DISEÑO DE PROCEDIMIENTOS DE SEGURIDAD BASADOS EN PRUEBAS DE PENTESTING APLICADAS A LA EMPRESA CJT&T INGENIERÍA DE SOFTWARE

MIGUEL ANGEL LÓPEZ PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO, COLOMBIA
2017

DISEÑO DE PROCEDIMIENTOS DE SEGURIDAD BASADOS EN PRUEBAS DE PENTESTING APLICADAS A LA EMPRESA CJT&T INGENIERÍA DE SOFTWARE

MIGUEL ANGEL LÓPEZ PARRA

Proyecto Aplicado

Asesor de Proyecto:
Juan Jose Cruz Garzón
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO, COLOMBIA
2017

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma de presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Ciudad y fecha (día, mes, año)

DEDICATORIA

Tras este largo camino lleno de contratiempos y que ha requerido un gran esfuerzo quiero brindar un especial reconocimiento a aquellas personas que de una u otra manera han acompañado con su granito de arena todo este proceso para lograr alcanzar una nueva meta en mi vida.

Por tanto, mi dedicatoria en primer lugar a Dios por darme las fuerzas para seguir adelante a pesar de todos los impases que se han presentado en el transcurso de este tiempo, y que me permitieron fortalecer mi carácter, mejorar mi criterio y tomar las mejores decisiones.

También se lo dedico a mis padres, por su preocupación, consejos y apoyo incondicional, por esas palabras de aliento en el momento preciso y por alentarme a continuar mis estudios ya que como siempre dicen la educación es el regalo más grande que me podrían brindar.

Finalmente, a toda mi familia por su amor y calidez que han sido mi motivación constante en los momentos difíciles.

AGRADECIMIENTOS

Resulta complicado identificar a todos aquellos actores que han sido participes de todo este proceso formativo, así como del planteamiento y desarrollo de este proyecto. Sin embargo, a todos aquellos que no podría nombrar les doy gracias de la manera más sincera.

Ahora, en primer lugar, infinitas gracias a mi Universidad y sus docentes, por brindarme la oportunidad de realizar mis estudios a distancia, por las grandes enseñanzas tanto profesionales como personales, por la paciencia y por la gran disposición para escuchar mis dudas e inquietudes, por que siempre es posible ser mejor.

Gracias a los consejeros académicos Alicia Paredes, Myriam Martinez y Edgardo Mafla, quienes siempre han estado pendientes de todas las situaciones e inconvenientes que pudieran surgir y han estado prestos a brindarme alternativas y soluciones.

Por último, gracias a la empresa CJT&T Ingeniería de Software, a los Ingenieros Juan Carlos Torres y Miguel Angel Tovar y a todos los compañeros de trabajo, quienes aceptaron amablemente proveer los recursos de la organización para poder aplicar mi proyecto. Por su gran disposición y colaboración continua, por su confianza y tiempo nunca podré hacer lo suficiente para retribuirles todo lo que hicieron por mí.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

La dinámica actual exige que las organizaciones hagan uso de la mayor cantidad de recursos tecnológicos que estén en sus posibilidades, todo con el fin de mejorar sus procesos internos. Sin embargo, dada la exposición de estos a través de Internet e Intranet, y teniendo en cuenta que la información es el recurso más valioso y su pérdida sería crítica se hace necesario la evaluación de aquellas medidas de seguridad de los sistemas.

Así, partiendo de la anterior premisa, se propone la realización de un Test de penetración teniendo como meta establecer un diagnóstico certero sobre el estado de la seguridad en la organización a través de pruebas ofensivas, que simulen el accionar de un atacante en búsqueda de puntos sensibles para aprovecharse de las debilidades encontradas en la infraestructura física, lógica y componente social.

Así, a pesar de que no existe un consenso claro sobre las etapas que comprenden este proceso, se ha decidido tomar como base la aplicación del Penetration Test Execution Standard (PTES) con el único fin de obtener resultados confiables. Las fases llevadas a cabo se indican a continuación:

- **Fase de planeación y preparación:** Durante esta fase se realiza un intercambio de información continuo entre los actores involucrados en la realización de las pruebas. Es fundamental establecer un acuerdo sobre las personas que estarán a cargo de las pruebas, aspectos legales, fechas de entrega, tiempo que tomará la ejecución y los privilegios requeridos. Asimismo, una vez identificados estos aspectos clave se planteará un alcance real y se informará la metodología a seguir.

- **Fase de Evaluación:** Comprende la ejecución de las pruebas comprendiendo la recolección de la información y el análisis de vulnerabilidades para su posterior explotación.

- **Fase de conclusión:** Reporte sobre las pruebas realizadas, así como los hallazgos encontrados, acompañados de recomendaciones para su tratamiento de acuerdo a las condiciones del sistema evaluado.

En apoyo a la fase de conclusión de las pruebas realizadas, se diseñan políticas de seguridad aplicadas al contexto de la organización que contengan las actividades necesarias para velar por la protección de los recursos físicos y lógicos con sus respectivos activos de información esenciales. Posterior a ello, se definen aquellos procedimientos de seguridad que indican como se va a materializar lo establecido en estas políticas.

INTRODUCCIÓN

CJT&T Ingeniería de Software es una empresa que por más de 10 años se ha encargado del desarrollo e implantación exitosa de proyectos informáticos a la medida de las organizaciones.

Así, la tecnología es su principal aliado en el quehacer diario de todos los que hacen parte de la empresa. Sin embargo, esta es un arma de doble filo, ya que debido al tipo de actividades que se ejercen, se almacena un gran volumen de información en formatos digitales. Esta información constituye el activo más valioso y crítico de la empresa, y su alteración o pérdida podría ocasionar grandes afectaciones a nivel operativo. Por esta razón, y en virtud de lo establecido tanto en el esquema de la certificación IT Mark como en otras posibles certificaciones con mayor exigencia en el apartado de seguridad, se ha visto la pertinencia de aplicar un Hacking Ético con el fin de establecer un diagnóstico a través de una evaluación integral desde diferentes perspectivas y niveles que incluyan una revisión detallada sobre aquellos activos físicos y lógicos, entre otros.

Para esto, se partirá desde una planificación con la organización que servirá para establecer las pautas de realización de las pruebas dejando en claro aspectos jurídicos, puntos clave sobre el uso de los activos de la empresa, tipos de pruebas que se realizarán y privilegios necesarios para ello. Posteriormente, se procederá a realizar la evaluación tomando como base el estándar PTES desde los componentes aplicables de común acuerdo con la organización. Una vez se logren completar las pruebas, se procede a realizar un reporte sobre estas y un resumen ejecutivo que permita conocer cuales fueron los hallazgos de mayor impacto.

Una vez las pruebas sean completadas, los resultados serán de mucha importancia para continuar con el diseño y planteamiento de políticas de seguridad que integrarán los puntos más relevantes para la protección de los activos con que actualmente cuente la empresa y sobre aquellos que se proyectan integrar.

Finalmente, se redactarán unos procedimientos que partan de las políticas definidas con los cuales se instaurarán procesos que deberán ser socializados con todos los recursos humanos de la empresa con el fin de que estos sean efectivos y aplicados en todo momento.

1. TITULO

Diseño de Procedimientos de Seguridad basados en pruebas de Pentesting aplicadas a la empresa CJT&T Ingeniería de Software.

Área: Seguridad Informática – Pruebas de Pentesting.

2. DEFINICIÓN DEL PROBLEMA

2.1. ANTECEDENTES DEL PROBLEMA

CJT&T Ingeniería de Software es una organización que desde sus inicios ha buscado satisfacer la necesidad de sus clientes mediante productos de alta calidad a través de desarrollos a la medida. Debido a esto, en su trayectoria de más de 10 años de operación ha existido la necesidad de ir acumulando información que con el pasar del tiempo ha pasado por distintos medios de almacenamiento tanto físicos como digitales. Asimismo, a medida que la demanda iba incrementándose, se ampliaban los espacios de interacción con empleados y clientes a través de plataformas en Internet y la Intranet como Visual Studio Team Services, TFS, mesas de ayuda con Mantis, Sharepoint, entre otros. Además, es un hecho que el uso de mensajería instantánea y correo electrónico son frecuentes como herramientas indispensables para la operación de la empresa día a día.

