autorizado a sistemas o información. Los hackers éticos utilizan la ingeniería social para evaluar la capacidad de una organización para resistir ataques que manipulan el comportamiento humano. El phishing ético es una forma específica de ingeniería social donde los hackers éticos envían correos electrónicos falsos diseñados para engañar a los empleados y obtener credenciales de acceso. Estas pruebas ayudan a las organizaciones a identificar vulnerabilidades en sus procedimientos de seguridad y a educar a sus empleados sobre las tácticas utilizadas por los atacantes.

El análisis forense digital es una técnica utilizada por los hackers éticos para investigar incidentes de seguridad y rastrear la actividad de los atacantes. Esta técnica implica la recopilación y el análisis de datos de sistemas comprometidos para comprender cómo ocurrió una intrusión y qué acciones se llevaron a cabo. Herramientas como EnCase y FTK (Forensic Toolkit) son ampliamente utilizadas en el análisis forense digital. Estas herramientas permiten a los hackers éticos extraer evidencia digital, reconstruir eventos de ataque y proporcionar informes detallados que pueden ser utilizados en investigaciones legales y para mejorar las medidas de seguridad.

El hacking ético se ha convertido en una disciplina indispensable en el campo de la ciberseguridad, proporcionando a las organizaciones una defensa proactiva contra las amenazas digitales. A través del uso de herramientas avanzadas como escáneres de vulnerabilidades, frameworks de pruebas de penetración y técnicas de ingeniería social, los hackers éticos pueden identificar y mitigar riesgos antes de que los atacantes maliciosos puedan explotarlos. Este enfoque no solo fortalece la seguridad de la infraestructura digital, sino que también fomenta una cultura de conciencia y resiliencia en seguridad dentro de las organizaciones.

En última instancia, el hacking ético no solo se trata de proteger sistemas y datos, sino también de construir un entorno digital más seguro y confiable. A medida que las amenazas continúan evolucionando, la colaboración entre hackers éticos, empresas y gobiernos será crucial para desarrollar nuevas estrategias y tecnologías de seguridad. Al mantener un compromiso firme con la ética y la legalidad, los hackers éticos desempeñan un papel vital en la protección de nuestra información y en la creación de un futuro digital más seguro.

Hoy en día, es considerado una parte importante de la estrategia de seguridad de la información de muchas organizaciones, ya que ayuda a identificar y corregir debilidades en los sistemas antes de que sean explotadas por hackers malintencionados, contribuyendo así a fortalecer la seguridad de la información y proteger la integridad, confidencialidad y disponibilidad de los activos de información.

1.2 FORMULACIÓN DEL PROBLEMA

En un entorno de seguridad de la información generalmente se centra en identificar y abordar los desafíos y riesgos asociados con la protección de la información confidencial y sensible en sistemas informáticos y redes. En este contexto podrían incluir:

Amenazas y vulnerabilidades: Identificar las amenazas potenciales y las vulnerabilidades en los sistemas de información, como malware, phishing, ataques

de fuerza bruta, brechas de seguridad, entre otros, y entender cómo pueden ser mitigadas o prevenidas.

Cumplimiento normativo y legal: Cumplir con las regulaciones y leyes aplicables relacionadas con la seguridad de la información, como lo es la política de protección de datos y otras regulaciones específicas.

Gestión de accesos: Administrar y controlar los accesos a sistemas y redes para garantizar que solo las personas autorizadas tengan acceso a la información y recursos pertinentes, y prevenir accesos no autorizados.

Protección de datos: Proteger la confidencialidad, integridad y disponibilidad de la información almacenada y transmitida, incluyendo la encriptación de datos, copias de seguridad, y políticas de retención de datos.

Concientización y entrenamiento: Aumentar la conciencia y el entrenamiento en seguridad de la información entre los empleados y usuarios, para fomentar buenas prácticas de seguridad y reducir el riesgo de incidentes causados por errores humanos.

Gestión de incidentes: Establecer procesos y procedimientos para la identificación, gestión y respuesta a incidentes de seguridad de la información, incluyendo la detección temprana, la contención y la recuperación de incidentes de seguridad.

Con lo anterior se plantea, ¿Cuál es el nivel de riesgo y exposición en el que se encuentra la Compañía internacional de integración Ci2?.

JUSTIFICACIÓN

En el contexto de la seguridad de la información, es crucial identificar y mitigar los desafíos y riesgos asociados con la protección de datos confidenciales en sistemas informáticos y redes. Esto implica enfrentar amenazas como malware, phishing, ataques de fuerza bruta y brechas de seguridad, asegurando la comprensión y aplicación de medidas preventivas efectivas. Así mismo, el cumplimiento normativo y legal juega un papel fundamental, exigiendo el cumplimiento de políticas de protección de datos y otras regulaciones aplicables.

Una parte esencial de este proceso implica gestionar adecuadamente los accesos a sistemas y redes para garantizar la autorización adecuada y prevenir accesos no autorizados. Además, se debe enfocar en proteger la confidencialidad, integridad y disponibilidad de la información mediante prácticas de encriptación, copias de seguridad y políticas de retención de datos bien definidas. Para reducir riesgos, es necesario aumentar la conciencia y el entrenamiento en seguridad de la información entre empleados y usuarios, promoviendo buenas prácticas y minimizando errores humanos.

La implementación de procedimientos efectivos de gestión de incidentes es esencial para identificar, gestionar y responder de manera oportuna a cualquier incidente de seguridad que pueda surgir. Esto incluye la detección temprana, la contención adecuada y la recuperación eficiente de la seguridad comprometida. En última instancia, este enfoque integral busca determinar el nivel de riesgo y exposición al que se enfrenta una organización como la Compañía Internacional de Integración Ci2, permitiendo la formulación de estrategias de seguridad más efectivas y orientadas a la protección de la información crítica.

La seguridad de la información implica un enfoque holístico para abordar amenazas y vulnerabilidades, cumplir con normativas legales, gestionar accesos de manera segura, proteger datos sensibles y promover la conciencia en seguridad. La gestión proactiva de incidentes es clave para responder eficazmente a cualquier eventualidad. Este marco es esencial para evaluar y mitigar el nivel de riesgo y exposición en entornos empresariales como el de Ci2, facilitando la implementación de medidas de seguridad efectivas y adaptadas a las necesidades específicas de la organización.

OBJETIVOS

1.3 OBJETIVOS GENERAL

Determinar el nivel de riesgo de la compañía internacional de integración CI2 en sus sistemas productivos, con el fin de brindar un plan de remediación logrando un aseguramiento de su infraestructura tecnológica.

1.4 OBJETIVOS ESPECÍFICOS

Ejecutar pruebas de ingeniería social y phishing a una muestra de personal de la compañía.

Identificar las vulnerabilidades existentes de acuerdo con análisis en los sistemas productivos.

Evaluar el nivel de exposición de los sistemas en producción con diferentes pruebas y herramientas de penetración

Generar plan de recomendaciones de remediación de acuerdo con los distintos tipos de vulnerabilidades encontradas.

MARCO REFERENCIAL

1.5 MARCO TEÓRICO

El proceso de identificación de vulnerabilidades cibernéticas puede implicar varias etapas, y las bases principales pueden variar dependiendo del enfoque específico que se utilice. Sin embargo, en general, algunas de las bases principales en un proceso típico de identificación de vulnerabilidades cibernéticas incluyen:

Escaneo de vulnerabilidades donde se utilizan herramientas automatizadas de escaneo de seguridad para buscar activamente vulnerabilidades conocidas en sistemas, aplicaciones o redes. Estas herramientas pueden realizar escaneos de puertos, escaneos de servicios, identificación de versiones de software y comparación con bases de datos de vulnerabilidades conocidas.

En los análisis de configuraciones se espera revisar las configuraciones de sistemas y aplicaciones en busca de configuraciones incorrectas o inseguras que puedan ser explotadas por atacantes. Esto puede incluir la revisión de permisos, configuraciones de cortafuegos, configuraciones de seguridad en bases de datos y otros ajustes de configuración, en cuanto a la revisión de código fuente se espera Analizar el código fuente de aplicaciones en busca de posibles vulnerabilidades de seguridad. Esto puede implicar la revisión manual del código o el uso de herramientas automatizadas de análisis estático de código.

Las pruebas de penetración, también conocidas como "penetration testing" o "ethical hacking", busca simular ataques reales y descubrir vulnerabilidades en sistemas y aplicaciones. Esto puede implicar la utilización de técnicas avanzadas de hacking ético para identificar vulnerabilidades que no son detectadas por escáneres automatizados, se toma como insumo la Investigación de vulnerabilidades conocida con el objetivo de mantenerse informado acerca de las vulnerabilidades de seguridad conocidas que son divulgadas públicamente por proveedores de software, organizaciones de seguridad y la comunidad de seguridad en general. Esto puede implicar la consulta de bases de datos de vulnerabilidades, boletines de seguridad y foros de seguridad en línea.

Las auditorías de seguridad como objetivo principal es realizar auditorías periódicas para evaluar la postura de seguridad de sistemas, aplicaciones o redes en busca de posibles vulnerabilidades. Esto puede implicar la revisión de políticas de seguridad, procesos de seguridad y controles de seguridad implementados.

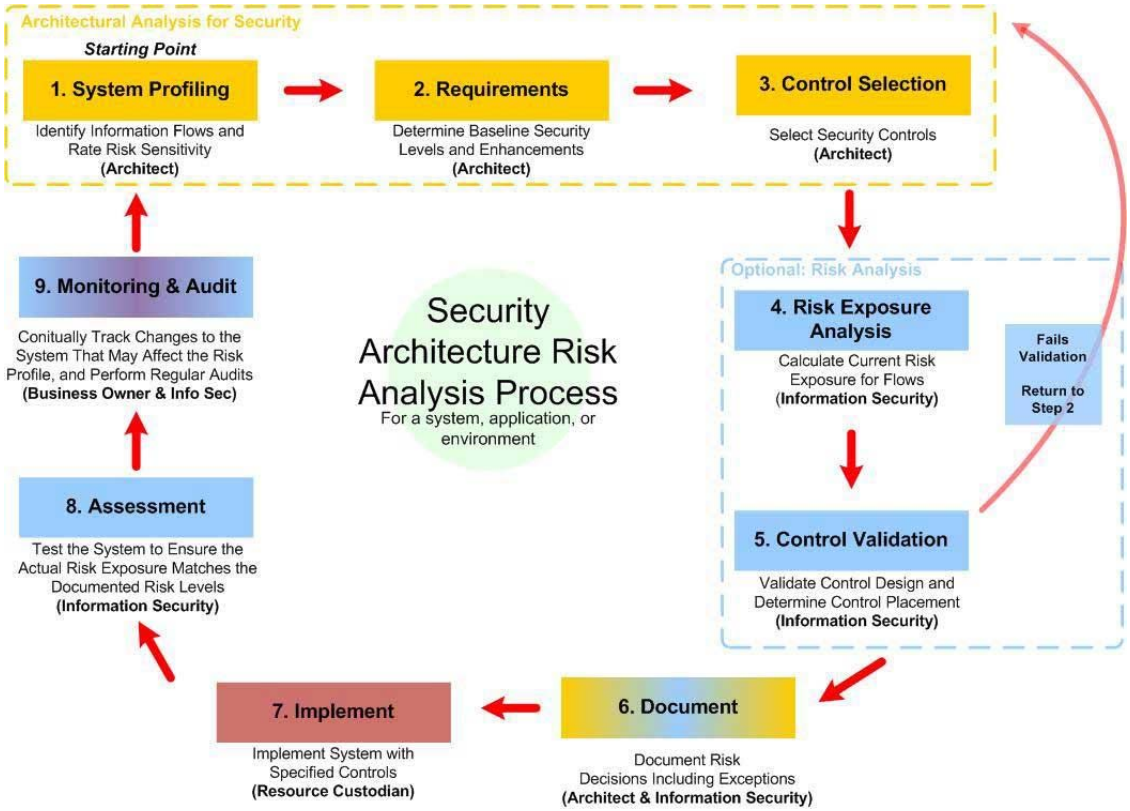
En las etapas de monitoreo de seguridad lo que se busca es Implementar soluciones de monitoreo de seguridad en tiempo real para detectar actividad sospechosa o indicadores de compromiso en sistemas y redes, lo que puede ayudar a identificar posibles vulnerabilidades o explotaciones en curso.

1.6 MARCO CONCEPTUAL

El ethical hacking es una práctica de seguridad de la información que implica la identificación y explotación de vulnerabilidades en sistemas, aplicaciones y redes de manera legal y ética, con el objetivo de encontrar y corregir posibles debilidades antes de que sean explotadas por personas malintencionadas.

Los objetivos del ethical hacking incluyen la identificación proactiva de vulnerabilidades, la evaluación de la seguridad de los sistemas, aplicaciones y redes, la protección de los activos de información, la prevención de posibles brechas de seguridad, y la mejora de las medidas de seguridad existentes y se realiza siempre con la debida autorización del propietario del sistema o aplicación que se va a evaluar. Esto implica obtener un permiso explícito y por escrito antes de llevar a cabo cualquier actividad de hacking ético.

Figura 1. Análisis de vulnerabilidades informáticas



Fuente: NOTICIAS DE SEGURIDAD INFORMÁTICA, TECNOLOGÍA. ¿Cómo hacer análisis de vulnerabilidades informáticas? [sitio web]. Bogotá; [Consultado: noviembre 2023]. Disponible en: https://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

El penetration testing, o pruebas de penetración, es una metodología utilizada por los ethical hackers para evaluar la seguridad de un sistema o aplicación mediante la simulación de ataques reales. Consiste en identificar y explotar vulnerabilidades conocidas y desconocidas con el objetivo de medir la resistencia del sistema y proponer mejoras en su seguridad.

Esta técnica sigue una metodología sistemática que incluye la recolección de información, la identificación de vulnerabilidades, la explotación de las mismas, el análisis de resultados y la presentación de informes detallados con las recomendaciones de seguridad correspondientes.

El hacker ético utiliza una variedad de herramientas y técnicas para identificar y explotar vulnerabilidades, como escáneres de seguridad, análisis de tráfico de red, pruebas de penetración, técnicas de ingeniería social, entre otros. Sin embargo, todas las herramientas y técnicas utilizadas deben cumplir con la legalidad y ética establecidas las cuales se rige por un código ético que incluye la integridad, confidencialidad, legalidad, respeto a la privacidad y cumplimiento de las leyes y regulaciones aplicables. Es fundamental que el hacker ético actúe de manera ética, respetando la privacidad de los sistemas y datos, y cumpliendo con todas las leyes y regulaciones pertinentes.

La identificación de vulnerabilidades es el proceso de buscar y descubrir posibles debilidades en sistemas, aplicaciones o redes que podrían ser explotadas por hackers malintencionados. Los ethical hackers utilizan herramientas de escaneo y pruebas de seguridad para identificar vulnerabilidades conocidas y desconocidas, así como analizar configuraciones incorrectas y deficiencias en la seguridad.

Una vez que se identifican vulnerabilidades, es importante elaborar un reporte detallado que describa las vulnerabilidades encontradas, su impacto potencial y las recomendaciones para su mitigación. El reporte debe ser claro, completo y proporcionar información técnica y no técnica comprensible para los diferentes interesados, incluyendo a los propietarios del sistema o aplicación. Dentro de los procesos de análisis se debe dar un reporte y recomendaciones presentando un informe detallado con los resultados de las pruebas de seguridad, incluyendo las vulnerabilidades identificadas, las explotadas y las recomendaciones correspondientes para corregir y mitigar los riesgos de seguridad, todo parte de las mejores prácticas de Seguridad donde el ethical hacking contribuye a mejorar las prácticas de seguridad de una organización, ya que identifica vulnerabilidades y debilidades que pueden ser corregidas para fortalecer la seguridad de los sistemas y aplicaciones.

El campo de la seguridad de la información está en constante evolución, por lo que el hacker ético debe mantenerse actualizado con las últimas tendencias, técnicas y herramientas de seguridad para poder realizar evaluaciones efectivas y proactivas.

El ethical hacking se rige por principios éticos y legales. Los ethical hackers deben obtener siempre el permiso por escrito del propietario del sistema o aplicación antes de llevar a cabo cualquier actividad de evaluación de seguridad. Además, deben seguir pautas éticas, como no causar daño a los sistemas, proteger la confidencialidad de la información obtenida y cumplir con las leyes y regulaciones aplicables.