Así, en la actualidad se ha podido identificar que no existen medidas de seguridad documentadas que puedan brindar un tratamiento adecuado sobre las interacciones que se realizan con la información de manera cotidiana. Además, existe conciencia sobre posibles riesgos como fugas o pérdida de información que han podido presentarse en alguna ocasión debido a continuas averias en los equipos de cómputo. Esto, en conjunto con la realidad de una continua interacción con los clientes donde existen intercambios de información habituales ha replanteado el concepto de seguridad para establecerlo como el gran protagonista aplicando el Pentesting para materializar políticas y procedimientos que serán la base para la protección de aquellos elementos que son de máximo interés para la organización.

2.2. FORMULACIÓN DEL PROBLEMA

¿Son los mecanismos de protección implementados por la empresa CJT&T Ingeniería de Software suficientes para evitar el impacto de los ataques informáticos perpetuados sobre los activos de información organizacionales?

2.3. DESCRIPCIÓN DEL PROBLEMA

CJT&T Ingeniería de Software es una empresa que ofrece soluciones tecnológicas de calidad a sus clientes a través el desarrollo e implementación de proyectos informáticos. Así, como empresa de tecnología en la búsqueda de mejorar la eficiencia en sus procesos desarrolla sus tareas cotidianas valiéndose de Hardware

y Software responsables de la generación de grandes volúmenes de datos, insumo para la toma de decisiones que pueden ser transmitidos a través de diferentes medios a las áreas que respondan al contexto y necesidad de la misma. Sin embargo, los activos organizacionales sensibles no son protegidos a través de procesos puntuales, mantenibles y escalables lo cual podría representar un alto peligro de ser el objetivo principal de los delincuentes aprovechando algún descuido para efectuar ataques informáticos. Cualquier riesgo o amenaza, debe ser tenida en cuenta, para garantizar un sistema seguro y mantener el impacto ocasionado al mínimo, estableciendo parámetros que permitan prevenir y detectar los posibles ataques o en caso de que estos ya se estén perpetrando se tenga un plan de apoyo.

En este sentido será de gran utilidad la aplicación de pruebas de penetración comprendiendo sus servicios y Metodología de trabajo. El compendio de pruebas de Hacking Ético consiste en la Evaluación integral y detección temprana de fallas de seguridad en los sistemas informáticos de la organización que contrata este tipo de servicios. Además, se busca proveer el perfil de las personas a cargo de esta importante tarea donde se indiquen sus fortalezas y las actividades asignadas como fuente informativa y garantía de veracidad al contar con personal capacitado que brinde confiabilidad a los resultados. Una vez las pruebas finalicen se proveerá de un resumen de hallazgos encontrados previamente documentados donde se incluyan soluciones conducentes que permitan corregir y prevenir los fallos detectados.

Además, será necesario valorar la implementación de políticas como un documento base de la seguridad en la empresa, definiendo responsabilidades, requisitos, funciones y normas para que los empleados tengan una guía que dirija sus acciones y estén enterados sobre todo lo que éstas implican. Por otro lado, no solo se trata de la formulación de políticas o directivas, sino también de la conciencia que se debe generar a los empleados, lo cual se puede lograr estableciendo un canal de comunicación permanente. Las políticas serán puestas en marcha a través de procedimientos verificables y de calidad que determinen la forma en la cual se garantiza la protección sobre los activos de la organización.

El fin principal es mitigar la problemática de seguridad para garantizar que se cumpla a cabalidad con los conceptos prioritarios de confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

3. JUSTIFICACIÓN

La incesante cantidad de delitos relacionados con la seguridad de la información ha obligado a un crecimiento en la capacitación de profesionales especializados en dicha área, con lo cual se pretende obtener los conocimientos sobre el cómo operan los delincuentes y las técnicas que se utilizan para realizar su cometido. Por tanto, las organizaciones han reflexionado sobre este gran riesgo y han buscado en los expertos de esta rama la solución para establecer un mayor control sobre la seguridad en toda su infraestructura tecnológica.

CJT&T Ingeniería de Software pretende alcanzar la certificación IT Mark para el año 2016 con el fin de mejorar sus procesos de negocio, técnicos y servicio al cliente. En este contexto, la Gestión de la Seguridad de la Información es un pilar fundamental para alcanzar el objetivo. Por esta razón, como medida de apoyo hacia esta meta se busca la aplicación de una metodología de Hacking Ético para simular mediante la ejecución de fases consecutivas posibles escenarios de ataque para identificar cuáles son las fallas de los sistemas y proceder a actuar en consecuencia de todos los resultados una vez se ha logrado la infiltración.

En este punto, es importante comprender que los riesgos no solo provienen de amenazas externas, sino que también pueden proceder de personas autorizadas que se encuentran contiguas al entorno objetivo. Por tanto, la confianza no es una opción, se deben evaluar todos los blancos sensibles para evitar que el atacante cumpla su cometido y obtenga aquellos activos que podrían significar la afectación en la productividad de la organización en materia de reputación, política, economía o incluso la afectación del personal. Los peligros son variados y la exposición severa es evitable; por tanto, las víctimas de incidentes pueden impedir la vulneración de la seguridad informática siguiendo precauciones oportunas. De esta manera, no se tendrá que lamentar la fuga de información, acceso no autorizado, pérdida de datos, entre otros.

El Hacking Ético permitirá determinar el nivel de seguridad de los sistemas presentes en una organización, con el fin de establecer la facilidad que tendría un atacante para acceder y llevarse elementos sensibles de la empresa. Es decir, brinda un panorama para conocer la situación real de los sistemas e implementar posteriores mejoras verificando cuáles son los mecanismos de seguridad operativos. Los resultados recopilados permitirán formular recomendaciones que sean convenientes y aplicables. De ahí que, posteriormente se generan procedimientos de seguridad acordes a la situación particular las cuales serán fundamentales para mantener todos los activos organizacionales a salvo de los peligros detectados.

Es por esto que mediante todo el proceso de investigación realizado se establecerá la necesidad e importancia de adoptar medidas de seguridad apropiadas y

establecer buenas prácticas en la administración de sistemas que parametricen la seguridad y hagan que los sistemas sean menos vulnerables y estén blindados desde la perspectiva de problemas generales y específicos detectados. Lo anterior brinda certeza a nivel interno y desde la perspectiva de clientes y proveedores de un factor diferenciador donde se promueve la seguridad como un pilar fundamental en el quehacer diario que se encuentra en continuo mejoramiento y evolución.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

- Diseñar procedimientos de seguridad eficientes que permitan establecer acciones de mitigación y contención mediante el resultado de pruebas de Pentesting para la solución de problemas de seguridad de la empresa CJT&T Ingeniería de Software

4.2. OBJETIVOS ESPECÍFICOS

1. Recolectar información a nivel organizacional, de talento humano e infraestructura tecnológica que sea insumo para las fases posteriores del Penetration Test, permitiendo generar una mayor cantidad de escenarios de ataque asumiendo la perspectiva de un atacante real.

2. Identificar el valor de los equipos que pueden ser blanco de un ataque informático, comprobando la sensibilidad de los datos almacenados y su grado de relación con otros equipos o con la red misma.

3. Documentar las herramientas necesarias para la ejecución de un Penetration Test con el fin de facilitar el cumplimiento de los resultados esperados al final de cada una de sus fases.

4. Descubrir problemas de seguridad en la organización a través de la detección de vulnerabilidades sensibles de explotación para irrupción en un sistema informático.

5. Diseñar políticas de seguridad para la implementación de mejoras sustanciales que sean fuente de soluciones efectivas para reducir la probabilidad de intrusiones abusivas.

6. Elaborar un resumen ejecutivo en un lenguaje sencillo que sumarice los hallazgos producto de las pruebas realizadas con el fin de generar interés en la gerencia sobre los problemas de seguridad encontrados en la organización.

5. MARCO REFERENCIAL

5.1. MARCO TEÓRICO

5.1.1. Antecedentes del Hacking Ético: Cuando se habla de Hacking ético o pruebas de penetración es muy probable que muchas personas se ubiquen exclusivamente en la era moderna. Aquí y ahora, los avances tecnológicos proporcionan al hombre dispositivos inteligentes, servicios automáticos, prestaciones que nunca se llegó a imaginar y que son posibles debido a toda una infraestructura física y lógica detrás del telón. Sin embargo, producto de la modernización surgen amenazas y riesgos que buscan tomar el control de aquellos elementos de propiedad ajena con gran valor; a éstos se les llama activos esenciales[1]. Así, como medio de prevención, con objetivos netamente defensivos, el Hacking ético se ha preocupado por determinar qué tan protegido está un sistema para que el titular tome las medidas que sean necesarias con el fin de evitar un ataque ofensivo y destructivo.

Así, a pesar de que el término originalmente fue inventado por la IBM en el año 1995[2], el problema data de muchos años atrás donde se han construido soluciones con el fin de mejorar el tema de la seguridad, por ejemplo:

- En 1932, se reporta el primer hecho conocido de hacking en el cuál se logra romper la máquina alemana de código morse criptográfico conocida como “Enigma”. Entonces, en 1939 el “bombe” se convierte en la primera máquina de Hacking ético, la que fue usada por los británicos para ayudar a descifrar mensajes alemanes durante la segunda guerra mundial[3].

- Para el año 1970, la USAF organiza equipos de expertos, conocidos como tiger teams para evaluar la seguridad de sus sistemas. El patrocinio tenía como meta que estos grupos intenten superar las defensas de los sistemas de computadores en un esfuerzo por descubrir y eventualmente corregir, fallos de seguridad[4].

---

[1] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT versión 3 (idioma español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1: Método. Disponible en: <http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf>

[2] HACK STORY. Hackstory.es El fin de la vieja escena. Disponible en: < http://hackstory.net/Hackstory.es_El_fin_de_la_vieja_escena#cite_note-33>

[3] WIKIWAND. Enigma Machine. Disponible en: < http://www.wikiwand.com/en/Enigma_machine>

[4] KHAN, Dawood. The Most In-depth Hacker’s Guide. Disponible en: <https://books.google.com.co/books?id=sAwiCwAAQBAJ&pg=PA83&lpg=PA83&dq=1971+usaf+tiger+team+hacking&source=bl&ots=-

- Otro hecho importante ocurrió en el año 1974. En aquel entonces, Multics era considerado como el Sistema Operativo más seguro. Así, la fuerza aérea de los Estados Unidos organizó uno de los primeros hacking éticos, realizando análisis de vulnerabilidades para evaluar la seguridad del S.O. encontrando que aunque era mejor que los demás, tenía vulnerabilidades de seguridad referentes a software y hardware[5].

Posterior al año donde se acotó el término que hoy es bien conocido, se presentaron algunos cambios buscando generar un marco de trabajo más organizado sobre este tipo de pruebas lo que ha permitido que se ofrezca un servicio de mayor calidad.

- La liberación de SATAN en 1995 por Dan Farmer y Wietse Venema claramente se convertiría en un gran acontecimiento. Este escáner de vulnerabilidades, se convertiría rápidamente en una popular herramienta de hacking.

- OWASP es fundada en el año 2001[6] como una comunidad preocupada por la seguridad en aplicaciones web. Es hasta el año 2003, donde esta comunidad impacta al mundo liberando la primera guía para ayudar a enseñar las mejores prácticas aplicadas a un Penetration Testing[7].

- Por último y no menos importante, el 2009 trae un gran acontecimiento: la creación del PTES (Penetration Testing Execution Standard) en respuesta al gran crecimiento de negocios referentes al Hacking ético. Su contenido ofrece a los proveedores de servicios de seguridad un lenguaje común para realizar sus pruebas[8].

Así, es claro que la preocupación por evaluar la seguridad de los sistemas no es una inquietud propiamente reciente, sino que ha conllevado todo un proceso evolutivo a lo largo de la historia donde ha reflejado la preocupación de las organizaciones por prevenir daños catastróficos a sus activos, de ahí que acciones oportunas permitirán mitigar o tratar cualquier tipo de inconveniente que sea encontrado producto de estas pruebas.

BD4fgD0QY&sig=7le5prZjpb6CVJCaFO2VZererd8&hl=es&sa=X&ved=0ahUKEwiUnPeWzs_LAhWLlR4KHUkBAnsQ6AEIJzAB#v=onepage&q=1971%20usaf%20tiger%20team%20hacking&f=false>

[5] BODHANI, Aasha. Ethical hacking: bad in a good way. Disponible en: < http://eandt.theiet.org/magazine/2012/12/bad-in-a-good-way.cfm>

[6] OWASP. About the Open Web Application Security Project. Disponible en: < https://www.owasp.org/index.php/About_OWASP>

[7] VELA, Alfredo. Historia del Hacking Ético #INFOGRAFÍA #INFOGRAPHIC. Disponible en: < https://ticsyformacion.com/2015/07/07/historia-del-hacking-etico-infografia-infographic/>

[8] PENTEST-STANDARD. Penetration Testing Execution Standard - the FAQ. Disponible en: < http://www.pentest-standard.org/index.php/FAQ>

5.1.2. Definición de Hacker: La era actual se destaca por la alta influencia de la tecnología sobre la vida de las personas. El conocimiento se amplía cada vez más y al parecer éste no tiene límites. Este hecho, ha permitido que existan nuevas áreas de interés para las personas y que éstas pongan mucho más su foco de atención sobre aquellas disciplinas relacionadas con la tecnología. En este sentido, existen personas con un alto grado de experticia y experiencia en alguna área de este ámbito, denominadas a menudo con el calificativo de "hacker", cuyas características los hacen individuos con las capacidades suficientes para intervenir o alterar productos o dispositivos haciendo uso de su conocimiento técnico.

La mala prensa y la ignorancia han estigmatizado el término e incluso a las mismas personas que se podrían catalogar con dicho calificativo, al punto de considerarlos criminales peligrosos y perversos con las más oscuras intenciones. Lo cierto es que un "hacker" no es necesariamente el autor de conductas y actividades delictivas, sino que se destaca por su gran pasión, iniciativa y perseverancia para lograr identificar vulnerabilidades en sistemas informáticos regidos desde una estricta protección.

5.1.3. Tipos de Hacker: Partiendo de la premisa sobre los criterios de actuación de un hacker en los cuales se le atribuye la figura de un experto con alto conocimiento técnico sobre áreas específicas de la tecnología; se podría decir que de acuerdo a sus intenciones o fines se genera la siguiente clasificación:

Hackers de sombrero blanco (White hats): Utilizan su gran conocimiento y habilidades en favor de que sus hallazgos sean de utilidad para la corrección de errores en un determinado sistema. Su interés es que dichos fallos y sus respectivas soluciones sean de divulgación pública y así contribuir con el perfeccionamiento de la tecnología. Su gran dominio les permite ser autoridad competente para emitir juicios sobre las medidas de seguridad más convenientes para garantizar la defensa de los sistemas con el fin de blindar al máximo los activos del usuario.

Hackers de sombrero negro (Black hats): Al contrario de los "White hats", los hackers de sombrero negro rigen su actividad desde una perspectiva mucho más lucrativa, buscando que sus conocimientos estén al servicio del mejor postor. Su intervención es mucho más nociva, buscando que sus intereses o los de su cliente se cumplan y poder así obtener una satisfacción y compensación mucho mayor. Violentan y obtienen acceso a sistemas de manera ilícita buscando explotar sus vulnerabilidades para corromper o manipular la información confidencial, colapsar los sistemas y en general desplazarse a su antojo.