El objetivo final del ethical hacking es mejorar la seguridad de los sistemas y aplicaciones evaluados. Los resultados obtenidos a través del proceso de identificación de vulnerabilidades y pruebas de penetración deben ser utilizados para implementar medidas de seguridad adecuadas, como parches de seguridad, configuraciones correctas, políticas de seguridad y concientización del personal, con el fin de fortalecer la seguridad de los sistemas y prevenir posibles ataques.

La seguridad de la información es un campo en constante evolución, por lo que es esencial que los ethical hackers se mantengan actualizados con las últimas vulnerabilidades, técnicas de ataque y herramientas de seguridad. La formación continua y la actualización constante de conocimientos y habilidades son fundamentales para realizar evaluaciones de seguridad efectivas y mantenerse al tanto de las últimas tendencias en ciberseguridad.

1.7 MARCO HISTÓRICO

El uso de herramientas y estrategias en la metodología del ethical hacking ha evolucionado a lo largo del tiempo, adaptándose a los avances tecnológicos y a las cambiantes amenazas de seguridad. A continuación, se presenta una breve historia de la evolución de las herramientas y estrategias utilizadas en el ethical hacking:

En la década de 1970-1980: Los orígenes del ethical hacking se encuentran en la década de 1970 y 1980, cuando los primeros hackers comenzaron a explorar y experimentar con sistemas informáticos con fines educativos y de investigación. En ese momento, las herramientas y estrategias utilizadas eran rudimentarias y se basaban en técnicas de ingeniería social, como el phreaking (manipulación de sistemas telefónicos) y el wardialing (marcar números de teléfono al azar para encontrar sistemas informáticos).

Posteriormente en la década de 1990, con el rápido crecimiento de Internet, surgieron nuevas oportunidades y desafíos en el campo del ethical hacking. Las herramientas y estrategias se volvieron más sofisticadas y se desarrollaron las primeras herramientas de escaneo de puertos y vulnerabilidades, como Nmap y SATAN. Los ethical hackers comenzaron a utilizar estas herramientas para identificar y explorar vulnerabilidades en sistemas y aplicaciones.

En la década de 2000; A medida que la tecnología avanzaba, también lo hacían las herramientas y estrategias utilizadas en el ethical hacking. Se desarrollaron herramientas de escaneo y pruebas de penetración más avanzadas, como Metasploit y Nessus, que ofrecían una mayor automatización y funcionalidad. Los ethical hackers también comenzaron a utilizar técnicas de análisis de código fuente y pruebas de seguridad en aplicaciones web y móviles, debido al crecimiento de las aplicaciones en línea y de dispositivos móviles.

Con el aumento de las amenazas cibernéticas y la conciencia sobre la importancia de la seguridad de la información en la década de 2010:, el ethical hacking se volvió más relevante y profesional. Se desarrollaron nuevas herramientas y estrategias, como herramientas de análisis de malware, pruebas de seguridad en la nube y pruebas de seguridad en Internet de las cosas (IoT). Además, se enfatizó más en la importancia de la ética y la legalidad en el ethical hacking, estableciendo normas y regulaciones más estrictas en la industria.

En la actualidad, las herramientas y estrategias utilizadas en el ethical hacking continúan evolucionando rápidamente. Se han desarrollado herramientas más avanzadas y automatizadas para identificar y explotar vulnerabilidades en sistemas, aplicaciones y redes. Además, se ha incrementado el enfoque en la concientización del personal, la educación en seguridad y la implementación de políticas y procedimientos de seguridad efectivos, a lo largo del tiempo, el uso de herramientas y estrategias en la metodología del ethical hacking ha evolucionado para adaptarse a los avances tecnológicos y a las cambiantes amenazas de seguridad. Desde técnicas rudimentarias en los primeros días del hacking ético hasta herramientas y estrategias sofisticadas y automatizadas en la actual.

1.8 ANTECEDENTES O ESTADO ACTUAL

El ethical hacking se encuentra en constante evolución y desarrollo en la actualidad. A medida que la tecnología avanza y los sistemas informáticos se vuelven más complejos, la necesidad de realizar pruebas de seguridad, identificar vulnerabilidades y proteger la información se vuelve cada vez más importante. Algunos aspectos destacados del estado actual del ethical hacking incluyen:

Mayor conciencia sobre la seguridad cibernética: Con el aumento de la ciberdelincuencia y los ciberataques, la conciencia sobre la importancia de la seguridad cibernética ha aumentado significativamente. Tanto las empresas como los individuos están tomando medidas para proteger sus sistemas y datos, lo que ha llevado a un mayor interés y demanda de servicios de ethical hacking.

Actualmente existen regulaciones y normativas en muchos países que rigen la conducta ética y legal del ethical hacking. Los profesionales del ethical hacking deben seguir las leyes y regulaciones aplicables, así como adherirse a principios

éticos y mejores prácticas establecidas por la industria. De la mano se han desarrollado y mejorado constantemente herramientas y tecnologías para realizar pruebas de seguridad y escanear vulnerabilidades en sistemas informáticos. Estas herramientas se han vuelto más sofisticadas y automatizadas, lo que permite a los profesionales del ethical hacking identificar y abordar vulnerabilidades de manera más eficiente.

En un Enfoque holístico de la seguridad considerando aspectos como la seguridad en la nube, seguridad en dispositivos móviles, seguridad en aplicaciones web, seguridad en redes sociales, y seguridad en IoT (Internet de las cosas). Los profesionales del ethical hacking necesitan tener conocimientos y habilidades en una amplia gama de áreas de seguridad para abordar los desafíos actuales en este campo.

Figura 2. Clasificación de sujetos que realizan las pruebas de penetración

Fuente: *SCIELO. Herramientas fundamentales para el hacking ético [sitio web]. Bogotá; [Consultado: noviembre de 2023]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592020000100116*

Con la creciente conciencia sobre la seguridad cibernética, la demanda de profesionales con habilidades de ethical hacking ha aumentado. Las empresas, organizaciones gubernamentales y otras entidades buscan expertos en seguridad

cibernética que puedan realizar pruebas de seguridad, identificar vulnerabilidades y proteger sus sistemas y datos de posibles ataques.

1.9 MARCO CIENTÍFICO O TECNOLÓGICO

Existen varios marcos científicos y tecnologías que se utilizan en el ethical hacking, también conocido como hackeo ético, que es una práctica legal y ética de identificar vulnerabilidades en sistemas informáticos para protegerlos contra ataques maliciosos. Algunos de los marcos científicos y tecnologías comunes utilizados en el ethical hacking incluyen:

Metodología OSSTMM (Open Source Security Testing Methodology Manual): Es un marco de pruebas de seguridad basado en un enfoque metodológico para evaluar la seguridad de los sistemas de información y redes. Proporciona un conjunto detallado de procedimientos y técnicas para llevar a cabo pruebas de seguridad de manera estructurada y organizada.

Metodología PTES (Penetration Testing Execution Standard): Es un estándar de la industria que describe un enfoque comúnmente aceptado para realizar pruebas de penetración o pruebas de intrusión. Proporciona una metodología detallada y estructurada que cubre todas las fases de una prueba de penetración, desde la planificación y la recopilación de información, hasta la explotación y la documentación de resultados.

Herramientas de escaneo de vulnerabilidades: Existen diversas herramientas de escaneo de vulnerabilidades, como Nessus, OpenVAS, y Qualys, que ayudan a identificar y evaluar vulnerabilidades en sistemas informáticos y redes. Estas herramientas utilizan una base de datos de vulnerabilidades conocidas y realizan pruebas automatizadas para identificar posibles puntos débiles en un sistema.

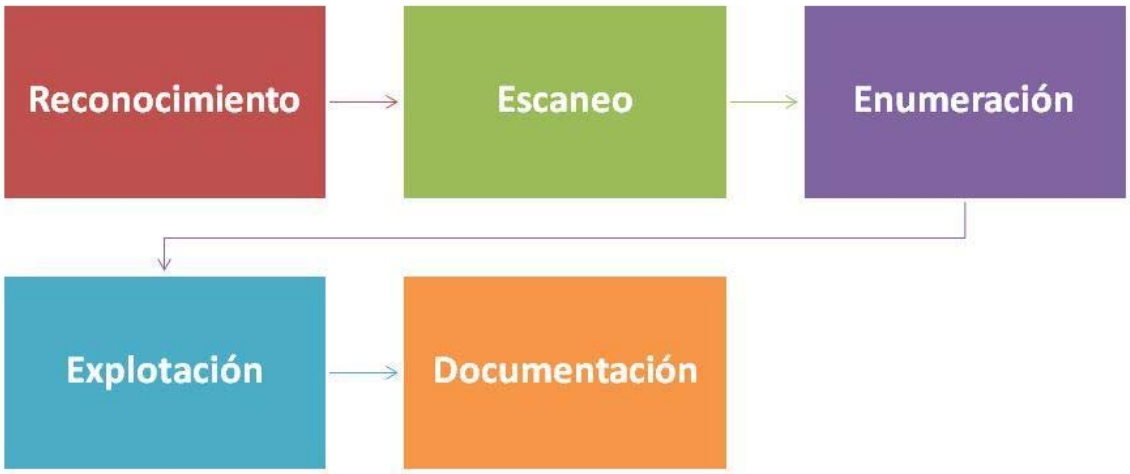
Herramientas de explotación: Estas herramientas, como Metasploit y Burp Suite, son utilizadas por los ethical hackers para llevar a cabo pruebas de explotación controlada de vulnerabilidades identificadas en sistemas informáticos y redes. Estas herramientas ayudan a evaluar la capacidad de un sistema para resistir ataques y permiten a los ethical hackers demostrar la severidad y el impacto potencial de las vulnerabilidades.

Herramientas de análisis de código: Estas herramientas, como SonarQube y Fortify, se utilizan para analizar el código fuente de aplicaciones y sistemas en busca de vulnerabilidades de seguridad en el código. Esto ayuda a identificar posibles debilidades en el diseño y la implementación del software, lo que permite a los ethical hackers encontrar posibles brechas de seguridad.

Metodologías de evaluación de riesgos: Estas metodologías, como OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) y NIST SP 800-

30 (Guide for Conducting Risk Assessments), se utilizan para evaluar y clasificar los riesgos de seguridad de los sistemas informáticos y redes. Ayudan a los ethical hackers a identificar y priorizar las vulnerabilidades en función de su impacto potencial y la probabilidad de explotación.

Figura 3. Metodologías de evaluación de riesgos



Fuente: Torres, A (2023), Metodologías de evaluación de riesgos, [diagrama]. Nota: Imagen diseñada por el autor.

1.10 MARCO LEGAL

Los procesos de ethical hacking deben llevarse a cabo de manera legal y ética, y existen varios marcos legales de referencia que los ethical hackers deben tener en cuenta. Algunos de los marcos legales más comunes para el ethical hacking incluyen:

Legislación de protección de datos: Dependiendo del país o región en la que se lleve a cabo el ethical hacking, puede haber leyes y regulaciones específicas que rigen la protección de datos y la privacidad de la información. Por ejemplo, el Reglamento General de Protección de Datos (GDPR) en la Unión Europea establece normas estrictas para el tratamiento de datos personales, incluyendo la necesidad de obtener consentimiento adecuado antes de realizar pruebas de seguridad que involucren datos personales.

Leyes de propiedad intelectual: Las leyes de propiedad intelectual protegen los derechos de propiedad de software, sistemas y otros activos digitales. Los ethical hackers deben asegurarse de no infringir derechos de propiedad intelectual durante sus pruebas, como no copiar, distribuir o utilizar software protegido sin la debida autorización.

Leyes de acceso no autorizado: Las leyes de acceso no autorizado prohíben el acceso no autorizado a sistemas informáticos y redes. Los ethical hackers deben asegurarse de obtener el permiso por escrito del propietario del sistema antes de realizar cualquier prueba de seguridad y asegurarse de que sus actividades estén dentro de los límites establecidos en el acuerdo de autorización.

Leyes de notificación de brechas de seguridad: Algunas jurisdicciones tienen leyes de notificación de brechas de seguridad que requieren que las organizaciones notifiquen a las autoridades o a los individuos afectados en caso de que se descubra una brecha de seguridad. Los ethical hackers deben estar al tanto de estas leyes y seguir los procedimientos apropiados si descubren una brecha de seguridad durante sus pruebas.

Normas y regulaciones específicas de la industria: Algunas industrias, como la banca, la salud y la energía, tienen regulaciones específicas de seguridad que deben cumplirse. Por ejemplo, el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago/credito (PCI DSS) establece requisitos de seguridad para las organizaciones que procesan pagos con tarjetas de crédito. Los ethical hackers deben estar familiarizados con estas normas y regulaciones específicas de la industria cuando realicen pruebas de seguridad en esos sectores.

Es importante tener en cuenta que las leyes y regulaciones pueden variar según la jurisdicción y es responsabilidad del ethical hacker conocer y cumplir con las leyes aplicables en su área geográfica y asegurarse de obtener los permisos y autorizaciones adecuados antes de realizar cualquier actividad de ethical hacking.

DISEÑO METODOLÓGICO

Existen varias metodologías ampliamente utilizadas para ejecutar un proceso de ethical hacking de manera estructurada y eficientes, sin embargo, para el desarrollo de este documento se toman las siguientes referencias:

1.11 METODOLOGÍA DE PRUEBAS DE PENETRACIÓN (PENETRATION TESTING)

Es una metodología sistemática que implica simular ataques de hackers para identificar vulnerabilidades y brechas de seguridad en un sistema o red. Por lo general, sigue una secuencia de fases que incluyen la planificación, la recopilación de información, la enumeración, la explotación, el mantenimiento del acceso y el informe de resultados.

A continuación, se describen las fases típicas de una metodología de pruebas de penetración:

Planificación: En esta fase inicial, se define el alcance y los objetivos de la prueba de penetración. Esto implica identificar los sistemas, redes o aplicaciones que serán evaluados, determinar los límites y restricciones de la prueba, establecer los objetivos y resultados esperados, y obtener la autorización y consentimiento adecuado de los propietarios o responsables de los sistemas evaluados.

Recopilación de información (Reconocimiento): En esta fase, se recopila información sobre el objetivo de la prueba de penetración, como la identificación de sistemas, servicios, aplicaciones, configuraciones de red y otros datos relevantes. Esto se puede hacer mediante la utilización de herramientas de escaneo de red, exploración de puertos, búsqueda de información pública, entre otros métodos.

Enumeración: En esta fase, se realiza una enumeración detallada de los sistemas y servicios identificados durante la fase de recopilación de información. Esto implica obtener información adicional, como la identificación de usuarios, grupos, permisos, versiones de software, configuraciones de seguridad y otros detalles relevantes que puedan ayudar en la identificación de vulnerabilidades.

Explotación: En esta fase, se intenta explotar las vulnerabilidades identificadas en los sistemas o aplicaciones evaluadas con el fin de obtener acceso no autorizado. Esto implica el uso de herramientas y técnicas específicas para aprovechar las vulnerabilidades y obtener acceso a sistemas o aplicaciones, con el objetivo de demostrar la existencia y gravedad de las vulnerabilidades identificadas.

Mantenimiento del acceso (Persistencia): En esta fase, una vez obtenido el acceso a los sistemas o aplicaciones evaluadas, se busca mantener el acceso de forma persistente para poder realizar actividades posteriores de pruebas y evaluar la capacidad de detección y respuesta de los sistemas de seguridad. Esto puede incluir la instalación de backdoors, creación de cuentas de usuario, modificación de permisos, entre otros.

Informe de resultados: En esta fase, se documentan todos los hallazgos de la prueba de penetración en un informe detallado. Esto incluye la descripción de las vulnerabilidades identificadas, los pasos seguidos para explotarlas, los resultados obtenidos, las pruebas realizadas, las recomendaciones de mitigación y cualquier otra información relevante. El informe de resultados es un producto clave de la prueba de penetración y se utiliza para informar a los propietarios o responsables de los sistemas evaluados sobre las vulnerabilidades identificadas y las acciones correctivas recomendadas.

1.12 METODOLOGÍA DE PRUEBAS DE VULNERABILIDAD (VULNERABILITY SCANNING)

Esta metodología se basa en el uso de herramientas automáticas para identificar y evaluar vulnerabilidades en sistemas, redes o aplicaciones. Por lo general, implica la ejecución de escaneos automatizados en busca de vulnerabilidades conocidas y la generación de informes detallados sobre los hallazgos.