Hackers de sombrero gris (Gray hats): Son un punto intermedio entre las dos clasificaciones anteriores, lo que claramente pone en tela de juicio su ética profesional. En general, se puede describir su accionar como un juego a dos bandos; por un lado, se encargan de explotar las vulnerabilidades de un sistema

para luego ofrecer sus servicios y mitigar sus afectaciones formulando los mecanismos de defensa para la protección de los mismos.

5.1.4. Otros actores intervinientes

Crackers: Al igual que el hacker, es poseedor de grandes conocimientos y habilidades técnicas. Sin embargo, su objetivo se centra en obtener control total sobre determinados programas o alterar su funcionamiento. Se valen de procesos de ingeniería inversa o software de aplicación que les permite el desbloqueo de claves de acceso o exploración del código fuente. Una vez las aplicaciones son crackeadas, con su sistema de seguridad burlado, se permite acceso libre a cualquier funcionalidad del sistema. Posteriormente, el cracker estará en capacidad de distribuir el software a su antojo.

Phreaker: Su interés en la tecnología se centra sobre el campo de las telecomunicaciones llevándolos a comprender de manera profunda su funcionamiento con la principal meta de vulnerar sistemas telefónicos. La búsqueda de beneficios les puede llevar a cumplir distintos propósitos como la obtención de llamadas gratis, espionaje o simplemente romper la seguridad.

Lammer: Persona presuntuosa de sus habilidades y que se califica como “hacker” sin serlo. Tratan de acumular la mayor cantidad de información posible con respecto al tema buscando nutrirse de esto para aparentar de la mejor manera dominio sobre lo que realmente no conoce.

Newbie: El anglicismo tiene como traducción la palabra novato. En sí, tal y como lo dice su nombre son personas que inician en el mundo del Hacking, pretendiendo investigar toda la información disponible y probando el impacto de las herramientas dispuestas por los demás de manera inofensiva. Generalmente carecen de conocimientos técnicos y dependiendo de su evolución pueden terminar siendo Lammers o Hackers.

5.1.5. Introducción al Hacking Ético: Generalmente es efectuado por Hackers de sombrero blanco (White hats) que utilizan todo su conocimiento adquirido con el fin de proveer a quien requiera de sus servicios, de mecanismos de defensa para mejorar la protección de los sistemas en una organización.

Así, se podrá determinar cuáles serían las acciones que podrían efectuar un intruso sobre el sistema y la información que éste contiene.

El perfil de la persona o personas que se encargan de ejecutar todo lo que conlleva ejecutar el Hacking ético incluye gran dominio sobre los siguientes campos:

- Informática y sistemas.
- Sistemas Operativos
- Hardware.
- Electrónica
- Redes y telecomunicaciones.
- Programación.

5.1.6. Tipos de Ataques: Desde el punto de vista técnico, dada la naturaleza y objetivo de los ataques informáticos, éstos se pueden clasificar de la siguiente manera: ataques dirigidos hacia los sistemas operativos, aplicaciones, configuraciones y protocolos.

- **Ataques a Sistemas Operativos:** El mercado de los Sistemas Operativos desde hace varios años ha tenido como principales protagonistas a tres grandes familias: Windows, Linux y MAC. Así, el gran auge de los sistemas Windows ha hecho que durante muchos años sea el objetivo principal de los atacantes debido a su alto grado de popularidad. Para Linux, el hecho de que su núcleo sea de libre acceso para todas las personas hace que el caso sea aún más peligroso debido a que se detectan con mayor facilidad problemas a nivel de código. La gran diferencia entre estos sistemas no radica en el hecho de la cantidad de errores que aparecen día a día, sino la rapidez en la cual se solucionan donde claramente Linux lleva las de ganar.

- **Ataques a Aplicaciones:** Aplicaciones a la medida son construidas debido a la alta demanda de funcionalidades personalizadas. Por lo tanto, se infiere que detrás de todo el proceso existen miles de líneas de código que son pensadas y plasmadas por talento humano competente; sin embargo, al ser un trabajo manual es susceptible a errores, con lo cual se pueden inyectar vulnerabilidades de diferente severidad. Además, el hecho de que una aplicación o una funcionalidad específica sean usadas por muchas personas hace que el blanco sea más atractivo para los atacantes. En este sentido, se sugiere aplicar el minimalismo para evitar la instalación de aplicaciones que no se necesiten o requieran. También se debe tener mucho cuidado con los privilegios con los cuales se ejecute una aplicación debido a que podría comprometer su funcionamiento y el de todo el sistema en el cual se encuentra implementado.

- **Errores en Configuraciones:** Cuando una aplicación no está configurada adecuadamente, la falsa sensación de seguridad puede jugar una mala pasada. Esto debido a que el establecer que la configuración por defecto es la mejor alternativa es una perspectiva totalmente equivocada. Se debe evaluar el contexto

para formular de qué manera es más efectiva la protección y aplicar las medidas que sean necesarias. Por ejemplo, se debe evitar utilizar datos de acceso por defecto.

Un sistema bien configurado es menos susceptible a vulnerabilidades. De todas formas, existen técnicas como el Hardening que pueden ayudar a fortalecer las medidas de seguridad existentes hacia unas más adecuadas para garantizar la máxima protección.

Errores en protocolos: Uno de los puntos más críticos en cuanto a fallos de seguridad está en aquellos que suceden en los protocolos. Independientemente de que los sistemas operativos, aplicaciones y sus configuraciones cumplan con las pautas de seguridad recomendadas, si un protocolo falla, la afectación podría ser irreparable. Detectar errores de diseño en un protocolo implica en muchas ocasiones situaciones no corregibles, por esto, si al realizar un análisis de su arquitectura no se encuentra una solución conducente o las posibles medidas correctivas no son suficientes, éste se debe cambiar por otro protocolo que sea más seguro.

5.1.7. Formas de Evaluación de la Seguridad: El proceso de evaluación de la seguridad implica determinar y comprender el alcance de las actividades que se llevan a cabo en una organización. Por esto, toman gran importancia dos conceptos fundamentales: *Vulnerability Assessment y Penetration Test.*

Sin embargo, antes de realizar cualquier evaluación vinculada con tareas de auditoria de seguridad es necesario firmar un acuerdo legal que brinde garantías y determine derechos y deberes de las partes implicadas en el proyecto, esto debido a que en muchos países la legislación considera que este tipo de actividades sin consentimiento de los titulares son causal de consecuencias penales, por tanto para no incurrir en delitos informáticos es necesario dejar claridad sobre todas las acciones a realizar.

5.1.8. Vulnerability Assessment: Se refiere a la búsqueda de vulnerabilidades en cualquier tipo de sistema sin importar su contexto. Se busca determinar amenazas, agentes de amenaza y vulnerabilidades a los cuales se encuentra expuesto el sistema.

En relación con el área de tecnología e informática, se refiere a un análisis técnico sobre debilidades en la infraestructura. Es decir, se analizan las vulnerabilidades con respecto a servidores, redes, sistemas operativos, aplicaciones, entre otros, donde podrían existir deficiencias de tipo técnico.

5.1.9. Penetration Test: Se refiere a un método utilizado para evaluar el nivel de seguridad en una organización simulando lo que haría un atacante real a través de diversas técnicas y con el objetivo de encontrar vulnerabilidades que sean o no conocidas a partir de falencias en configuraciones o procesos.

Adicionalmente se analizan aspectos como el uso de técnicas de ingeniería social y la búsqueda de información de la organización en medios físicos o electrónicos. Es decir, se centra mucho más en el proceso que llevaría un atacante real al efectuar el ataque.

Entonces, es necesario tener claro que un Penetration Test:

- No es una Auditoria de Seguridad donde se evalúa hasta qué punto están bien implementadas ciertas medidas alineadas a normas o estándares.