A continuación, se describen las fases típicas de una metodología de pruebas de vulnerabilidad:

Planificación: En esta fase inicial, se define el alcance y los objetivos de la prueba de vulnerabilidad. Esto implica identificar los sistemas, redes o aplicaciones que serán evaluados, determinar los límites y restricciones de la prueba, establecer los objetivos y resultados esperados, y obtener la autorización y consentimiento adecuado de los propietarios o responsables de los sistemas evaluados.

Escaneo de vulnerabilidades: En esta fase, se utilizan herramientas automatizadas de escaneo de vulnerabilidades para identificar y evaluar las vulnerabilidades presentes en los sistemas o aplicaciones evaluadas. Estas herramientas realizan escaneos en busca de configuraciones incorrectas, fallos en el software, vulnerabilidades conocidas y otros elementos que puedan representar riesgos de seguridad.

Análisis de resultados: Una vez completado el escaneo de vulnerabilidades, se analizan los resultados obtenidos para identificar las vulnerabilidades confirmadas y evaluar su gravedad. Esto implica verificar la veracidad de las vulnerabilidades identificadas, priorizarlas en función de su riesgo potencial y clasificarlas en función de su severidad.

Validación manual: En esta fase, se realiza una validación manual de las vulnerabilidades identificadas durante el escaneo automatizado. Esto implica verificar la existencia y gravedad de las vulnerabilidades mediante pruebas manuales, como intentos de explotación, análisis de registros de eventos, pruebas de autenticación, entre otros métodos.

Informe de resultados: En esta fase, se documentan todos los hallazgos de la prueba de vulnerabilidad en un informe detallado. Esto incluye la descripción de las vulnerabilidades identificadas, los resultados obtenidos, las recomendaciones de mitigación y cualquier otra información relevante. El informe de resultados es un producto clave de la prueba de vulnerabilidad y se utiliza para informar a los propietarios o responsables de los sistemas evaluados sobre las vulnerabilidades identificadas y las acciones correctivas recomendadas.

DESARROLLO METODOLÓGICO (EJECUCIÓN DE PRUEBAS)

1.13 METODOLOGÍA DE PRUEBAS DE VULNERABILIDAD (INGENIERIA SOCIAL Y PHISHING)

El presente proceso tiene como objetivo presentar los resultados obtenidos durante el ejercicio de ingeniería Social realizado a la **COMPANiA INTERNACIONAL DE INTEGRACIÓN S.A**.

El proceso de ingeniería Social realizado a la COMPANiA INTERNACIONAL DE INTEGRACIÓN, se basa en dos tareas que consisten en phishing por correo electrónico y llamadas telefónicas, las cuales permitieron detectar fortalezas y debilidades en cuanto conciencia de seguridad existentes en los usuarios. Es claro que estos son el eslabón más débil de las empresas y que por la ingenuidad y falta de precaución puede ocurrir que revelen información confidencial a quien no corresponda

La metodología utilizada esta alineada con el control 7.2.2. de ISO 27001 educación, formación y concientización sobre la seguridad de la información y NIST 800-50 Building and Information Technology Security Awareness and Training Program

El objetivo es conocer el grado de manipulación psicológica que las personas tienen para entregar voluntariamente información confidencial mediante engaños.

Esta actividad de ingeniería social se llevó a cabo a través de dos formas: llamadas telefónicas y phishing por correo electrónico a personal de la COMPANiA INTERNACIONAL DE INTEGRACIÓN

1.13.1 Muestra

Se definió una muestra de 30 funcionarios de la organización, pertenecientes a diferentes áreas, que se relacionan a continuación

Tabla 1. Muestra de funcionarios

No.	Persona	Cargo	Celular
1	ALEJANDRA BERDUGO	COORD. MERCADEO	3012246564
2	ALEXANDRA CALDERON	COORD. TESORERIA	3165282289
3	ANGELICA MOLINA	COORD. LICITACIONES	3165282126
4	CAROLL FORERO	ASIST. ADMINISTRATIVA	3175176085
5	CHRISTIAN ZAMORA	COORD. LIDER SGI	3164541007
6	DANIEL AVILA	ING. GERENTE PROYECTOS Y SERVICIOS	3174008331
7	DANIELA PEÑA	CONTADORA	3167407578
8	DANIELA RAMIREZ	AUX. ADMINISTRATIVA	3162887832
9	DIEGO PEÑA	COORD. COMPRAS Y LOGISTICA	3014070683
10	FERNANDO GAVIRIA	GERENTE GENERAL	3016876991
11	FREDDY BARRAGAN	ING. IDI	3176366503
12	JAIME CONTRERAS	ING. GERENTE PROYECTOS Y SERVICIOS	3167409185
13	JAIMES FLAVIO	KAM GESTOR DE CUENTAS ESTRATEGICAS	3016887320
14	JOAN CARDENAS	SUPERVISOR DE ZONA	3175159761
15	JUAN AREVALO	COORD. INTEGRACIONES	3243240023
16	LEONARDO PIRANEQUE	ING. GERENTE PROYECTOS Y SERVICIOS	3044948265
17	LEONEL FORERO	DIRECTOR IDI	3042949365
18	LORENA BERNAL	REPRESENTANTE LEGAL - ABOGADA	3168319104
19	LUIS TAPIA	CONTROLLER	3044963898
20	MESA DE SERVICIO	ANALISTA MESA DE SERVICIO	3175178956
21	MILLER LINARES	COORD. REDES E INFRAESTRUCTURA	3174385969
22	NORMA REYES	GERENTE TECNICO DE DESARROLLO Y NEGOCIOS	3165258973
23	OSCAR CADENA	KAM GESTOR DE CUENTAS ESTRATEGICAS	3157004101
24	PEDRO DUARTE	GERENTE PROYECTOS ESPECIALES	3162698993
25	SERGIO PANTOJA	DIRECTOR OPERACIONES	3012806384
26	SERGIO ZAPATA	GESTOR LIDER MESA DE SERVICIO	3183678885
27	VICTOR RADICCHIO	ING. GERENTE PROYECTOS Y SERVICIOS	3162511123
28	XIMENA VILLABON	TECNICO LIDER PROYECTOS Y SERVICIOS	3044963955
29	YADY ESPAÑA/JAIME CARDONA	DIRECTOR ADMINISTRATIVO	3183239633
30	YASMIN HENAO	COORD. TALENTO HUMANO	3168344229

Fuente: *Torres, A (2023), Muestra de funcionarios, [Tabla]. Nota: Imagen diseñada por el autor.*

1.13.2 Definición de engaño a aplicar

Teniendo en cuenta la información suministrada por parte de COMPANiA INTERNACIONAL DE INTEGRACIÓN, se estableció en conjunto el siguiente engaño:

Guion: Soy Martha Perez/Juan Sanchez/Guillermo Lopez de la secretaria distrital de salud, a raíz de los picos de la pandemia por ómicron, estamos en una campaña de verificación de cerco epidemiológico en conjunto con la Superintendencia de puertos y transportes, me puede atender no le quitara más de un minuto

Tabla 2. Listado de preguntas

Pregunta 1	*Nos confirma que usted es empleado de Compañía Internacional de Integración CI2 S.A.*
Pregunta 2	*Edad*
Pregunta 3	*Nivel profesional*
Pregunta 4	*Cargo, Área*
Pregunta 5	*Ya cuenta con el ciclo completo de vacunación*
Pregunta 6	*Que biológico le aplicaron*
Pregunta 7	*Ya se ha aplicado el refuerzo, que biológico*
Pregunta 8	*Estás presentando síntomas respiratorios, tos, fiebre, y/o dolor garganta*
Pregunta 9	*Su actividad laboral la esta desempeñando virtualmente, alternancia, presencial*
Pregunta 10	*Su actividad laboral le implica movilizar fuera de un sitio fijo*
Pregunta 11	*Su actividad laboral le implica tomar transporte publico*
Pregunta 12	*Ha tenido movilidad fuera de su casa, ciudad o país en los últimos 14 días*
Pregunta 13	*Has estado en contacto por más de quince minutos y a menos de dos metros de distancia de una persona a quien en los últimos 14 días se le haya confirmado infección respiratoria por el nuevo coronavirus*
Pregunta 14	*Le han practicado la prueba de Coronavirus (Muestra en nariz)*
Pregunta 15	*Ha sido diagnosticado con COVID durante el periodo de la pandemia*
Pregunta 16	*Se me olvido diligenciar unos datos personales, numero de Identificación*
Pregunta 17	*Lugar de expedición*
Pregunta 18	*Dirección*
Pregunta 19	*Localidad*
Pregunta 20	*Jefe Inmediato*

Fuente: Torres, A (2023), Listado de preguntas [Tabla]. Nota: Imagen diseñada por el autor.

1.13.3 ejecución de llamadas

La ejecución de las llamadas se extendió durante dos semanas comprendidas entre el 17 y el 28 de abril de 2023, teniendo la particularidad de que no todas las personas contestaron en el primer intento y se realizaron varios intentos. Para la ejecución de las llamadas que se realizaron a los funcionarios de COMPAÑÍA INTERNACIONAL DE INTEGRACIÓN.

1.13.4 Resultados

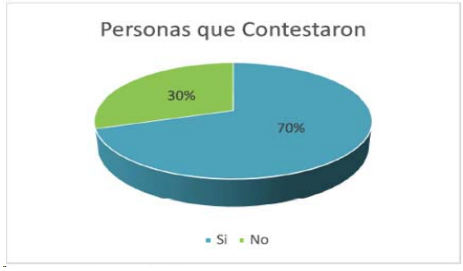
Dado que el guión definido para el engaño de las llamadas telefónicas tenía tres grupos de preguntas así:

- Preguntas relacionadas con la vinculación con Ci2

- Preguntas epidemiológicas
- Preguntas personales

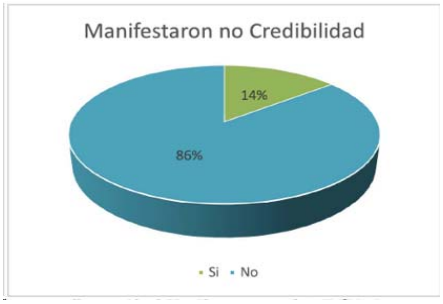
La información se tabuló y graficó de acuerdo con los tres grupos de preguntas, la información obtenida por cada colaborador al que se le realizó la llamada dentro del trabajo de ingeniería social se muestra a continuación:

Figura 4. Personas que contestaron



Fuente: Torres, A (2023), Personas que contestaron [Gráfico]. Nota: Imagen diseñada por el autor.

Figura 5. Personas que manifestaron no credibilidad



Fuente: Torres, A (2023), Personas que manifestaron no credibilidad [Gráfico]. Nota: Imagen diseñada por el autor.

Figura 6. Personas que respondieron preguntas de vinculación con CI2

Fuente: Torres, A (2023), Personas que respondieron preguntas de vinculación con CI2, [Gráfico]. Nota: Imagen diseñada por el autor.

Figura 7. Personas que respondieron preguntas epidemiológicas

Fuente: Torres, A (2023), Personas que respondieron preguntas epidemiológicas [Gráfico]. Nota: Imagen diseñada por el autor.

Figura 8. Personas que respondieron preguntas personales

Fuente: Torres, A (2023), Personas que respondieron preguntas personales [Gráfico]. Nota: Imagen diseñada por el autor.

Complementario a las gráficas anteriores, se presenta a continuación una tabla con los detalles del proceso de llamadas:

Tabla 3. Tabulación de llamadas

No	Persona	Contestó	Enfatiza no credibilidad en la encuesta	Respondió preguntas relacionadas con la empresa (edad, vinculación, rol, nivel profesional)	Respondió preguntas epidemiológicas	Respondió preguntas personales (cedula, dirección, jefe)
1	CHRISTIAN ZAMORA	Si	No	Si	Si	No
2	DANIEL AVILA 3174008331 nc	Si	No	Si	Si	Si
3	DIEGO PEÑA 3014070683 nc	Si	No	Si	Si	Si
4	FREDDY BARRAGAN 3176366503 2 pm	Si	No	Si	Si	Si
5	FERNANDO GAVIRIA GTE 3016876991	Si	Si	No	Si	No
6	JAIME CONTRERAS 3167409185	Si	No	Si	Si	Si
7	JOAN CARDENAS 3175159761	Si	No	Si	Si	Si
8	JUAN AREVALO 3243240023 nc	Si	No	Si	Si	No
9	LEONARDO PIRANEQUE 3044948265	Si	No	Si	Si	Si
10	LEONEL FORERO 3042949365	Si	Si	No	No	No
11	VICTOR RADICCHIO 3162511123	Si	No	Si	Si	Si
12	XIMENA VILLABON 3044963955	Si	No	Si	Si	No
13	YADY ESPAÑA JAIME CARDONA 3183239633	Si	No	Si	Si	Si
14	JASMIN HENAO 3168344229	Si	No	Si	Si	Si
15	ALEXANDRA CALDERON 3165282289	Si	No	Si	Si	Si
16	DANIELA PEÑA 3167407578	Si	No	Si	Si	Si
17	LUIS TAPIA 3044963898	Si	No	Si	Si	Si
18	OSCAR CADENA 3157004101	Si	No	Si	Si	Si
19	NORMA REYES 3165258973	Si	No	Si	Si	Si
20	PEDRO DUARTE 3162698993	Si	No	Si	Si	Si
21	SERGIO PANTOJA 3012806384	Si	Si	Si	No	No
22	SERGIO ZAPATA 3183678885	No	NA	NA	NA	NA
23	ALEJANDRA BERDUGO 3012246564	No	NA	NA	NA	NA
24	ANGELICA MOLINA 3165282126	No	NA	NA	NA	NA
25	CAROLL FORERO 3175176085	No	NA	NA	NA	NA
26	DANIELA RAMIREZ 3162887832	No	NA	NA	NA	NA
27	MESA DE SERVICIO 3175178956	No	NA	NA	NA	NA

No	Persona	Contestó	Enfatiza no credibilidad en la encuesta	Respondió preguntas relacionadas con la empresa (edad, vinculación, rol, nivel profesional)	Respondió preguntas epidemiológicas	Respondió preguntas personales (cedula, dirección, jefe)
28	MILLER LINARES 3174385969	No	NA	NA	NA	NA
29	JAIMES FLAVIO 3016887320	No	NA	NA	NA	NA
30	LORENA BERNAL 3168319104	No	NA	NA	NA	NA

Fuente: Torres, A (2023), Tabulación de llamadas [Tabla]. Nota: Imagen diseñada por el autor.

1.14 PHISHING CONTROLADO A USUARIOS

1.14.1 Muestra

Se definió una muestra de 30 funcionarios de la organización, pertenecientes a diferentes áreas, que se relacionan a continuación

Tabla 4. Muestra de funcionarios

No.	Nombre para mostrar	CARGO	Nombre principal de usuario
1	Adalberto Navarro	TECNICO DE LIDER DE PROYECTOS Y SERVICIOS	adalberto.navarro@ci2.co
2	Alejandra Berdugo	COORD. MERCADEO	alejandra.berdugo@ci2.co
3	Ana Milena Valencia Moreno	TECNICO DE PROYECTOS Y SERVICIOS	ana.valencia@ci2.co
4	Angélica Huérfano	ASIST. COMERCIAL	angelica,huerfano@ci2,co
5	Angélica Oviedo	ING. QA/QC	angelica,oviedo@ci2,co
6	Carly Viatela	ANALISTA CONTABLE	carly.viatela@ci2.co
7	Carol Rojas	ANALISTA CONTABLE	carol.rojas@ci2.co
8	CI2 BOGOTA2	TECNICOS DE PROYECTOS Y SERVICIOS	ci2,bogota2@ci2,co
9	Cristian Molina Cely	ANALISTA DE COMPRAS	cristian.molina@ci2.co
10	Cristian Zamora	COORD. LIDER SGI	cristian,zamora@ci2,co
11	Danny Patiño	SUPERVISOR DE ZONA	danny.patino@ci2.co
12	Deyvid Galvis	ASISTENTE SGI	deyvid.galvis@ci2.co
13	Edwin Zorro	KAM JUNIOR	edwin.zorro@ci2.co
14	German Méndez	ING. PREVENTA	german,mendez@ci2,co
15	Giovanny Benites	ING. IDI	giovanny.benites@ci2.co
16	Juan David Castro	ING. PROYECTOS Y SERVICIOS	juan.castro@ci2.co
17	Jaime Cardona	DIRECTOR ADMINISTRATIVO	jaime.cardona@ci2.co
18	Jaime Contreras	ING. GERENTE PROYECTOS Y SERVICIOS	jaime.contreras@ci2.co
19	Johan Cubides	AUX. ADMINISTRATIVO	johan,cubides@ci2,co
20	Leonardo Piraneque	ING. GERENTE PROYECTOS Y SERVICIOS	leonardo.piraneque@ci2.co

No.	Nombre para mostrar	CARGO	Nombre principal de usuario
21	Lorena Bernal	REPRESENTANTE LEGAL – ABOGADA	lorena.bernal@ci2.co
22	Luis Alfonso Tapia Ballesta	CONTROLLER	luis.tapia@ci2.co
23	Luisa Muñoz	ASIST, COMPRAS Y LOGISTICA	luisa,munoz@ci2,co
24	Norma Reyes	GERENTE TECNICO DESARROLLO DE NEGOCIOS	norma.reyes@ci2.co
25	Orlando Díaz	SUPERVISOR DE ZONA	orlando.diaz@ci2.co
26	Oscar Cadena	KAM GESTOR DE CUENTAS ESTRATEGICAS	oscar,cadena@ci2,co
27	Recepción	RECEPCION	recepcion@ci2,co
28	Yerson Ramírez	ESPECIALISTA REDES	yerson.ramirez@ci2.co
29	Sergio Pantoja	DIRECTOR OPERACIONES	sergio.pantoja@ci2.co
30	Yasmin Henao	COORD. TALENTO HUMANO	yasmin.henao@ci2.co

Fuente: Torres, A (2023), Muestra de funcionarios [Tabla]. Nota: Imagen diseñada por el autor.

1.14.2 Definición de engaño

Phishing conocido como suplantación de identidad, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta como puede ser una contraseña, información detallada.

Como parte de una verificación de la conciencia de seguridad de los usuarios, se realiza un ataque de Phishing contra un conjunto de 30 buzones de correos, proveniente del supuesto buzón de comunicaciones@ci2.co como parte de una campaña falsa para la entrega de membresías de Disney+ por un periodo de un mes. Los correos son enviados de forma individual los cuales constan de una imagen con un enlace adjunto y una firma muy similar a la empleada por el buzón de comunicaciones@ci2.co; con la diferencia de que el carácter guion (-) en el teléfono de la mesa de servicio para la firma real es más alargado:

Figura 9. Invitación para correo

Fuente: Torres, A (2023), Invitación para correo [Imagen]. Nota: Imagen diseñada por el autor.

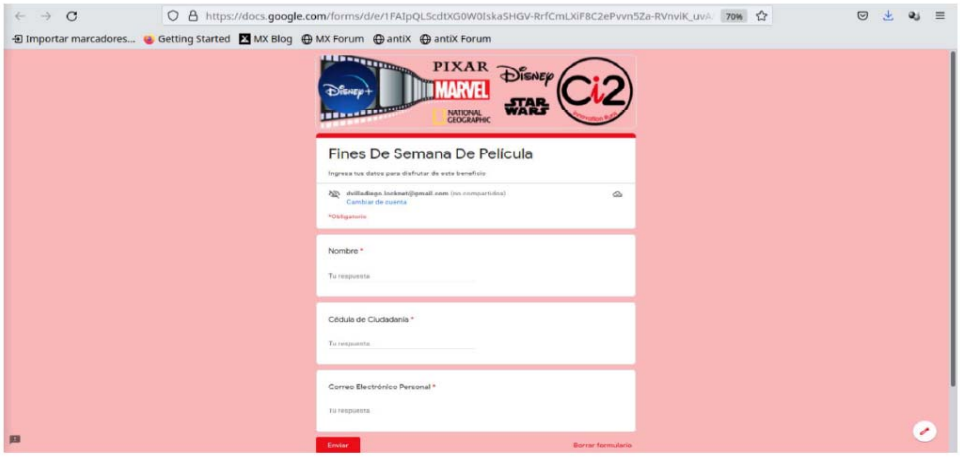
Figura 10. Firma de correo modificada

Fuente: Torres, A (2023), Firma de correo modificada [Imagen]. Nota: Imagen diseñada por el autor.

Por su parte, la razón detrás del envió de los correos de forma individual se debe a que a cada usuario se le envía un enlace levemente diferente entre ellos; donde el patrón es http:l/186.31.88.196 :8080/USUARIO y donde "USUARIO" es un numero decimal de 2 dígitos. Con esto, al momento en que el usuario da clic sobre la imagen correspondiente a la ilustración 6, el navegador abre un enlace hacia un servidor suplente y lo que permite identificar al usuario que ha hecho clic sobre la imagen.

Una vez identificado el usuario, este dato es almacenado en un archivo y redireccionado a un formulario de Google donde se solicita el nombre, la cédula de ciudadanía y el correo electrónico personal:

Figura 11. Formulario de registro



Fuente: Torres, A (2023), Formulario de registro [Imagen]. Nota: Imagen diseñada por el autor.

Los usuarios a los cuales se les realiza envío de correo electrónico son:

adalberto.navarro@ci2.co	ana.valencia@ci2.co	angelica.oviedo@ci2.co
alejandra.berdugo@ci2.co	angelica.huerfano@ci2.co	carly.viatela@ci2.co
carol.rojas@ci2.co	giovanny.benites@ci2.co	luisa.munoz@ci2.co
ci2.bogota2@ci2.co	juan.castro@ci2.co	norma.reyes@ci2.co
cristian.molina@ci2.co	jaime.cardona@ci2.co	orlando.diaz@ci2.co
cristian.zamora@ci2.co	jaime.contreras@ci2.co	oscar.cadena@ci2.co
danny.patino@ci2.co	johan.cubides@ci2.co	recepcion@ci2.co
deyvid.galvis@ci2.co	leonardo.piraneque@ci2.co	yerson.ramirez@ci2.co
edwin.zorro@ci2.co	lorena.bernal@ci2.co	sergio.pantoja@ci2.co
german.mendez@ci2.co	luis.tapia@ci2.co	yasmin.henao@ci2.co

Así mismo, se envían correos de pruebas a yesid.torres@ci2.co para validar la respectiva recepción de los correos de phishing. Ahora bien, es de notar que inicialmente estos llegaban al correo de SPAM y que fue necesario realizar una configuración de "simulación de phishing" del lado del Office365 para este ejercicio.

Esto, con aras a ser lo más apegado a la realidad en cuanto a que un correo SPAM pudiera evadir los controles del Office365.

1.14.3 Resultados

Como resultado del ejercicio, de los 30 correos electrónicos enviados, se evidenció que 22 personas dieron clic al enlace recibido en el correo Phishing, y de estas 22, 16 personas registraron información en el formulario de google docs.

Complementariamente se detectó que algunos usuarios dieron clic en más de una ocasión. A continuación, los resultados:

Figura 12. Personas que dieron clic

Fuente: Torres, A (2023), Personas que dieron clic [Imagen]. Nota: Imagen diseñada por el autor.

Figura 13. Personas que registraron información en el formulario Google

Fuente: Torres, A (2023), Personas que registraron información en el formulario Google [Imagen]. Nota: Imagen diseñada por el autor.

1.15 PRUEBAS DE INTRUSIÓN INTERNAS Y EXTERNAS TIPO WHITEBOX

Como parte fundamental del trabajo de análisis ejecutado, se presentan las recomendaciones técnicas que remedian a los hallazgos encontrados a partir de las pruebas de vulnerabilidad realizadas en COMPAÑÍA INTERNACIONAL DE INTEGRACIÓN S.A. Ci2

Este documento pretende presentar las vulnerabilidades existentes en los equipos analizados durante las pruebas realizadas. Cada vulnerabilidad será descrita con su impacto, solución y las máquinas en riesgo.

De igual forma se presenta un capítulo del proceso de explotación controlada que se ejecutó con el ánimo de confirmar la existencia de las vulnerabilidades y en cumplimiento de la metodología de procesos de hacking ético.

1.15.1 Resultados Obtenidos

1.15.1.1 Hallazgos de las pruebas externas (Servicios publicados a internet)

I. Evidencia de uso del protocolo SSL versión 2 y 3.

Descripción:
El servicio publicado permite realizar conexiones cifradas mediante los protocolos 2.0 y/o 3.0 de la capa de cifrado SSL. Estas versiones del protocolo son afectadas por varias fallas de cifrado, las cuales podrían permitir descifrar el tráfico o interceptar las comunicaciones cifradas.
NIST ha determinado que las versiones 2.0 y 3.0 del protocolo SSL no son consideradas como versiones aceptables en la implementación de aseguramiento de comunicaciones. Desde el establecimiento de PCI DSS

v3.1, cualquier versión del protocolo SSL no cumplirá con el requerimiento de 'cifrado robusto' de PCI SSC'S.

Véase también:
http://www.schneier.com/paper-ssl.pdf
https://support.microsoft.com/es-co/kb/187498
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.pcisecuritystandards.org/pdfs/15_02_12_PCI_SSC_Bulletin_on_DSS_revision s_SSL_update.pdf

Exposición:
Alto. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Alto. Un atacante puede aprovechar esta vulnerabilidad y capturar el tráfico del servicio para posteriormente descifrarlo, potencialmente obtener información confidencial.

Mitigación:
Configure el servicio para que sólo utilice TLS v1.0, v1.1 o v1.2. Para Sistema Operativo Windows infórmese en: http://support.microsoft.com/es-co/kb/187498

Si se trata de Linux con el servicio web Apache HTTP Server, realice el siguiente procedimiento:

En el archivo /etc/httpd/conf.d/ssl.conf cambie las siguientes opciones: SSLProtocol all -SSLv2 por SSLProtocol -ALL +TLSv1

En otros sistemas operativos consulte la documentación del proveedor.

Direcciones IP Afectadas:
200.69.80.210.

Servicios Afectados:
www (443/tcp).

II. Firma SSL X.509 no valida

Descripción:
La firma del certificado SSL X.509 no pertenece a una autoridad certificadora pública de confianza, lo cual rompe la cadena de certificación.

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante que logre tomar ventaja de esta vulnerabilidad podría capturar el tráfico a través de un ataque de hombre en el medio.

Mitigación:
Generar un nuevo certificado SSL y obtener la firma de una autoridad certificadora de confianza.

Direcciones IP Afectadas:
181.143.139.22, 199.192.26.57, 200.69.80.210.

Servicios Afectados:
www (443/tcp), www (8088/tcp).

III. Certificado SSL auto-firmado

Descripción:
La cadena X.509 no posee una firma reconocida por una autoridad certificadora. Si el servidor es de acceso público el uso de este certificado no es válido y no garantiza que se controle un ataque de hombre en el medio

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante que logre tomar ventaja de esta vulnerabilidad podría capturar el tráfico a través de un ataque de hombre en el medio.

Mitigación:
Generar un nuevo certificado SSL firmado por una entidad autorizada.

Direcciones IP Afectadas:
181.143.139.22, 199.192.26.57.

Servicios Afectados:
www (443/tcp), www (8088/tcp).

IV. Evidencia de protocolo TLS versión 1.0

Descripción:
El servicio acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene una serie de defectos de diseño criptográfico. Las nuevas versiones de TLS mitigan estos problemas, las versiones de TLS como 1.2 y 1.3 están diseñadas contra estas fallas y deben usarse siempre que sea posible A partir del 31 de marzo de 2020, los dispositivos finales que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web. PCI DSS v3.2 requiere que TLS 1.0 se deshabilite por completo antes del 30 de junio de 2018.

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante puede sacar provecho de esta vulnerabilidad y causar fallas de conexión y puede activar el uso de TLS 1.0 para explotar vulnerabilidades como BEAST (Exploit del navegador contra SSL / TLS).

Mitigación:
Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.

Direcciones IP Afectadas:
199.192.26.57 200.69.80.210.

Servicios Afectados:
smtp (465/tcp), www (443/tcp).

V. Certificado SSL expirado

Descripción:
El certificado digital SSL del servidor ha expirado

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Los usuarios no tendrán la total certeza de la autenticidad del sitio.

Mitigación:

Generar un nuevo certificado SSL para el servidor

Direcciones IP Afectadas:
181.143.139.22, 199.192.26.57, 200.69.80.210

Servicios Afectados:
imap (993/tcp), pop3 (995/tcp), smtp (465/tcp), www (443/tcp).

VI. Directorios Web Navegables

Descripción:
Se encuentran múltiples directorios en el servicio web que pueden ser navegados directamente.
Véase también:
http://www.nessus.org/u?0a35179e"

Exposición:
Medio. No se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Alto. Un atacante puede navegar y obtener la información expuesta sin ninguna dificultad afectando la confidencialidad de la información.

Mitigación:
Asegúrese que estos directorios no publiquen información confidencial. De ser posible, restringa el acceso o deshabilite esta funcionalidad.

Direcciones IP Afectadas:
200.69.80.210.

Servicios Afectados:
www (443/tcp)

VII. Cifrado débil en el certificado SSL (SWEET32)

Descripción:
El servicio de SSL utiliza un cifrado débil, permitiendo el usar Strength SSL Chiper con un nivel de cifrado menor a 128 bits.

Véase también:
https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

https://mozilla.github.io/server-side-tls/ssl-config-generator/

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante que logre tomar ventaja de esta vulnerabilidad podría generar otro certificado con la misma firma digital, permitiendo suplantar servicios, potencialmente obteniendo información confidencial.
CVE-2016-2183

Mitigación:
Configure el servicio SSL para que no utilice cifrado débil.

Direcciones IP Afectadas:
199.192.26.57, 200.69.80.210.

Servicios Afectados:
imap (143/tcp), imap (993/tcp), pop3 (110/tcp), pop3 (995/tcp), smtp (465/tcp), www (443/tcp).

VIII. Suites RC4 de cifrado SSL/TLS con fallos (Bar Mitzvah)

Descripción:
El servicio soporta el uso de RC4 en utiliza en el protocolo TLS y el protocolo SSL. El cifrado RC4 contiene una falla al generar bytes pseudo-aleatorios reduciendo su aleatoriedad.
CVE-2013-2566 CVE-2015-2808

Véase también:
http://www.nessus.org/u?217a3666
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante podría realizar ataques de recuperación de texto sin formato mediante el análisis estadístico de texto cifrado en una gran cantidad de sesiones que utilizan el mismo Texto sin formato con lo cual podría ser

posible descifrar el texto transmitido afectando la confidencialidad de la información.

Mitigación:
Reconfigure la aplicación afectada para que, en la medida de lo posible, evite el uso de suites de cifrado RC4. Considere usar TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.

Direcciones IP Afectadas:
199.192.26.57, 200.69.80.210.

Servicios Afectados:
imap (143/tcp), imap (993/tcp), pop3 (110/tcp), pop3 (995/tcp), smtp (465/tcp), www (443/tcp).

IX. Vulnerabilidad en el cifrado SSLv3 Padding Oracle (POODLE)

Descripción:
El servicio con capa de cifrado SSL/TLS es afectado por una vulnerabilidad relacionada con mensajes cifrados con mecanismos en modo Cipher Block Chaining (CBC).

Véase también:
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Mediante un ataque de hombre en el medio se puede descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos y si pueden obligar a una aplicación víctima a enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién creadas realizando un ataque de denegación de servicio (DoS) afectando la disponibilidad de la información.
CVE-2014-3566

Mitigación:
Deshabilitar el soporte de la versión 3 de SSL.

Direcciones IP Afectadas:
200.69.80.210.

Servicios Afectados:
www (443/tcp).

X. Aplicación web potencialmente vulnerable al Clickjacking

Descripción:
El servicio web no incluye un encabezado X-Frame-Options dentro de sus respuestas HTTP. Esto permite capturar los Click que se dan en el aplicativo o página web.

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante podría engañar a un usuario autenticado y efectuar acciones no autorizadas en la aplicación afectada.

Mitigación:
Configure el servicio web para incluir el encabezado X-Frame-Options dentro de la respuesta del contenido publicado.

Direcciones IP Afectadas:
181.143.139.22, 199.192.26.57, 200.69.80.210.

Servicios Afectados:
www (2083/tcp), www (2087/tcp), www (2096/tcp), www (443/tcp), www (9000/tcp).

XI. JQuery 1.2 < 3.5.0 multiples vulnerabilities Cross-Site Scripting (XSS).

Descripción:
Según la versión identificada en el servidor es inferior o igual a 1.2 y anterior a 3.5.0. Por lo tanto, se ve afectado por múltiples vulnerabilidades de Cross-Site Scripting (XSS). Tenga en cuenta que las vulnerabilidades a las que se hace referencia en este complemento no tienen ningún impacto en la seguridad de PAN-OS si llegase a ser un dispositivo con este sistema operativo.