- No es un análisis de riesgos en el que en función de los activos se analiza el impacto que tendrían amenazas con respecto a estos.

- No es un Vulnerability Assessment que se limite específicamente a vulnerabilidades de la infraestructura empresarial.

5.1.10. Fases de un Hacking Ético: Debido a que la atención del estudio se centra en la realización de pruebas de penetración, es necesario establecer un proceso lógico organizado en el cual se diferencien las fases del Hacking Ético y que permitan arrojar resultados contundentes cuyos hallazgos sean de utilidad para acciones preventivas y correctivas.

Así, comprendiendo que no existe un consenso claro sobre lo que es Penetration Test, tampoco se tiene un estándar sobre las etapas o fases que comprende, sin embargo, comparando las opiniones de entidades y expertos se podrían definir las siguientes etapas:

Fase de Planeación y Preparación: Acuerdo entre la ética del experto y la organización a la cual se aplica el Hacking ético donde se mencionan los tipos de ataques y pruebas a realizar.

Fase de Evaluación: Proceso central donde se aplica la intrusión o penetración en el sistema. Para garantizar su éxito se requiere de las siguientes actividades:

- *Recopilación de Información y Reconocimiento:* Recolección y validación de información de forma directa o indirecta con el objetivo.

- *Escaneo y Enumeración:* Escaneo de red para obtener información específica basándose en la información obtenida en fases anteriores. Se pretende el escaneo de puertos mediante el uso de dialers, escaneadores de puertos, mapeadores de red, barridos, escaneadores de vulnerabilidades, entre otros. El resultado final será la recopilación de información de los sistemas. El escaneo intensivo del objetivo permite identificar: puertos accesibles, localización de puerta de enlace, detalles del sistema operativo, hosts accesibles, entre otros.

- *Otorgamiento/obtención de acceso a red y sistemas:* Se obtiene acceso al Sistema Operativo o máquina de la red mediante abuso o subversión y se escalan privilegios para obtener completo control. En el proceso, los sistemas intermedios que se encuentran conectados quedan comprometidos. El atacante decide a que nivel quiere realizar el ataque: sistema operativo, aplicación o red.

- *Mantener acceso:* Se trata de evitar la pérdida de propiedad del acceso obtenido. Es posible mediante uso de puertas traseras, troyanos o rootkits (Payload). El atacante puede subir, bajar o manipular información, aplicaciones y configuración del Sistema Operativo. Se suelen usar los sistemas de los cuales se tiene control para realizar otros ataques posteriormente.

- *Limpiar los rastros:* Para finalizar la fase de evaluación donde se efectúa el ataque al sistema, es necesario evitar dejar rastros sobre toda actividad maliciosa con el fin de evitar posibles sospechas que entorpezcan ataques futuros. Es decir, se pretende continuar con el acceso sin ser detectado. En este contexto, es conveniente realizar limpieza sobre los logs de servidor, sistema y aplicaciones para evitar cualquier indicio. Con estas acciones, se pretende evitar que, tras análisis forense, se logren descubrir hallazgos que comprometan la acción del atacante. También, es importante tener en cuenta que entre más recursos sean manipulados existen más oportunidades de descubrimiento sobre las acciones efectuadas.

Fase de Conclusión: Presentación y recopilación de pruebas que conlleven a la formulación de recomendaciones del tratamiento de los problemas encontrados en el sistema evaluado. Se realiza un reporte ejecutivo y técnico como documentación final informativa para la organización y expertos respectivamente.

5.1.11. Metodologías y Marcos de Trabajo

(V 3.0) **Open Source Security testing Methodology (OSSTMM):** Es un manual de metodologías con el fin de conocer y medir el nivel de conformidad de una empresa a nivel de seguridad. Además, permite comprobar si los procesos hacen realmente lo que deben hacer y no lo que otros dijeron que hacen.

Como aspecto importante a resaltar es que OSSTMM es un proyecto libre por lo cual está totalmente abierto a la contribución de terceros sobre mejoras para garantizar que las pruebas ejecutadas son certeras, verídicas, eficaces y eficientes[9].

Su uso permite obtener una comprensión profunda sobre la interacción de los elementos, donde a través de la prueba de operaciones se obtiene una gran imagen de todas sus relaciones. Se obtiene una mirada de la interconexión de las operaciones en detalle y el mapa de lo que realiza el negocio[10].

(V 4.0) **OWASP Testing Guide:** Esta guía, producto del consenso y desarrollo expuesto a diferentes ambientes y culturas permite a las organizaciones aplicar un marco general de pruebas y técnicas asociadas con el fin de comprobar que el producto de la construcción de aplicaciones web es seguro y fiable haciendo especial énfasis en las áreas de debilidad siguiendo una serie de guías y listas propias de OWASP[11].

(V 0.59) **Penetration Testing Framework (PTF):** Es un marco de trabajo que parte de las actividades comprendidas en la fase de evaluación de un Penetration Test para proponer una serie de prácticas y herramientas estándar que permitan llevar a cabo cada tarea con los resultados esperados.

(LV 1.0) **Penetration Test Execution Standard (PTES):** Sus siete secciones comprenden el contenido de un estándar que concentra las características comunes y más representativas referentes a los casos de éxito correspondientes a la aplicación de Penetration Test. El PTF inicia con la comunicación y razonamiento para continuar posteriormente con la recolección de información y las fases de modelado de amenazas para que el equipo de trabajo sea capaz de obtener una mayor abstracción sobre los procesos de negocio la organización. Posteriormente, procede la investigación de vulnerabilidades, explotación y post explotación.

Se cierra el proceso con el reporte de resultados presentando la información al cliente en un lenguaje sencillo para proveer al documento del mayor valor posible.[12].

---

[9] UNAD. OSSTMM. Disponible en: <http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_27_osstmm.html>

[10] ISECOM. Open Source Security Testing Methodology Manual (OSSTMM). Disponible en: < http://www.isecom.org/research/>

[11] OWASP. Testing Guide Introduction. Disponible en: < https://www.owasp.org/index.php/Testing_Guide_Introduction#The_OWASP_Testing_Project >

[12] PENTEST-STANDARD. High Level Organization of the Standard. Disponible en: <http://www.pentest-standard.org/index.php/Main_Page>

Como nota final referente a este punto, es clave que al efectuar evaluaciones de seguridad se cuente con personal totalmente objetivo, por tanto, es preferible realizar contratación externa para concretar este tipo de actividades.

5.2. MARCO CONCEPTUAL

Los términos más importantes relacionados con la investigación se relacionan a continuación:

- *Confidencialidad:* Los recursos son usados únicamente por personal autorizado.
- *Integridad:* La información es verídica y confiable debido a que es modificada exclusivamente por personal autorizado.
- *Disponibilidad:* Los recursos están disponibles en cuanto son necesarios por cualquier área de la organización.
- *Autenticidad:* La identidad de remitente y destinatario son verificadas para garantizar seguridad en la comunicación entre dos partes.
- *No repudio:* Una vez se verifica la identidad de los implicados en una comunicación, se garantiza que la información sea enviada o recibida.
- *Seguridad Informática:* Mecanismos para asegurar la información presente a través del uso de recursos tecnológicos (Hardware, Software y Aplicaciones) en una red.
- *Seguridad de la Información:* Mecanismos de protección de datos que garanticen los principios de confidencialidad, integridad, disponibilidad, etc.
- *Seguridad Física:* Mecanismos físicos de prevención y detección que se encuentran orientados hacia la protección de recursos en la organización.
- *Seguridad Computacional:* Mecanismos lógicos implementados para proteger la información.
- *Vulnerabilidad:* Debilidad del sistema que lo hace susceptible a amenazas que podrían significar la afectación de los recursos.
- *Debilidad:* Pérdida parcial o total de un control.

- *Amenaza:* Materialización potencial de una debilidad, que puede significar la realización de un ataque informático.

- *Riesgo:* Probabilidad de que una amenaza sea producida y afecte la organización.