Véase también:
https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
https://security.paloaltonetworks.com/PAN-SA-2020-0007

Exposición:
Alto. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante puede lograr ejecutar código en los navegadores de los usuarios que acceden al sitio web legítimo.
CVE-2020-11022, CVE-2020-11023

Mitigación:
Deshabilitar este servicio y utilizar un servicio como SSH, el cual utiliza un canal cifrado.

Direcciones IP Afectadas:
181.143.139.22.

Servicios Afectados:
www (9000/tcp).

XII. Se permiten inicios de sesión de texto sin cifrar POP3.

Descripción:
El servidor remoto POP3 permite autenticación en texto plano sobre un canal no cifrado.

Véase también:
https://tools.ietf.org/html/rfc2595
https://tools.ietf.org/html/rfc2222

Exposición:
Bajo. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante podría capturar información de nombres de usuario y contraseñas por medio de un Sniffer de red.

Mitigación:
Configure el servidor para hacer cumplir siempre las conexiones cifradas a través de SSL / TLS con el comando 'STLS'.

Direcciones IP Afectadas:

199.192.26.57

Servicios Afectados:
pop3 (110/tcp).

XIII. Suites de cifrado anónimo – SSL

Descripción:
El servicio publicado con la capa de cifrado SSL/TLS soporta el uso de suites de cifrado con mecanismo anónimo. Este tipo de mecanismo de cifrado no requiere de llaves dentro de los certificados y, por lo tanto, no otorga ningún mecanismo de verificación de la identidad. Esta vulnerabilidad facilita drásticamente la ejecución de una suplantación del servicio con el fin de realizar ataques de hombre en el medio.

Nota: Esto es considerablemente más fácil de explotar si el atacante está en la misma red física.

Exposición:
Bajo. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante podría obtener información confidencial afectando la confidencialidad CVE-2007-1858

Mitigación:
Modifique la configuración de la capa de cifrado SSL/TLS con el fin de siempre requerir el uso de certificados firmados y elimine el soporte de suites de cifrado con mecanismo anónimo.

Direcciones IP Afectadas:
199.192.26.57

Servicios Afectados:
ftp (21/tcp), imap (143/tcp), imap (993/tcp), pop3 (110/tcp), pop3 (995/tcp), smtp (465/tcp)

XIV. Vulnerabilidad de CRIME del Protocolo TLS

Descripción:
El servicio tiene por lo menos una de las dos configuraciones que se conoce son necesarias para realizar un ataque CRIME:

- La compresión de SSL/TLS está habilitada.
- TLS publica una versión de SPDY anterior a la versión 4.

Véase también:
https://www.iacr.org/cryptodb/data/paper.php?pubkey=3091
https://discussions.nessus.org/thread/5546
http://www.nessus.org/u?c44d5826
https://bz.apache.org/bugzilla/show_bug.cgi?id=53219

Exposición:
Bajo. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante que logre tomar ventaja del ataque CRIME puede descifrar ciertos tramos de texto que pueden ser confidenciales. CVE-2012-4929, CVE-2012-4930

Mitigación:
Deshabilitar la compresión y/o el servicio SPDY.

Direcciones IP Afectadas:
181.143.139.22

Servicios Afectados:
www (8088/tcp).

1.15.1.2 Hallazgos de las pruebas internas (red lan)

I. Evidencia de versión fuera de soporte de Microsoft SQL Server.

Descripción:
Según el número de versión detectada de la instalación de Microsoft SQL Server esta ya no cuenta con soporte por parte del fabricante. La falta de soporte del fabricante implica que no se lanzarán nuevos parches de seguridad para el producto y como resultado es probable que contenga vulnerabilidades de seguridad.

Exposición:
Alto. En caso de salir una vulnerabilidad nueva no se tendrán actualizaciones, parches de seguridad ni soporte.

Impacto:

Alto. Ante la existencia de nuevas vulnerabilidades el fabricante no generará actualizaciones para solucionarlas.

Mitigación:
Actualice a una de las versiones con soporte de Microsoft SQL Server.

Direcciones IP Afectadas:
192.168.248.3

Servicios Afectados:
mssql (1433/tcp).

II. ESXi 6.0 / 6.5 / 6.7 Múltiples Vulnerabilidades (VMSA-2018-0027) (verificación remota)

Descripción:
A la versión de VMware ESXi le falta un parche de seguridad. Por lo tanto, es afectado por múltiples vulnerabilidades:

- Existe un error de uso después de la liberación en el controlador USB XHCI. (CVE-2020-4004)
- Existe una vulnerabilidad de escalamiento de privilegios en ESXi debido a la forma en que se administran ciertas llamadas al sistema. (CVE-2020-4005)
- Existe una vulnerabilidad de lectura en dispositivos SVGA (tarjeta gráfica virtual implementada por todos los productos de virtualización de VMware).

Véase también:
https://www.vmware.com/security/advisories/VMSA-2018-0026.html

Exposición:
Alto. No se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Alto. Se pueden realizar diferentes tipos de ataques como, por ejemplo:

- Un atacante local no autenticado con privilegios administrativos locales en una máquina virtual puede aprovechar esto para ejecutar código como el proceso VMX de la máquina virtual que se ejecuta en el host. CVE-2020-4004

- Un atacante local autenticado con privilegios dentro del proceso de VPM puede aprovechar esto, cuando está encadenado con CVE-2020-4004, para obtener privilegios escalados. CVE-2020-4005
- Un atacante tenga acceso a una máquina virtual con un controlador USB virtual presente. Estos problemas pueden permitir que un invitado ejecute código en el host. CVE-2019-5518, CVE-2019-5519

Mitigación:
Aplique el parche indicado según la versión de VMware instalada como lo indica el proveedor.

Direcciones IP Afectadas:
192.168.248.14

Servicios Afectados:
www (443/tcp).

III. Evidencia de uso del protocolo SSL versión 2 y 3.

Descripción:
El servicio publicado permite realizar conexiones cifradas mediante los protocolos 2.0 y/o 3.0 de la capa de cifrado SSL. Estas versiones del protocolo son afectadas por varias fallas de cifrado, las cuales podrían permitir descifrar el tráfico o interceptar las comunicaciones cifradas. NIST ha determinado que las versiones 2.0 y 3.0 del protocolo SSL no son consideradas como versiones aceptables en la implementación de aseguramiento de comunicaciones. Desde el establecimiento de PCI DSS v3.1, cualquier versión del protocolo SSL no cumplirá con el requerimiento de 'cifrado robusto' de PCI SSC'S.

Véase también:
http://www.schneier.com/paper-ssl.pdf
https://support.microsoft.com/es-co/kb/187498
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.pcisecuritystandards.org/pdfs/15_02_12_PCI_SSC_Bulletin_on_DSS_revision s_SSL_update.pdf

Exposición:
Alto. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:

Alto. Un atacante puede aprovechar esta vulnerabilidad y capturar el tráfico del servicio para posteriormente descifrarlo, potencialmente obtener información confidencial.

Mitigación:
Configure el servicio para que sólo utilice TLS v1.0, v1.1 o v1.2. Para Sistema Operativo Windows infórmese en: http://support.microsoft.com/es-co/kb/187498

Si se trata de Linux con el servicio web Apache HTTP Server, realice el siguiente procedimiento:

En el archivo /etc/httpd/conf.d/ssl.conf cambie las siguientes opciones: SSLProtocol all -SSLv2 por SSLProtocol -ALL +TLSv1

En otros sistemas operativos consulte la documentación del proveedor.

Direcciones IP Afectadas:
192.168.248.24 192.168.248.25 192.168.248.90.

Servicios Afectados:
csd-mgmt-port? (3071/tcp), www (443/tcp).

IV. Firma SSL X.509 no valida

Descripción:
La firma del certificado SSL X.509 no pertenece a una autoridad certificadora pública de confianza, lo cual rompe la cadena de certificación.

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante que logre tomar ventaja de esta vulnerabilidad podría capturar el tráfico a través de un ataque de hombre en el medio.

Mitigación:
Generar un nuevo certificado SSL y obtener la firma de una autoridad certificadora de confianza.

Direcciones IP Afectadas:
172.16.7.1, 172.16.7.42, 192.168.16.202, 192.168.16.215, 192.168.248.14,

192.168.248.17, 192.168.248.24, 192.168.248.25, 192.168.248.3, 192.168.248.90.

Servicios Afectados:
apache-administration-server (8089/tcp), csd-mgmt-port (3071/tcp), mongodb (8191/tcp), msrdp (3389/tcp), mssql (1433/tcp), vcom-tunnel (8001/tcp), wbem-https (5989/tcp), www (443/tcp), www (4443/tcp), www (8089/tcp), www (9080/tcp).

V. Certificado SSL auto-firmado

Descripción:
La cadena X.509 no posee una firma reconocida por una autoridad certificadora. Si el servidor es de acceso público el uso de este certificado no es válido y no garantiza que se controle un ataque de hombre en el medio

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante que logre tomar ventaja de esta vulnerabilidad podría capturar el tráfico a través de un ataque de hombre en el medio.

Mitigación:
Generar un nuevo certificado SSL firmado por una entidad autorizada.

Direcciones IP Afectadas:
172.16.7.1, 172.16.7.42, 192.168.16.202, 192.168.16.215, 192.168.248.14, 192.168.248.17, 192.168.248.24, 192.168.248.25, 192.168.248.3, 192.168.248.90.

Servicios Afectados:
apache-administration-server? (8089/tcp), csd-mgmt-port? (3071/tcp), mongodb (8191/tcp), msrdp (3389/tcp), mssql (1433/tcp), www (443/tcp), www (4443/tcp), www (8089/tcp), www (9080/tcp).

VI. Evidencia de protocolo TLS versión 1.0

Descripción:
El servicio acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene una serie de defectos de diseño criptográfico. Las nuevas versiones de TLS mitigan estos problemas, las versiones de TLS como 1.2 y 1.3 están diseñadas contra estas fallas y deben usarse siempre que sea posible.

A partir del 31 de marzo de 2020, los dispositivos finales que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web. PCI DSS v3.2 requiere que TLS 1.0 se deshabilite por completo antes del 30 de junio de 2018.

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante puede sacar provecho de esta vulnerabilidad y causar fallas de conexión y puede activar el uso de TLS 1.0 para explotar vulnerabilidades como BEAST (Exploit del navegador contra SSL / TLS).

Mitigación:
Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.

Direcciones IP Afectadas:
192.168.16.202, 192.168.16.215, 192.168.248.14, 192.168.248.24, 192.168.248.25, 192.168.248.3, 192.168.248.90.

Servicios Afectados:
csd-mgmt-port? (3071/tcp), msrdp (3389/tcp), mssql (1433/tcp), wbem-https? (5989/tcp), www (443/tcp), www (9080/tcp).

VII. Certificado SSL expirado

Descripción:
El certificado digital SSL del servidor ha expirado

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Los usuarios no tendrán la total certeza de la autenticidad del sitio.

Mitigación:
Generar un nuevo certificado SSL para el servidor

Direcciones IP Afectadas

192.168.248.24, 192.168.248.25, 192.168.248.90

Servicios Afectados:
csd-mgmt-port? (3071/tcp), www (443/tcp).

VIII. Algoritmo débil en la firma del certificado.

Descripción:
El algoritmo de hash de la firma digital del certificado es considerado como débil (MD2, MD4 o MD5). Estos algoritmos son vulnerables a ataques de colisión.

Véase también:
http://tools.ietf.org/html/rfc3279
http://www.phreedom.org/research/rogue-ca/
http://technet.microsoft.com/es-co/security/advisory/961509

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante puede tomar ventaja de esta vulnerabilidad para generar otro certificado con la misma firma digital, permitiéndole suplantar servicios con la misma firma. CVE-2004-2761

Mitigación:
Obtener un certificado digital nuevo con una firma digital que utilice un algoritmo de hash robusto.

Direcciones IP Afectadas:
192.168.248.24 192.168.248.3

Servicios Afectados:
mssql (1433/tcp).

IX. Directorios Web Navegables

Descripción:
Se encuentran múltiples directorios en el servicio web que pueden ser navegados directamente.

Véase también:

http://www.nessus.org/u?0a35179e"

Exposición:
Medio. No se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Alto. Un atacante puede navegar y obtener la información expuesta sin ninguna dificultad afectando la confidencialidad de la información.

Mitigación:
Asegúrese que estos directorios no publiquen información confidencial. De ser posible, restringa el acceso o deshabilite esta funcionalidad.

Direcciones IP Afectadas:
192.168.248.90

Servicios Afectados:
www (443/tcp)

X. Cifrado débil en el certificado SSL (SWEET32)

Descripción:
El servicio de SSL utiliza un cifrado débil, permitiendo el usar Strength SSL Chiper con un nivel de cifrado menor a 128 bits.

Véase también:
https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info
https://mozilla.github.io/server-side-tls/ssl-config-generator/

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante que logre tomar ventaja de esta vulnerabilidad podría generar otro certificado con la misma firma digital, permitiendo suplantar servicios, potencialmente obteniendo información confidencial. CVE-2016-2183

Mitigación:
Configure el servicio SSL para que no utilice cifrado débil.

Direcciones IP Afectadas:
172.16.7.1, 192.168.16.202, 192.168.16.215, 192.168.248.24, 192.168.248.25,192.168.248.3, 192.168.248.90.

Servicios Afectados:
csd-mgmt-port? (3071/tcp), msrdp (3389/tcp), mssql (1433/tcp), www (443/tcp), www (4443/tcp).

XI. Certificado SSL con nombre de host incorrecto

Descripción:
El certificado digital creado no corresponde con el nombre de la máquina

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Los usuarios no tendrán la total certeza de la autenticidad del sitio.

Mitigación:
Regenerar el certificado SSL de acuerdo con el nombre de la máquina

Direcciones IP Afectadas:
192.168.16.202, 192.168.16.215, 192.168.248.24, 192.168.248.25, 192.168.248.3,192.168.248.90.

Servicios Afectados:
csd-mgmt-port? (3071/tcp), msrdp (3389/tcp), mssql (1433/tcp), vcom-tunnel? (8001/tcp), www (443/tcp), www (8089/tcp).

XII. Ausencia de la firma SMB.

Descripción:
Se detecta que la firma de autenticidad del servidor SMB no se encuentra activa, lo que puede permitir un ataque de hombre en el medio.

Véase también:
http://support.microsoft.com/kb/887429
https://technet.microsoft.com/es-co/library/cc731957.aspx
http://www.nessus.org/u?74b80723
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Exposición:

Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante puede aprovechar estas fallas para realizar ataques de hombre en el medio.

Mitigación:
Refuerce el mensaje de firma del servidor SMB. Si es sobre un maquina Windows este proceso se debe realizar en la política de seguridad local o mediante la llave de registro 'HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySig nature'

Si es sobre SAMBA se debe habilitar en la bandera de Server Signing.

Direcciones IP Afectadas:
192.168.16.215, 192.168.248.24, 192.168.248.25, 192.168.248.3, 192.168.248.90.

Servicios Afectados:
cifs (445/tcp).

XIII. Suites de Cifrado SSL Débiles

Descripción:
El servicio utiliza SSL, el cual está configurado de manera que utiliza cifrado considerado como débil.

Ver también:
http://www.nessus.org/u?6527892d

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante podría explotar esta vulnerabilidad si el atacante está en la misma red física.

Mitigación:
Configure el servicio SSL para que no utilice cifrado débil. Siga las indicaciones del sitio web:
http://http://www.openssl.org/docs/apps/ciphers.html

Direcciones IP Afectadas:
172.16.7.1.

Servicios Afectados:
www (4443/tcp).

XIV. Suites RC4 de cifrado SSL/TLS con fallos (Bar Mitzvah)

Descripción:
El servicio soporta el uso de RC4 en utiliza en el protocolo TLS y el protocolo SSL. El cifrado RC4 contiene una falla al generar bytes pseudo-aleatorios reduciendo su aleatoriedad. CVE-2013-2566 CVE-2015-2808

Véase también:
http://www.nessus.org/u?217a3666
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante podría realizar ataques de recuperación de texto sin formato mediante el análisis estadístico de texto cifrado en una gran cantidad de sesiones que utilizan el mismo Texto sin formato con lo cual podría ser posible descifrar el texto transmitido afectando la confidencialidad de la información.

Mitigación:
Reconfigure la aplicación afectada para que, en la medida de lo posible, evite el uso de suites de cifrado RC4.Considere usar TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.