- *Control:* Mecanismo de reducción de debilidades o amenazas, ya sean por prevención, corrección o detección.

- *Ataque Informático:* Método por el cual un individuo o grupo buscan de manera intencional causar daño o problemas a un sistema informático o red.

- *Diagnóstico:* Determinar estado de nivel de seguridad en la organización.

- *Diseño de Seguridad:* Planeación y Formulación de políticas, normas y estándares o procedimientos desarrollando arquitectura de seguridad, planes de continuidad y cultura de seguridad.

- *Implementación de Modelo de Seguridad:* Creación final de políticas, normas, estándares, procedimientos, arquitectura, planes de continuidad y capacitación en seguridad.

- *Hacking Ético:* Conocimiento de debilidades de la organización de forma no intrusiva como punto de partida para la detección de vulnerabilidades en sistemas de información para posterior aplicación de acciones correctivas.

5.3. MARCO HISTÓRICO

De acuerdo a los hechos relacionados con la creación de los computadores, aparición de Internet, organización del Hacking y asimilación de la necesidad de Seguridad Informática, se puede brindar los siguientes antecedentes de situaciones que marcaron la historia como referentes en la investigación del Hacking Ético y todos sus desencadenantes.

Tabla 1. Antecedentes Históricos Hacking Ético.

Hechos	Descripción
Creación de la Computadora	Fuente de curiosidad que acompañó a los expertos a lo largo del tiempo, realizando continuos aportes al proceso de sofisticación tecnológico y evolución a lo largo del tiempo.

Hechos	Descripción
Caja Azul	Creado como método de Hacking Telefónico a través de un juguete simple.
Creación Chaos Computer Club	Formación de la asociación de hackers más grande en Europa.
Ataque a red de equipos federales	Kevin Poulsen perseguido por la policía en respuesta a su intrusión abusiva a la red de equipos federales.
Aparición de los Primeros Virus Informáticos	Aparece el gusano de Morris causando estragos en Internet.
Primera Condena por Fraude Informático y Acto Abusivo	Kevin Morris es capturado y encerrado por las consecuencias desencadenadas por su gusano de Morris.
Hacking aplicado a robo Bancario	Vladimir Levin accede a cuentas de clientes Citibank y roba aproximadamente 10 millones de dólares.
Sociedad Digital	La tecnología se encuentra en todos los contextos, desde la empresa hasta el hogar. La información es almacenada por cada acción realizada, desde una compra en un almacén hasta la realización de un documento simple.
Ataque de Denegación de Servicio	Michael Calce realiza un ataque DDos a Yahoo!, eBay, CNN, Amazon y Dell.
Robo de Información Personal	Diversidad de hechos de intrusión dejan como consecuencia el robo de información personal de usuarios debido al almacenamiento masivo registrado en las bases de datos empresariales reflejado por ejemplo, en el robo de cuentas a clientes AOL y más recientemente a clientes de Tarjetas Visa y Mastercard.
Hacking aplicado a dispositivos modernos	George Hotz consigue desbloquear el iPhone y hackear el PS3.
Protesta social a través del Hacking	Grupos como Anonymous expresan su inconformismo con las medidas políticas de los gobiernos a nivel mundial, a través de hackeo de cuentas en servicios como Facebook, Twitter o Flickr.
Seguridad Informática Aplicada.	Se potencia el desarrollo de Software encargado de proteger equipos de cómputo de manera más efectiva garantizando la tranquilidad del usuario.
Fuente: El autor	

5.4. ESTADO ACTUAL

A continuación, se analizan los hechos y estadísticas más representativas que permiten establecer un panorama claro sobre la situación de las empresas en Colombia con respecto a los delitos informáticos y la importancia de la seguridad

para establecer medidas pertinentes en favor de la preservación de los activos organizacionales.

Hechos relevantes

- Durante el 2007, las empresas sufrieron pérdidas por más de 6.6 billones de pesos a raíz de delitos informáticos[13], cifra que se repitió nuevamente en el 2012.

- Según un estudio realizado por Symantec, se afirma que entre los años 2011 y 2012, el robo y fuga de datos de las empresas aumento en un 42% representando pérdidas a nivel mundial de un 0.7% en relación a sus ingresos.

- La "Encuesta Global Sobre Fraude 2012" realizado por la empresa MaTTica reveló que el 19% de las empresas colombianas fueron víctima del hurto de información, siendo un 7% superior a la media mundial.

- En 2012, Colombia fue el tercer país en Latinoamérica donde se cometió mayor cantidad de delitos informáticos prevaleciendo en mayor proporción las denuncias por fraudes a nivel bancario[14].

- Samuel Alberto Yohai, presidente de la Cámara Colombiana de Informática y Telecomunicaciones afirmó que los delitos cibernéticos le cuestan al país alrededor de los 500 millones de dólares, siendo las entidades gubernamentales las más vulneradas[15].

La sofisticación de los atacantes, es decir, su adaptabilidad ante cualquier circunstancia cambiante, hace que evitar la materialización de este tipo de ataques sea muy complicado, por tanto, dado el contexto actual donde el crecimiento de los delitos informáticos es evidente, es necesario que las empresas tomen conciencia sobre la problemática y actúen acorde a la situación para prevenir circunstancias inesperadas que afecten gravemente su estabilidad.

En este sentido, el Hacking ético toma mayor protagonismo dadas las circunstancias logrando disminuir la magnitud o impacto desencadenado por las amenazas externas o internas. Su ejecución no solo permitirá establecer el nivel de seguridad en el cuál se encuentran las empresas sino también generar resultados positivos posteriores para tomar acciones concretas en favor de fortalecer las defensas y

[13] INFORMATICA FORENSE COLOMBIA. Colombia. Disponible en: <http://www.informaticaforense.com.co/index.php/colombia>

[14] EL PAIS. En Colombia las cifras de delitos informáticos van en aumento. Disponible en: <http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento>

[15] VANGUARDIA. En Colombia se pierden US$500 millones de delitos informáticos. Disponible en: <http://www.vanguardia.com/colombia/322059-en-colombia-se-pierden-us500-millones-de-delitos-informaticos>

tener unas políticas orientadas totalmente hacia la obtención de una mayor seguridad de los recursos.

5.5. MARCO TECNOLÓGICO

El ser humano aprovecha los recursos que se encuentran en su medio para mejorar su calidad de vida. La tecnología e informática han sido un gran aliado de las personas para que sus tareas sean cada vez mucho más fáciles de realizar automatizando gran cantidad de procesos.

La seguridad informática no es ajena a esta realidad, y además, partiendo de diferentes factores como las facilidades para compartir, el interés por la colaboración, las redes de conocimiento y la rápida integración entre herramientas, hacen más que necesaria una obligación del experto, recurrir al uso de herramientas de software adecuadas para facilitar su tarea y efectuar análisis de mayor calidad y con menor probabilidad de errores.

5.5.1. Requerimientos de Software y Hardware: Se requiere de la instalación y uso de Sistemas Windows y GNU/Linux como plataforma de Software obligatoria para poder instalar las aplicaciones que sean necesarias con el propósito de atender los requerimientos del Penetration Test.

Es de señalar que, si se habla de Linux, existen distribuciones dedicadas exclusivamente a la temática de seguridad, por tanto, muchas de estas tendrán sus respectivos paquetes preinstalados y listos para usarse.

Las exigencias a nivel de Hardware no son muy altas, de todas formas, entre mayores sean las capacidades de los equipos de cómputo se podrá obtener un mayor rendimiento de las aplicaciones. A continuación, se establecen los requerimientos mínimos:

Windows[16]:

- Procesador: mínimo 1 GHz o más rápido.
- RAM: 1 GB (32-bit) o 2 GB (64 bits).
- Espacio en disco duro: 16 GB (32 bits) o 20 GB (64 bits).

[16] MICROSOFT. Windows 10. Requisitos del sistema. Disponible en: <https://www.microsoft.com/es-co/windows/windows-10-specifications>

Linux[17]:

- Procesador: mínimo 1GHz o más rápido.
- RAM: 512 MB.
- Espacio en disco duro: 8 GB.