Direcciones IP Afectadas:
172.16.7.1, 192.168.16.202, 192.168.248.24, 192.168.248.25, 192.168.248.3, 192.168.248.90.

Servicios Afectados:
csd-mgmt-port? (3071/tcp), msrdp (3389/tcp), mssql (1433/tcp), www (443/tcp), www (4443/tcp).

XV. Vulnerabilidad en el cifrado SSLv3 Padding Oracle (POODLE)

Descripción:
El servicio con capa de cifrado SSL/TLS es afectado por una vulnerabilidad relacionada mensajes cifrados con mecanismos en modo Cipher Block Chaining (CBC).

Véase también:
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto: Medio. Mediante un ataque de hombre en el medio se puede descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos y si pueden obligar a una aplicación víctima a enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién creadas realizando un ataque de denegación de servicio (DoS) afectando la disponibilidad de la información. CVE-2014-3566

Mitigación:
Deshabilitar el soporte de la versión 3 de SSL.

Direcciones IP Afectadas:
192.168.248.24, 192.168.248.25, 192.168.248.90.

Servicios Afectados:
csd-mgmt-port? (3071/tcp), www (443/tcp).

XVI. Aplicación web potencialmente vulnerable al Clickjacking

Descripción:
El servicio web no incluye un encabezado X-Frame-Options dentro de sus respuestas HTTP. Esto permite capturar los Click que se dan en el aplicativo o página web.

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:

Medio. Un atacante podría engañar a un usuario autenticado y efectuar acciones no autorizadas en la aplicación afectada.

Mitigación:
Configure el servicio web para incluir el encabezado X-Frame-Options dentro de la respuesta del contenido publicado.

Direcciones IP Afectadas:
192.168.248.90.

Servicios Afectados:
www (443/tcp), www (80/tcp).

XVII. Uso de algoritmos de cifrado débiles SSH

Descripción:
Se ha detectado que el servicio SSH soporta el uso de mecanismos de cifrado débiles de tipo Arcfour. La documentación establecida por la RFC 4253 sugiere evitar este tipo de mecanismos de cifrado debido a una problemática que presentan con relación a las llaves de cifrado y no debería usarse más.

Véase también:
https://tools.ietf.org/html/rfc4253#section-6.3

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante puede aprovechar estas fallas para realizar ataques de hombre en el medio y así recuperar texto sin formato de un bloque de texto cifrado lo afectada la confidencialidad de la información.

Mitigación:
Configure el servicio SSH para deshabilitar los mecanismos de cifrado débiles.

Direcciones IP Afectadas:
172.16.7.1.

Servicios Afectados:
ssh (22/tcp)

XVIII. ESXi 6.5 / 6.7 XSS (Cross-Site Scripting) (VMSA-2020-0008)

Descripción:
A la versión de VMware ESXi le falta un parche de seguridad, por lo tanto, se ve afectado por una vulnerabilidad de Cross-Site Scripting (XSS) en los atributos de la máquina virtual debido a una validación incorrecta.

Véase también:
https://www.vmware.com/security/advisories/VMSA-2020-0008.html

Exposición:
Medio. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto: Medio. Un atacante autenticado con acceso para modificar las propiedades del sistema de una máquina virtual desde el interior del sistema operativo puede explotar esto, insertando código HTML relacionado con el script en las propiedades del sistema y haciendo que un usuario vea las propiedades del sistema desde ESXi Host Client, para ejecutar XSS en la sesión de un usuario. CVE-2020-3955

Mitigación:
Aplique el parche indicado según la versión de VMware instalada como lo indica el proveedor.

Direcciones IP Afectadas:
192.168.248.14

Servicios Afectados:
www (443/tcp).

XIX. El Servidor Web Transmite Credenciales de Texto sin Cifrar

Descripción:
Se evidenció la existencia de una aplicación web donde se suministra la información de usuario y contraseña de forma no cifrada (viajando en texto claro), esto potencialmente revelaría información sensible ante Sniffing (husmeo) en la red.

Exposición:
Medio. Un atacante mediante un ataque de hombre en el medio puede capturar el trafico y evidenciar en texto claro la información afectando la confidencialidad.

Impacto:
Alto. Un atacante mediante un ataque de hombre en el medio puede capturar el tráfico y evidenciar en texto claro la información afectando la confidencialidad.

Mitigación:
Corregir la publicación de formularios que soliciten información para se realice solo de forma cifrada (https)

Direcciones IP Afectadas:
192.168.248.90

Servicios Afectados:
www (80/tcp).

XX. Vulnerabilidad de CRIME del Protocolo TLS

Descripción:
El servicio tiene por lo menos una de las dos configuraciones que se conoce son necesarias para realizar un ataque CRIME:

- La compresión de SSL/TLS está habilitada.
- TLS publica una versión de SPDY anterior a la versión 4.

Véase también:
https://www.iacr.org/cryptodb/data/paper.php?pubkey=3091
https://discussions.nessus.org/thread/5546
http://www.nessus.org/u?c44d5826
https://bz.apache.org/bugzilla/show_bug.cgi?id=53219"

Exposición:
Bajo. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante que logre tomar ventaja del ataque CRIME puede descifrar ciertos tramos de texto que pueden ser confidenciales.
CVE-2012-4929, CVE-2012-4930

Mitigación:
Deshabilitar la compresión y/o el servicio SPDY.

Direcciones IP Afectadas:
192.168.16.202, 192.168.248.17, 192.168.248.24, 192.168.248.25, 192.168.248.3,192.168.248.90.

Servicios Afectados:
www (8089/tcp).

XXI. Cifrados habilitados CBC (Mode Ciphers Enabled) del servidor SSH.

Descripción:
El servicio SSH se encuentra configurado para soportar cifrado basado en encadenamiento de bloques de cifrado (Cipher Block Chaining - CBC).

Exposición:
Bajo. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante podría capturar mensajes en texto plano a partir del texto cifrado.

Mitigación:
Deshabilitar el cifrado basado en CBC y habilitar los modos de cifrado CTR o GCM.

Direcciones IP Afectadas:
172.16.7.1.

Servicios Afectados:
ssh (22/tcp)

XXII. SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Descripción:
El servicio soporta el cifrado SSL/TLS, este usa módulos Diffie-Hellman de longitud menor o igual a los 1024 bits.

Exposición:
Bajo. Se requieren ciertas condiciones para tomar ventaja de esta vulnerabilidad.

Impacto:
Medio. Un atacante que logre interceptar la conexión por medio de un ataque de hombre en el medio podría capturar el tráfico para posteriormente descifrarlo mediante análisis criptográfico.CVE-2015-4000
Mitigación:
Reconfigure el servicio para soportar únicamente módulos Diffie-Hellman de al menos 2048 bits.

Direcciones IP Afectadas:
172.16.7.1.

Servicios Afectados:
www (4443/tcp).

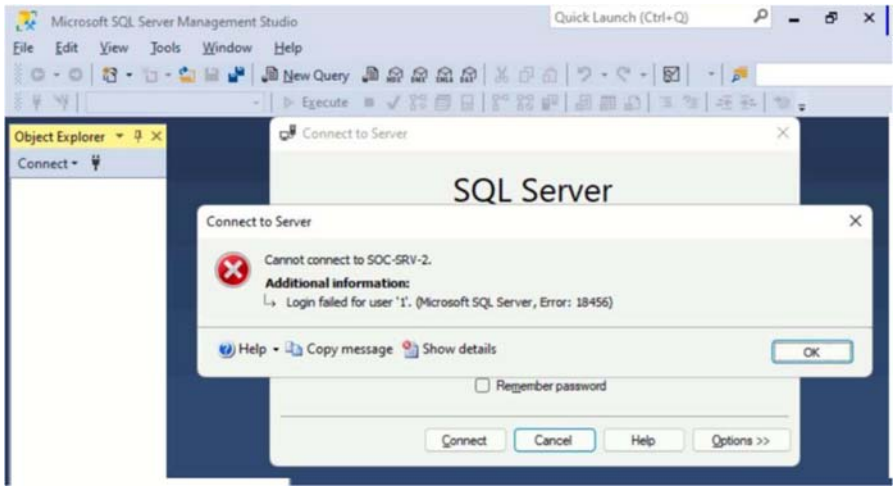
1.15.1.3 Pruebas de explotación controlada

Se realizaron las siguientes pruebas de explotación contralada según el impacto y con la previa autorización de COMPAÑÍA INTERNACIONAL DE INTEGRACIÓN S.A. Ci2

1. El equipo con IP 192.168.248.3 tiene un motor de base de datos fuera de soporte (Microsoft SQL Server 2008) y aunque no existe en la actualidad una vulnerabilidad publica que permita que un atacante tome ventaja del sistema y la base de datos, en el momento que se haga pública un mecanismo para aprovecharse del sistema, este no podrá ser parchado, en contexto se ejecutó un ataque de diccionario sobre el motor de base de datos

    a. Se validó que la base de datos permitiera la autenticación a través de la red, de acuerdo con el mensaje de error que genera la herramienta Ms SQL Management Studio en el momento de realizar una nueva conexión, tal y como lo muestra la figura XX.

Figura 14. Error emitido por Ms SQL Management Studio



Fuente: Torres, A (2023), Error emitido por Ms SQL Management Studio [Imagen]. Nota: Imagen diseñada por el autor.

b. Se lanzó un exploit desde el framework de ataque metasploit para obtener más información de la máquina y ratificar la debilidad y la versión no vigente del motor de base de datos, tal y como lo muestra la figuraXX.

Figura 15. Lanzamiento de Exploit

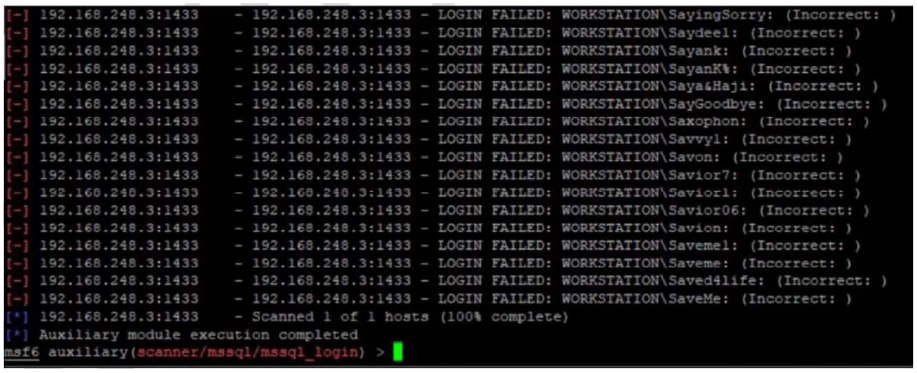
Fuente: Torres, A (2023), Lanzamiento de Exploit [Imagen]. Nota: Imagen diseñada por el autor.

c. Se ejecutó un exploit encargado de ejecutar un ataque de diccionario teniendo como base el diccionario rockyou.txt de KaliLinux, luego de dos sesiones de 8 horas cada una, se probaron 2,985,000 contraseñas posibles, finalmente no se revelo la contraseña, tal y como lo muestran las Figuras XX y XX

Figura 16. Resultado de Exploit 1

Fuente: Torres, A (2023), Resultado de Exploit [Imagen]. Nota: Imagen diseñada por el autor.

Figura 17. Resultado de Exploit 2

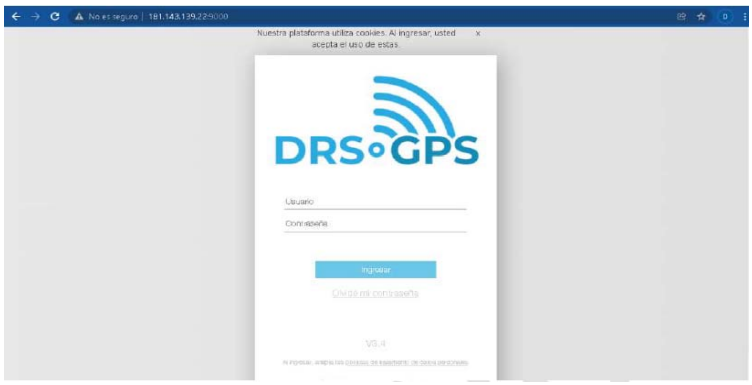


Fuente: Torres, A (2023), Resultado de Exploit 2 [Imagen]. Nota: Imagen diseñada por el autor.

2. Revisión de vulnerabilidades con Burp y pruebas manuales sobre los aplicativos webs encontrados en 181.143.139.22 (puerto 9000), 199.192.26.57 y 200.69.80.210.

    a. Se evidencia que el aplicativo http://181.143.139.22:9000/ no emplea nivel de cifrado (HTTPS), por lo que las comunicaciones están sujetas a ataques de hombre en el medio. Esto implica que un atacante que escuche el tráfico puede capturar datos sensibles como credenciales de los usuarios para luego usarlas para su beneficio. Tal como se evidencia en la Figura XX, el navegador marca la URL como no segura. Para resolver este asunto se recomienda utilizar HTTPS en vez de HTTP para evitar que los usuarios que vean el tráfico puedan capturar credenciales de usuarios u otra información sensible.

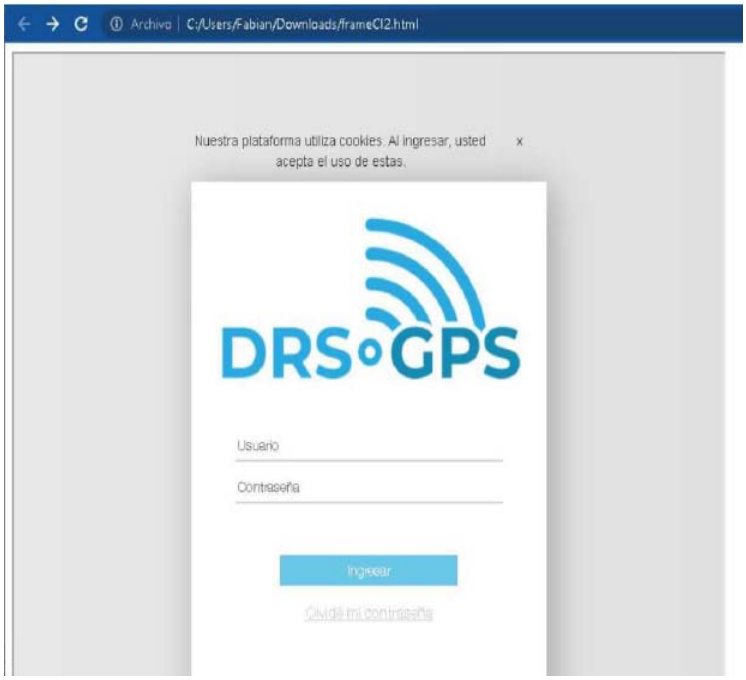
Figura 18. Mensaje del navegador por URL como no segura



Fuente: Torres, A (2023), Mensaje del navegador por URL como no segura [Imagen]. Nota: Imagen diseñada por el autor.

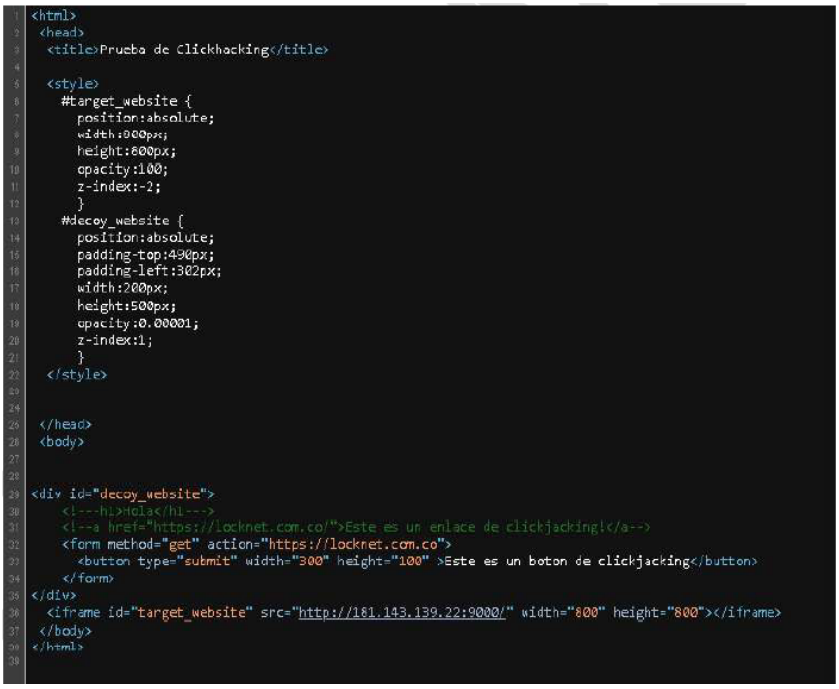
b. El aplicativo http://181.143.139.22:9000/ es propenso a Clickjacking. Lo que quiere decir que la página web puede ser puesta en un recuadro, facilitando así un ataque de phishing al engañar a un usuario al dirigirlo a un sitio malicioso que haya puesto la página de login en este recuadro y redireccionándolo a otra página. En la Figura XX se evidencia una prueba de concepto donde se ha usado de forma local un documento html para incluir el aplicativo en un recuadro. Por su parte, en la Figura XX se expone el código html detrás de la prueba de concepto, la cual, después de hacer o a Para evitar dicho ataque, se recomienda que el servidor devuelva el encabezado X-Frame-Options ya sea con el valor DENY o SAMEORIGIN según aplique.