5.5.2. Tipos de licenciamiento de Software:

Licencia EULA: Aplica para el caso de productos Microsoft. Se refiere a un tipo de licencia de software con código cerrado, es decir, software propietario o privativo donde se restringen los derechos del usuario de acuerdo a las condiciones impuestas por la empresa proveedora[18].

Licencia Freeware: Ofrece funcionalidad completa del programa gratuitamente, sin embargo, el contenido de su código es cerrado al usuario y existen restricciones en cuanto a su distribución. Algunas de las herramientas utilizadas en Windows y que facilitan el Penetration Test entran en esta categoría[19].

Licencia GNU / GPL: Las distribuciones Linux y la mayoría de aplicaciones que se ejecutan en esta plataforma y hacen parte de este proyecto usan este tipo de licencia. Ésta pretende promover los derechos del usuario y brindar mayores libertades para compartir el conocimiento en comunidad.

5.6. MARCO LEGAL

La tecnología hace presencia en todo contexto. Su vertiginoso avance ha permitido su uso masivo. Sin embargo, a su vez esto ha representado una gran problemática global debido al aprovechamiento de los recursos telemáticos para alcanzar grandes distancias en tan solo un segundo. Por otra parte, como toda obra del hombre, tanto Software como Hardware son susceptibles a fallos, y aquellas debilidades pueden ser la puerta hacia aquel activo de gran valor llamado información. Servicios como Internet, tecnologías como las inalámbricas, entre otros, son el canal propicio para que delincuentes o curiosos puedan adquirir aquello que buscan en los demás.

---

[17] KALI. Instalación de Kali Linux en un disco duro. Disponible en: <http://es.docs.kali.org/installation-es/instalacion-de-kali-linux-en-un-disco-duro>

[18] USEMOSLINUX. EULA (Windows) vs. GPL (Linux): Duelo de licencias. Disponible en: <http://blog.desdelinux.net/eula-windows-vs-gpl-linux-duelo-de-licencias/>

[19] ESPINAL, Juan. Que son las licencias de software: Freeware, adware, shareware y software libre. Disponible en: <http://www.downloadsource.es/que-son-las-licencias-de-software-freeware-adware-shareware-y-software-libre/a/110/>

De ahí que, el gobierno colombiano en el afán de proteger sus intereses y los de la ciudadanía, ha sido pionero en la creación de instrumentos jurídicos que castiguen severamente a aquellas personas que pretendan utilizar las TIC para manipular información confidencial sin la autorización de sus dueños.

5.6.1. Ley 1273 de 2009: Colombia adoptó por medio de la Ley 1273 de 2009 un nuevo bien jurídico conocido como "de la protección de la información y de los datos". Este recurso legal permite hacer frente a la nueva gama de amenazas contra la información desencadenada por los delitos informáticos. Las conductas tipificadas y castigadas están divididas en dos categorías: aquellas que atentan contra la confidencialidad, integridad y disponibilidad de los datos y aquellas que atentan contra los sistemas informáticos y otros.

Atentados contra confidencialidad, integridad y disponibilidad de los datos

- **Acceso abusivo a un sistema informático:** Se aprovecha de las debilidades en materia de seguridad de un sistema informático para acceder a éste sin autorización.

- **Obstaculización ilegitima de sistema informático o red de telecomunicación:** Se impide el ingreso normal a los sistemas debido a bloqueos ilícitos sin el consentimiento de los afectados.

- **Interceptación de datos informáticos:** Obstrucción de datos en su origen o destino utilizando como medio de transmisión las redes informáticas del mismo sistema.

- **Daño Informático:** Acción de manipulación sin autorización de datos electrónicos.

- **Uso de Software malicioso:** Se refiere a la acción de distribución de Software malicioso sin autorización con la única intención de causar daños en los activos de información de una empresa.

- **Violación de datos personales:** Violación a la privacidad a través de la revelación, tráfico o divulgación sin autorización de los datos personales que puedan violar la intimidad u honor del afectado.

- **Suplantación de sitios web para capturar datos personales:** Creación de clones de páginas de interés generalizado, con lo cual los criminales obtienen información privilegiada del afectado y hacen uso de ella para satisfacer sus intereses personales.

Atentados hacia sistemas informáticos y otros

- **Hurto por medios informáticos y semejantes:** Manipulación de un sistema informático para permitir acciones relacionadas con transferencias de activos que pueda perjudicar a otras personas.

- **Transferencia no consentida de activos:** Técnicas para almacenar de manera no autorizada información estrictamente privada de los usuarios para su difusión posterior por cualquier medio con fines lucrativos.

5.6.2. Decreto 1377 de 2013: Debido a que la realización de un proceso de Hacking Ético o pruebas de pentesting requiere la manipulación de activos de información con datos confidenciales de la empresa, este decreto es fundamental como un medio para establecer las responsabilidades del encargado y las acciones para las cuales está autorizado.

Pautas para Autorización

El responsable de las pruebas debe garantizar las siguientes pautas:

- **Recolección de datos personales:** La manipulación de datos personales o empresariales está justificada únicamente para las actividades autorizadas a efectuar por la gerencia en la organización.

En este punto, se profundiza sobre cuáles serán los procedimientos usados para el tratamiento de la información, explicando su respectiva finalidad y necesidad en cada caso que lo requiera.

- **Autorización del Tratamiento:** Es necesario contar con una autorización para recabar datos preferiblemente antes de efectuar cualquier tipo de acción. Por lo tanto, para obtener dicho consentimiento por parte del titular, es fundamental informarle la finalidad correspondiente a la recolección de datos.

Además, en este proceso se comunica al titular cuales de los datos tratados son sensibles y por qué se necesitan o se dará tratamiento a los mismos, ratificando la obtención del respectivo consentimiento.

Como evidencia se deberá conservar la autorización del titular mediante manifestaciones escritas, orales o conductuales que permitan inferir o concluir de manera contundente que efectivamente se otorgó el permiso.

- **Revocatoria de la autorización:** El titular puede solicitar en cualquier momento que los datos personales sean borrados o asimismo, revocar la autorización para el

tratamiento de información a menos que se tenga una obligación contractual con el responsable.

Políticas de Tratamiento

- **Políticas de tratamiento de la información:** Se deben especificar en medio físico o electrónico, en un lenguaje claro para ser dispuesto hacia los titulares y debe contener al menos la siguiente información:

    - Datos personales del responsable.
    - Tratamiento al cual se someten los datos y su finalidad.
    - Derechos que tiene el titular.
    - Persona que atiende al titular en caso de que tenga alguna petición, queja o reclamo.
    - Procedimiento para que el titular pueda ejercer sus derechos con respecto a la autorización brindada.
    - Fecha de vigencia de la política.

- **Aviso de privacidad:** Se debe disponer de un medio informativo por medio del cual el titular pueda conocer de la existencia de la política de tratamiento en el caso de que no fuere posible ponerla a su disposición de manera directa. Así, como mínimo este documento deberá tener:

    - Datos personales del responsable.
    - Tratamiento al cual se someten los datos y su finalidad.
    - Derechos que tiene el titular.
    - Mecanismos de difusión de las políticas de tratamiento y los cambios que se realicen en esta.

5.6.3. Ley 1581 de 2012: Esta ley se constituye como aquella que describe todas las disposiciones concernientes a la protección de datos personales. Así, se aplica a personas naturales, las cuales pueden autorizar acciones relacionadas con el tratamiento de la información incluyendo el almacenamiento, actualización y rectificación que contengan algún tipo de dato personal.

Cuando se habla de datos personales, se dice de aquellas unidades de información que se pueden relacionar con la persona y que tiene cierto grado de uso y nivel de intimidad. Así, según estos criterios descritos los datos pueden ser de tipo público, semiprivado o privado.