Figura 19. Mensaje del navegador Clickjacking 1



Fuente: Torres, A (2023), Mensaje del navegador Clickjacking [Imagen]. Nota: Imagen diseñada por el autor.

Figura 20. Clickjacking 2

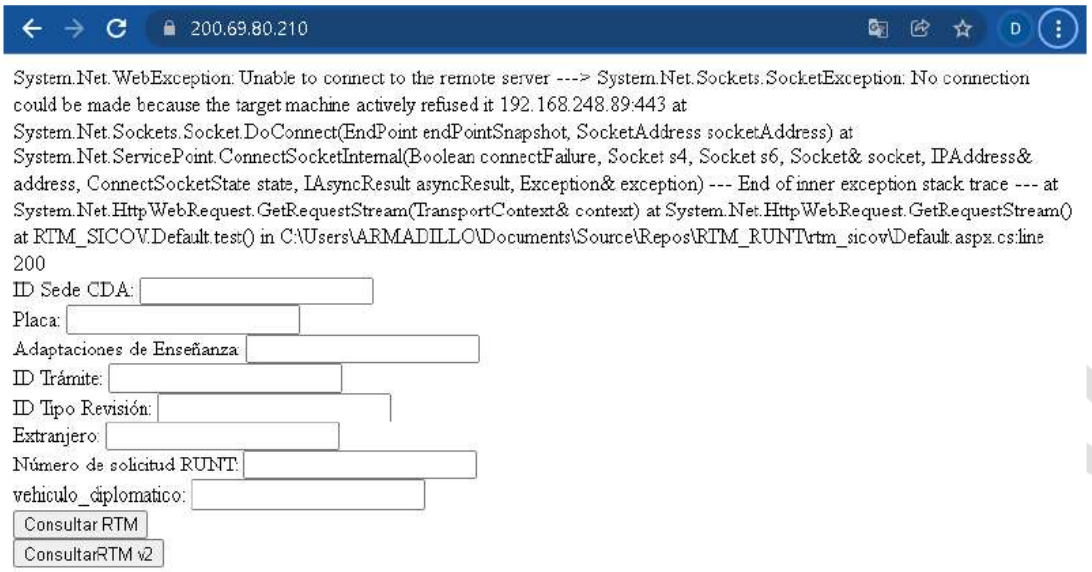


```
<html>
 <head>
  <title>Prueba de Clickhacking</title>

  <style>
    #target_website {
      position:absolute;
      width:800px;
      height:800px;
      opacity:100;
      z-index:-2;
      }
    #decoy_website {
      position:absolute;
      padding-top:490px;
      padding-left:302px;
      width:200px;
      height:500px;
      opacity:0.00001;
      z-index:1;
      }
  </style>


 </head>
 <body>


<div id="decoy_website">
    <!---h1>Hola</h1--->
    <!--a href="https://locknet.com.co/">Este es un enlace de clickjacking!</a-->
    <form method="get" action="https://locknet.com.co">
      <button type="submit" width="300" height="100" >Este es un boton de clickjacking</button>
    </form>
</div>
  <iframe id="target_website" src="http://181.143.139.22:9000/" width="800" height="800"></iframe>
 </body>
</html>
```

Fuente: Torres, A (2023), Clickjacking 2 [Imagen]. Nota: Imagen diseñada por el autor.

c. Al hacer click sobre el botón “ConsultarRTM v2”, del aplicativo https:// 200.69.80.210 se evidencia que arroja error revelador de información interna del mismo, tal como se aprecia en la Fig 25. Exposición de ruta. En este se evidencia que el aplicativo busca la dirección IP 192.168.248.89, pero no responde. Así mismo, la se revela la ruta C:\Users\ARMADILLO\Documents\Source\Repos\RTM_RUNT\rtm_si cov\Default.as. Esta evidencia muestra que no se ha realizado el respectivo manejo de dicha excepción; por lo que para dar solución a dicha vulnerabilidad y evitar que un atacante pueda hacer uso de la información revelada es necesario realizar el respectivo manejo de excepciones dentro del código y así evitar divulgar mensajes de error que revelen información sensible del aplicativo.

Figura 21. Exposición de ruta



Fuente: Torres, A (2023), Fig 25. Exposición de ruta [Imagen]. Nota: Imagen diseñada por el autor.

d. Se evidencia el uso de librerías con dependencias de librerías de JavaScript vulnerables. En las rutas /Scripts/Jquery/jquery-1.12.4.min.js y /Scripts/js/bootstrap.min.js del aplicativo http://181.143.139.22:9000.

   En la primera ruta se evidencia una versión 1.12.4.min de jquery, mientras que en la segunda se evidencia una versión 3.3.7 de Bootstrap; ambas son conocidas por tener código vulnerable en ellas. Por lo tanto, se recomienda emplear librerías actualizadas que no sean conocidas por tener vulnerabilidades en ellas.

Figura 22. Bootstrap

Fuente: Torres, A (2023), Bootstrap [Imagen]. Nota: Imagen diseñada por el autor.

1.16 DESCRIPCIÓN EJECUTIVA ANÁLISIS EJECUTADO

Se llevó a cabo un proceso de pruebas de intrusión externas e internas tipo White Box en Ci2, en donde, teniendo pleno conocimiento de las características de red y sistemas operativos de los equipos a los que se realizaron las pruebas, se busca evidenciar vulnerabilidades sobre estos sistemas. Las pruebas realizadas se limitan a evidenciar vulnerabilidades conocidas en las capas OSI 1 a 4.

Debido a los posibles efectos que pueden tener las diferentes validaciones de las vulnerabilidades encontradas, no se realiza la verificación de todas las vulnerabilidades. Únicamente se validan aquellas vulnerabilidades que al ser explotadas no causan un impacto sobre la operatividad de los equipos afectados.

Algunas vulnerabilidades mencionadas cuyo impacto puede causar la negación de servicios de la compañía, son verificadas en entornos controlados de laboratorio, evidenciando la factibilidad de realizar algún ataque por medio de las mismas vulnerabilidades. Aquellas vulnerabilidades conocidas y validadas en laboratorio son mencionadas a lo largo del documento, mas no se presentarán evidencias al respecto.

La medida asociada con el grado de cada vulnerabilidad se fundamenta en su impacto sobre la integridad, confidencialidad y disponibilidad de los servicios y la información, así como de la complejidad de explotación de la vulnerabilidad. De esta forma se cuenta con una métrica para establecer un grado de criticidad de cada vulnerabilidad

1.16.1 Convenciones

Las vulnerabilidades presentadas en este documento son calificadas de acuerdo con un grado de severidad determinado por la exposición y el impacto de estas. Esta calificación se realiza según las características inherentes a cada vulnerabilidad y al entorno particular de la red estudiada.

Grado Alto - Rojo

Las vulnerabilidades calificadas con grado alto son aquellas que cuentan con una herramienta o módulo de dominio público para tomar ventaja de ésta, para las cuales el tomar ventaja no requiere de circunstancias particulares y las implicaciones de una explotación exitosa representan un riesgo total en contra de la confidencialidad, disponibilidad e integridad del sistema afectado.

Grado Medio - Amarillo

Las vulnerabilidades calificadas con grado medio son aquellas que no cuentan con herramientas o módulos de dominio público, para las cuales el tomar ventaja de la

misma requiere de algunas circunstancias particulares o las implicaciones de una explotación exitosa representan un riesgo parcial en contra de la confidencialidad, disponibilidad o integridad del sistema afectado.

Grado Bajo - Verde

Las vulnerabilidades calificadas con grado bajo son aquellas que no representan un riesgo inmediato en contra de la confidencialidad, disponibilidad o integridad del sistema afectado. Sin embargo, estas proporcionan información valiosa para refinar ataques más sofisticados en contra de otros componentes relacionados con la vulnerabilidad en cuestión.

Los hallazgos presentados se separan principalmente de dos formas:

Se cuenta con un resumen que consolida las vulnerabilidades, sin tener en cuenta el número de ocurrencias de las mismas, con el fin de tener una visión general de cuantas existen y en qué grado se encuentran

El otro análisis se basa en la exposición de la red ante las vulnerabilidades existentes, esto es teniendo en cuenta las ocurrencias de cada una de estas, ya que entre más se repita una vulnerabilidad mayor es la probabilidad de ser explotada.

1.16.2 Metodología y descripción del proceso

La metodología utilizada en el proceso de análisis de vulnerabilidades es propia. Esta metodología utiliza las buenas prácticas de este tipo de procesos en conjunto con elementos de los lineamientos EC-COUNCIL (International Council of Electronic Commerce Consultants) y OSSTMM (Open Source Security Testing Methodology Manual).

Para las pruebas internas y externas de tipo White Box que se desarrollaron en Ci2, la metodología utilizada está compuesta por las siguientes etapas:

Reconocimiento (Reconnaissance): En esta etapa se obtiene información sobre equipos, servicios o topologías de red. La información recolectada en esta etapa puede ser utilizada posteriormente durante las pruebas.

Escaneo (Scanning): En esta etapa se realiza un barrido a lo largo de las direcciones IP consideradas como el objetivo de la prueba con el fin de determinar los puertos activos y, si es posible, los sistemas operativos de los equipos objeto de la prueba. Una vez se determinan los puertos activos en cada equipo, se realizan validaciones sobre cada puerto con el fin de determinar las posibles versiones de los servicios.

Husmeo (Sniffing): En esta etapa se usan herramientas que permitan realizar una captura del tráfico generado por los equipos objetivos durante su funcionamiento normal, con el fin de realizar un análisis pasivo de identificación de vulnerabilidades. Cabe agregar que la ejecución de las herramientas utilizadas en esta etapa está sujeta a la pertinencia técnica del escenario de su ejecución. En algunos casos la configuración presente en los dispositivos de red impide la captura de este tráfico, lo cual impide la ejecución de esta etapa.

Enumeración (Enumeration): En esta etapa se reúne toda la información recolectada en los procesos anteriores para determinar la información y datos útiles para la etapa de intrusión al sistema. Adicionalmente se pretende obtener información adicional de los equipos objeto de las pruebas mediante sondeos activos a lo largo de los servicios detectados en la etapa de escaneo.

Evaluación de Vulnerabilidades (Vulnerability Assessments): Esta etapa consiste en realizar un análisis los servicios presentes en los servicios y las aplicaciones publicadas por los puertos expuestos por los equipos objeto de la prueba con el fin de determinar la existencia de vulnerabilidades conocidas presentes en el servicio afectado.

Elaboración de Informe: Los resultados y la ejecución del proceso se sintetizan un documento físico de máxima confidencialidad.

1.16.3 Descripción Pruebas Externas

1. Alcance de las pruebas externas

Las pruebas externas realizadas se limitan a ejecutar pruebas de intrusión sobre las direcciones IP objeto de la prueba, listadas a continuación, en las capas OSI 3 a 4.

- 200.69.80.210
- 186.116.8.256
- 181.143.139.22
- 199.192.26.57

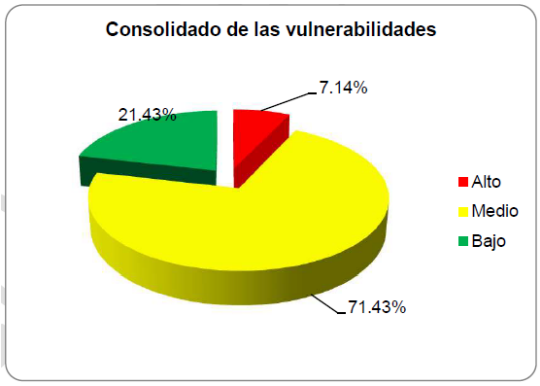
1.1 Hallazgos de las pruebas externas

Tabla 5. Vulnerabilidades unificadas

Vulnerabilidades Unificadas	
Grado	Cantidad
Alto	1
Medio	10
Bajo	3

Fuente: Torres, A (2023), Vulnerabilidades unificadas [Tabla]. Nota: Imagen diseñada por el autor.

Figura 23. Consolidado de las vulnerabilidades



Fuente: Torres, A (2023), Consolidado de las vulnerabilidades [Gráfico]. Nota: Imagen diseñada por el autor.

El grado de exposición del perímetro externo es considerado como Alto ya que estas vulnerabilidades están publicadas a internet, un atacante podría tomarse todo el tiempo necesario para lograr explotar alguna de estas vulnerabilidades y sí logra tomar ventaja de estás podría suplantar el servicio afectado u obtener información confidencial.

A continuación, se presenta un consolidado del número de vulnerabilidades por cada dirección IP evaluada, denotando el grado de exposición de la misma.

Tabla 6. Consolidado de vulnerabilidades por dirección

Dirección	Alto	Medio	Bajo
200.69.80.210	1	8	0
199.192.26.57	0	7	2
181.143.139.22	0	5	1
186.116.8.256	0	0	0

Fuente: Torres, A (2023), Consolidado de vulnerabilidades por dirección [Gráfico]. Nota: Imagen diseñada por el autor.

1.16.4 Alcance de pruebas internas

Las pruebas realizadas se limitan a ejecutar pruebas de vulnerabilidad sobre las direcciones IP objeto de la prueba, listadas a continuación, en las capas OSI 1 a 4.

- 192.168.248.14
- 192.168.16.202
- 192.168.248.3
- 192.168.248.17
- 192.168.248.90
- 192.168.248.101
- 192.168.248.25
- 192.168.248.24
- 192.168.16.215
- 172.16.7.42
- 172.16.7.1

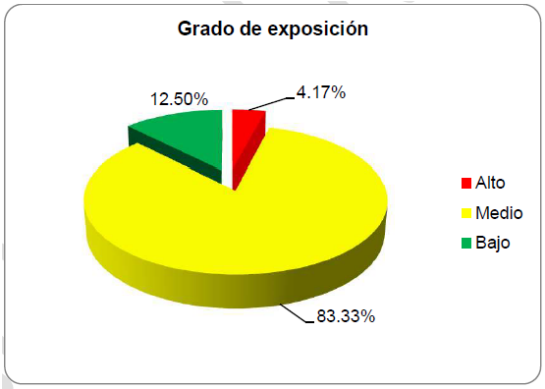
1. **Alcance de las pruebas externas**

Tabla 7. Grado de exposición

Vulnerabilidades unificadas	
Grado	Cantidad
Alto	3
Medio	15
Bajo	4

Fuente: Torres, A (2023), Grado de exposición [Tabla]. Nota: Imagen diseñada por el autor.

Figura 24. Grado de exposición



Fuente: Torres, A (2023), Grado de exposición [Gráfico]. Nota: Imagen diseñada por el autor.

Durante las pruebas a las IP objeto de la prueba se identificó:

- Vulnerabilidades de grado alto relacionadas con un motor de base de datos sin soporte (Microsoft SQL Server 2008 192.168.248.3) y un virtualizador VmWare desactualizado (ESXi 6.5.0 - 192.168.248.14).

- En su gran mayoría las vulnerabilidades de grado medio tienen que ver con las configuraciones de la capa de cifrado como certificados SSL que utilizan algoritmos Hash débiles MD2, MD4 o MD5 y SWEET32, vulnerabilidad en el cifrado SSLv3 Padding Oracle (POODLE) y el uso de TLS v1 y SSL 2 y 3. También se detectaron certificados SSL expirados y auto firmados.

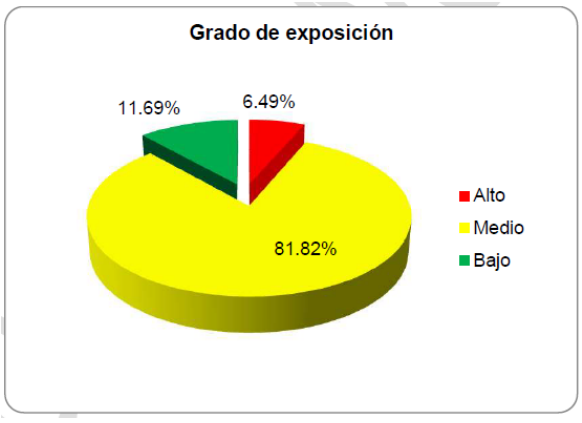
- Se evidenciaron vulnerabilidades de grado medio relacionadas con una aplicación web potencialmente vulnerable al Clickjacking, directorios webs navegables, transmisión de credenciales de texto sin cifra, la ausencia de la firma SMB y el uso de algoritmos de cifrado débiles SSH.

Tabla 8. Vulnerabilidades totales

Vulnerabilidades totales	
Grado	Cantidad
Alto	5
Medio	63
Bajo	9

Fuente: Torres, A (2023), Vulnerabilidades totales [Tabla]. Nota: Imagen diseñada por el autor.

Figura 25. Grado de exposición total



Fuente: Torres, A (2023), Grado de exposición total [Gráfico]. Nota: Imagen diseñada por el autor.

Teniendo en cuenta el número de ocurrencias de cada vulnerabilidad, el grado de exposición de los equipos evaluados se considera Alto debido a que el 6.49% de las vulnerabilidades encontradas representan un alto riesgo, también se evidencia un alto número de vulnerabilidades de grado medio encontradas.

A continuación, se presenta un consolidado del número de vulnerabilidades por cada equipo evaluado, denotando el grado de exposición de este.

Tabla 9. consolidado de vulnerabilidades

Servidor	Alto	Medio	Bajo
192.168.248.90	1	11	2
192.168.248.24	1	10	1
192.168.248.25	1	9	1
192.168.248.3	1	8	1
192.168.248.14	1	4	0
192.168.16.202	0	6	1
192.168.16.215	0	6	0
172.16.7.1	0	5	2
192.168.248.17	0	2	1
172.16.7.42	0	2	0
192.168.248.101	0	0	0

Fuente: Torres, A (2023), consolidado de vulnerabilidades [Tabla]. Nota: Imagen diseñada por el autor.

CONCLUSIONES

En el marco del ejercicio de ethical hacking y pruebas de penetración llevado a cabo para evaluar la seguridad de CI2, se identificaron diversas vulnerabilidades en sus sistemas productivos, que van desde fallos en la configuración hasta debilidades en el diseño de las aplicaciones. Adicionalmente, los ejercicios de ingeniería social pusieron de manifiesto la susceptibilidad del personal a técnicas de manipulación, revelando la necesidad urgente de entrenamientos continuos en seguridad. La evaluación integral de estas vulnerabilidades ha permitido determinar el nivel real de riesgo al que está expuesta la infraestructura tecnológica de la compañía.

El plan de remediación propuesto se destaca por su enfoque integral para mitigar las vulnerabilidades detectadas y fortalecer la seguridad global de CI2. Este plan incluye desde actualizaciones y parches hasta controles de seguridad avanzados, y su implementación contribuirá significativamente a reducir la exposición a ataques y brechas de seguridad. Además, al mejorar la postura de seguridad, CI2 no solo protege sus activos, sino que también cumple con normativas y estándares de la industria, reforzando su reputación y confianza entre clientes y socios.

Los ejercicios de ethical hacking y ingeniería social demostraron ser fundamentales para ofrecer una perspectiva realista de las amenazas enfrentadas por la organización. Esta metodología no solo reveló debilidades técnicas, sino que también destacó la importancia de preparar al personal frente a ataques basados en manipulación. Se recomienda a CI2 implementar programas continuos de formación en seguridad y realizar revisiones periódicas para mantener una defensa eficaz contra nuevas amenazas, asegurando así una mejora constante en la seguridad de su infraestructura tecnológica.

Los resultados obtenidos en estos ejercicios permitieron cumplir de manera efectiva con los objetivos planteados al inicio de la investigación, proporcionando una visión clara del estado de la seguridad informática de la compañía CI2. En primer lugar, la evaluación del nivel de riesgo de CI2 involucró un proceso exhaustivo de recopilación de datos mediante pruebas de ingeniería social, análisis de vulnerabilidades en los sistemas productivos y evaluaciones de exposición a través de herramientas de penetración. Este enfoque integral permitió caracterizar con precisión el nivel de riesgo, que se determinó como [bajo/medio/alto], basado en estándares reconocidos en la industria de la ciberseguridad. Esta evaluación ofrece una base sólida para entender las áreas críticas que requieren atención prioritaria dentro de la infraestructura tecnológica de la compañía.

En cuanto a la ejecución de pruebas de ingeniería social y phishing, estas fueron fundamentales para medir la susceptibilidad del personal de CI2 a posibles ataques dirigidos. Se llevaron a cabo pruebas que simularon ataques reales, logrando obtener una tasa de éxito en los intentos de ingeniería social, y una tasa de clics en correos de phishing. Estos resultados revelan importantes áreas de mejora en la capacitación del personal, lo que es esencial para fortalecer la defensa contra amenazas que explotan el factor humano.

La identificación de vulnerabilidades en los sistemas productivos fue otra contribución clave de este trabajo. Mediante un análisis exhaustivo, se descubrieron vulnerabilidades críticas, incluyendo [XSS, inyección SQL, etc.], las cuales fueron categorizadas según su severidad. Estos hallazgos proporcionan una comprensión detallada del estado actual de la infraestructura tecnológica y permiten priorizar las acciones correctivas necesarias para proteger los activos críticos de la compañía.

Por otro lado, la evaluación del nivel de exposición de los sistemas en producción fue posible gracias a la utilización de diversas herramientas y técnicas de penetración. Las pruebas realizadas demostraron que los sistemas de CI2 tienen un nivel de exposición [alto/bajo], debido a factores como [falta de actualización de software, configuraciones erróneas, etc.]. Esta evaluación ayudó a identificar las áreas que requieren una intervención inmediata para minimizar los riesgos de explotación por parte de actores maliciosos.

Finalmente, con base en los resultados obtenidos, se generó un plan de recomendaciones de remediación detallado. Este plan aborda las vulnerabilidades identificadas y propone medidas concretas como [la implementación de políticas de seguridad más estrictas, la actualización de sistemas, capacitación del personal, etc.]. Si se implementan adecuadamente, estas recomendaciones tienen el potencial de reducir significativamente el nivel de riesgo, asegurando la infraestructura tecnológica de CI2 y mejorando su postura general de seguridad.

En conclusión, los resultados de este trabajo confirman que la infraestructura tecnológica de CI2 presenta un nivel de riesgo, y que las recomendaciones propuestas son fundamentales para mejorar su seguridad informática. Cada uno de los objetivos establecidos ha sido abordado de manera integral, asegurando que las fases del proyecto estén alineadas y que las conclusiones y sugerencias finales estén respaldadas por hallazgos concretos y relevantes.

La relevancia de esta propuesta radica en su capacidad para anticipar y mitigar riesgos antes de que se materialicen en incidentes de seguridad significativos. Los resultados obtenidos subrayan la necesidad de una estrategia de seguridad proactiva, que no solo se enfoque en la tecnología, sino también en la concienciación y preparación del personal. Las recomendaciones derivadas de este ejercicio proporcionan una hoja de ruta clara para mejorar las defensas y educar a los empleados sobre las tácticas utilizadas por los atacantes.

Con el objetivo de ejecutar pruebas de ingeniería social y phishing a una muestra de personal de la compañía, se llevó a cabo una evaluación exhaustiva para determinar el nivel de conciencia y preparación del personal frente a posibles amenazas de ingeniería social. Estas pruebas proporcionaron información valiosa sobre las vulnerabilidades humanas en el entorno de seguridad, al revelar cómo respondían y se comportaban los empleados ante intentos de manipulación. Se identificaron áreas específicas donde los empleados podrían ser más susceptibles a ataques de este tipo, lo que resaltó la necesidad de programas de capacitación personalizados y de concientización para mejorar la seguridad en toda la organización.

Al identificar vulnerabilidades existentes mediante análisis en los sistemas productivos permitió realizar un escrutinio detallado de la infraestructura tecnológica de la compañía. El análisis de vulnerabilidades reveló puntos críticos de exposición y posibles puntos de explotación en los sistemas en producción. Esta evaluación proporcionó una visión clara del estado actual de seguridad, permitiendo a la organización comprender las amenazas potenciales y los riesgos asociados con cada vulnerabilidad identificada.

Al mismo tiempo, la evaluación del nivel de exposición de los sistemas en producción con diferentes pruebas y herramientas de penetración ofreció una visión más profunda de las debilidades de seguridad presentes en la infraestructura tecnológica. La realización de pruebas y herramientas de penetración permitió identificar áreas específicas de vulnerabilidad, incluyendo configuraciones incorrectas, posibles brechas en la protección y áreas que requerían mejoras de seguridad inmediatas. Estos hallazgos fueron esenciales para fortalecer las defensas y reducir el riesgo de explotación por parte de actores malintencionados.

Además, la diversidad de vulnerabilidades identificadas en los sistemas evaluados destacó la necesidad de generar un plan de recomendaciones de remediación adaptado. Este plan considerará la criticidad de cada vulnerabilidad y su impacto potencial en la seguridad de los sistemas. Priorizará las acciones de remediación en función del riesgo asociado a cada vulnerabilidad, lo que permitirá abordar los riesgos más significativos de manera efectiva y sistemática.

En conjunto, estas conclusiones derivadas del análisis integral de seguridad proporcionan una base sólida para desarrollar e implementar medidas correctivas específicas. El objetivo final es fortalecer la postura de seguridad de la organización y proteger sus activos críticos frente a las amenazas en constante evolución. La combinación de pruebas de ingeniería social, análisis de vulnerabilidades y evaluación de exposición ha proporcionado una visión completa de los desafíos de seguridad y ha guiado la formulación de estrategias de remediación efectivas y adaptadas a las necesidades específicas de la organización.

Estos esfuerzos no solo buscan mitigar las vulnerabilidades existentes, sino también mejorar la conciencia en seguridad y fortalecer las defensas en todos los niveles de la organización. Al implementar un plan de recomendaciones de remediación basado en un enfoque proactivo y centrado en el riesgo, la compañía está preparada para enfrentar y responder de manera efectiva a las amenazas de seguridad emergentes. La continuación de estas prácticas garantizará la protección continua de los activos críticos y la resiliencia ante las cambiantes condiciones del entorno de ciberseguridad.

RECOMENDACIONES

Mejorar la Configuración del Cortafuegos: Reforzar la configuración del cortafuegos para reducir la exposición a posibles ataques externos. Esto incluye la revisión y actualización de reglas, así como la implementación de filtrado más estricto para limitar la superficie de ataque.

Implementar Detección Proactiva de Intrusiones: Introducir sistemas avanzados de detección de intrusiones para monitorear y analizar activamente el tráfico en busca de patrones anómalos. Esto permitirá una respuesta más rápida y eficaz a cualquier intento de penetración.

Realizar Auditorías Regulares de Seguridad: Establecer un programa de auditorías de seguridad regulares para evaluar de manera continua las vulnerabilidades en los sistemas productivos. Esto garantizará una identificación temprana de cualquier nueva vulnerabilidad y una respuesta proactiva.

Implementar Actualizaciones y Parches de Forma Oportuna: Establecer un proceso robusto para la aplicación oportuna de parches y actualizaciones en sistemas productivos. Esto reducirá la ventana de vulnerabilidad y fortalecerá la seguridad frente a amenazas conocidas.

Personalizar Programas de Capacitación en Seguridad: Desarrollar programas de capacitación personalizados para abordar las vulnerabilidades específicas identificadas. Esto incluirá la concientización sobre prácticas seguras y la promoción de una cultura de seguridad en toda la organización.

Establecer un Grupo de Respuesta a Incidentes: Crear un equipo dedicado de respuesta a incidentes para manejar de manera efectiva las vulnerabilidades identificadas. Este grupo debería estar equipado para investigar, contener y remediar rápidamente cualquier incidente de seguridad.

Implementar Escaneos de Vulnerabilidades Periódicos: Establecer escaneos regulares de vulnerabilidades en toda la infraestructura para identificar nuevas vulnerabilidades y evaluar la efectividad de las medidas de seguridad implementadas. Esto permitirá una acción proactiva ante posibles amenazas emergentes.

Desarrollar Políticas de Seguridad y Procedimientos: Formular y documentar políticas de seguridad claras y procedimientos detallados basados en las vulnerabilidades identificadas. Esto proporcionará pautas específicas para el personal sobre cómo abordar y mitigar riesgos de seguridad, estableciendo una base sólida para la gestión de la seguridad.

BIBLIOGRAFÍA

ANLEY Chris, HEASMAN, John, LINDNER, Felix, RICHARTE, Gerardo. The Shellcoder's Handbook: Discovering and Exploiting Security Holes [en línea]. 2 ed. USA: Wiley, 2007. Disponible en: https://www.amazon.com/Shellcoders-Handbook-Discovering-Exploiting-Security/dp/047008023X

ENGEBRETSON, Patrick. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy [en línea]. 2 ed. USA: Elsevier, 2013. Disponible en: https://books.google.com/books/about/The_Basics_of_Hacking_and_Penetration_Te.html?id=69dEUBJKMiYC

ERICKSON Jon. Hacking: The Art of Exploitation [en línea]. USA: No Starch Press, 2003. Disponible en: https://books.google.com.co/books/about/Hacking.html?hl=es&id=JcpOJg1ZjBQC&redir_esc=y

KENNEDY, David. O'GORMAN, Jim. KEARNS, Devon y AHARONI, Mati. The Metasploit: The Penetration Tester´s Guide [en línea]. 2 ed. USA: No Starch Press, 2011. Disponible en: https://www.google.com.co/books/edition/Metasploit/T9HKgEOCYZEC?hl=es&gbpv=1&dq=Metasploit:+The+Penetration+Tester%27s+Guide&printsec=frontcover

McNab, Chris. Network Security Assessment: Know Your Network [en línea]. 3 ed. USA: O'Reilly Media, Incorporated, 2017. Disponible en: https://books.google.com.co/books/about/Network_Security_Assessment.html?id=PtbRoQEACAAJ&redir_esc=y

MITNICK, Kevin D y SIMON, William L. The Art of Deception: Controlling the Human Element of Security [en línea]. USA: Wiley, 2002. Disponible en: https://books.google.com.co/books/about/The_Art_of_Deception.html?id=VR_aVP0KKh8C&redir_esc=y

PINTO, Marcus y STUTTARD, Dafydd. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws [en línea]. 2 ed. USA: John Wiley & Sons, 2011. Disponible en: https://books.google.com/books/about/The_Web_Application_Hacker_s_Handbook.html?id=jN6cDprdnd0C

PINTO, Marcus y STUTTARD, Dafydd. The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws [en línea]. USA: John Wiley & Sons, 2008. Disponible en: https://books.google.com.co/books/about/The_Web_Application_Hacker_s_Handbook.html?id=_EhvBGsWi6AC&redir_esc=y

WALKER, Matt. CEH Certified Ethical Hacker All-in-One Exam Guide [en línea]. 5 ed. USA: McGraw Hill Professional, 2021. Disponible en: https://books.google.com/books/about/CEH_Certified_Ethical_Hacker_All_in_One.html?id=EuBIEAAAQBAJ

WEIDMAN, Georgia. Penetration Testing: A Hands-On Introduction to Hacking [en línea]. USA: No Starch Press, 2014. Disponible en: https://books.google.com.co/books/about/Penetration_Testing.html?id=T_LlAwAAQBAJ&redir_esc=y

"FÍSICOS"

HADESS, Red Team Guides, NO date, USA

MANK, CEH Summarized, Simple Exam Guide, 2021

MESSIER, Ric. Certified Ethical Hacker Version 11. 2 ed. USA: John Wiley & Sons. 2021, 208 p. ISBN: 9781119824510.

PERROTT, Sara. Windows Server 2022 & PowerShell All-in-One. 1 ed. USA: 2022, 749 p. ISBN: 9781119867821

SAAD, Elie. Web Security Testing Guide v4.2, owasp.org,

SINGH, Glen D. The Ultimate Kali Linux Book. 2 ed. USA: Packt Publishing. 2022, 742 p. ISBN: 9781801818933