Adicionalmente, la persona natural podría en cualquier momento solicitar prueba sobre la autorización que brindó previamente, ser informado sobre las acciones que se efecúan con sus datos, anular la autorización y solicitar que sus datos sean

borrados sobre cualquier medio de almacenamiento. Así también, puede presentar solicitudes o quejas ante la entidad regulatoria que garantice a cabalidad la protección de sus datos.

La autorización del titular debe ser previa, informada y expresa, especificando la finalidad para la obtención de datos personales. La autorización puede ser escrita, física o digital permitiendo su consulta posterior.

5.6.4. Sobre CJT&T Ingeniería de Software

Es una compañía dedicada al desarrollo e implantación exitosa de proyectos informáticos. Consciente de la problemática existente con el uso y aprovechamiento de herramientas de software y por ello tiene soluciones que facilitan la toma de decisiones por parte de la alta gerencia en todo lo relacionado con la infraestructura tecnológica.

6. DISEÑO METODOLÓGICO

6.1. TIPO DE PROYECTO

El documento actual corresponde a un proyecto aplicado, en tanto permite dar solución a un problema especifico a través de los conocimientos obtenidos durante todo el proceso formativo que otorga el programa de especialización en Seguridad Informática.

Por tanto, se pretende realizar un aporte significativo en la ejecución metodológica de las pruebas de Pentesting mediante la formulación de buenas prácticas relacionadas con todo el proceso, lo cual permitiría modificar la realidad con única finalidad práctica

Por consiguiente, se responde a un problema frecuente a nivel organizacional como es la exposición de activos críticos a múltiples riesgos internos y externos debido a la carencia de medidas de seguridad eficientes que mitiguen la mayor cantidad de peligros que puedan afectar a los elementos que conforman el contexto. Así, a partir de diversas pruebas específicas se logrará establecer un diagnóstico inicial que sea de utilidad para un posterior análisis que será la base para la configuración e implementación de controles.

6.2. MÉTODO DE INVESTIGACIÓN

En el siguiente proyecto de investigación aplicado se hará uso de los métodos de investigación con enfoque inductivo-deductivo con el fin de organizar los procedimientos lógicos y llegar mediante diferentes técnicas e instrumentos hacia una descripción más detallada de la realidad relacionada con la Seguridad Informática y Hacking Ético.

- *Método Inductivo:* Desde conceptos generales a particulares se infiere que la detección de vulnerabilidades y su posterior explotación permitirán determinar la situación de seguridad en la organización e identificar los controles más convenientes para su evitar que las amenazas se materialicen en posibles ataques informáticos.

- *Método deductivo:* Desde una premisa general a conceptos particulares, se parte de la situación de seguridad de la organización para determinar los ítems aplicables para complementar o generar la política de seguridad de la organización.

6.3. POBLACIÓN

La población del estudio se relaciona en la tabla 2, clasificando el talento humano según las áreas a la que pertenecen en la empresa CJT&T.

Tabla 2. Población del estudio

Contratación	Área	Campo	Sexo		Total	%
			M	F		
Directa	Tecnología	Desarrollo	10		10	43.5
		Arquitectura de Software	1	1	2	8.7
		Pruebas	1	1	2	8.7
		Garantías	1		1	4.3
		Líder técnico	1	1	2	8.7
		Gerencia de proyectos	1		1	4.3
	Administración	Contabilidad		2	2	8.7
		Administración		1	1	4.3
		Dirección		1	1	4.3
Servicios		Aseo		1	1	4.3
TOTALES					23	100
Fuente: El autor						

Las 23 personas listadas en la tabla anterior realizan sus labores en la sede principal de la empresa CJT&T ubicada en el barrio Las Acacias de la ciudad de Pasto.

De aquí se destaca que la mayoría de la población corresponde a desarrolladores con un 43.5%, de los cuales se desprende la labor de construcción de aplicaciones. Además, éstos hacen uso continuo de los servidores que almacenan información sensible de la empresa, por lo cual es muy importante comprobar su grado compromiso y además el nivel de seguridad que aportan sus equipos.

6.4. ESTRUCTURA DE LA UNIDAD DE ANÁLISIS

Debido a que el estudio pretende realizar un análisis de vulnerabilidades a través de pruebas de Pentesting aplicado a la empresa CJT&T, partiendo de la población y analizando el área de impacto se establece que la unidad de análisis más conveniente será el área de tecnología de la empresa debido a que está en contacto

continuo con los activos de mayor valor y por tanto sus interacciones con otros empleados y equipos tecnológicos toman mayor relevancia.

6.5. DEFINICIÓN DE HIPÓTESIS

- **Hipótesis de Investigación (Hi):** Los resultados de las pruebas de Pentesting permiten establecer mecanismos de control que brindan protección en los activos de la organización sobre los riesgos asociados al uso de tecnologías, información y sistemas informáticos.

- **Hipótesis nula (Ho):** Los resultados de las pruebas de Pentesting NO permiten establecer mecanismos de control que brindan protección en los activos de la organización sobre los riesgos asociados al uso de tecnologías, información y sistemas informáticos.

6.6. VARIABLES E INDICADORES

- **Variable 1 -** Nivel de seguridad en la empresa.
    - **Indicador 1:** Fallas de seguridad.
    - **Escala de medición:** Bajo, medio, alto.

- **Variable 2** - Infraestructura tecnológica.
    - **Indicador 1:** Nivel de degradación.
    - **Escala de medición:** Bajo, medio, alto.

- **Variable 3 -** Riesgos asociados a la manipulación de información y uso de sistemas informáticos
    - **Indicador 1:** Frecuencia de riesgos
    - **Indicador 2:** Reporte de incidencias
    - **Escala de medición:** Bajo, medio, alto

6.7. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Tabla 3. Técnicas e Instrumentos para Recolección de Información.

Procedimiento	Descripción	Instrumento	Formato
Observación	Recolección de información de carácter cualitativo de utilidad para identificación de infraestructura física de la organización.	Personal	Directa. Registro audiovisual.
Análisis de documentos	Análisis no intrusivo de información registrada en documentos escritos y visuales para interpretación de contenidos de utilidad para el objeto de estudio de la presente investigación.		Medios impresos, fotos, grabaciones de audio y video. Internet.
Fuente: El autor			

Procedimiento a seguir

- Identificación y localización de fuentes de información.
- Consulta de fuentes localizadas.
- Recolección y Ordenamiento de Información
- Interpretación y análisis de Información
- Presentación de análisis final a manera de conclusiones y presentación formal del proyecto.

6.8. FUENTES DE INFORMACIÓN

Se hará uso de fuentes primarias y secundarias tal y como se indica a continuación:

- **Primarias:** Contacto con el personal interno de la organización como evidencia testimonial o entrevistas que permitan conocer su grado de capacitación y su disposición para asumir las políticas de seguridad que sean planteadas.

Además, es muy importante la realización de consultas a expertos, que en este caso serán los tutores de la UNAD para obtener información relevante sobre la manera más adecuada para abordar la metodología de trabajo en la fase de Evaluación correspondiente al Hacking ético.

- **Secundarias:** Se utilizarán documentos impresos y digitales como artículos y ensayos, archivos multimedia tomados de Internet desde las páginas oficiales de las Metodologías que se decida aplicar con el fin de asegurar que la información obtenida sea verídica y autentica y evitar que todas las actividades ejecutadas no correspondan a prácticas adecuadas en ejercicio de las herramientas dispuestas para ello.

7. ESQUEMA TEMÁTICO

7.1. DISTRIBUCIONES LINUX EN EL ÁMBITO DE LA SEGURIDAD INFORMÁTICA

Kali Linux: Distribución Linux especializada para las tareas de auditoria y pruebas de penetración proporcionado un repositorio centralizado que contiene las herramientas idóneas para cada una de las fases que comprende este tipo de procesos.

Samurai Linux: Samurai WTF (Web Testing Framework) es más que un entorno de trabajo. Se basa en la distribución Ubuntu y utiliza un entorno gráfico KDE optimizado y preconfigurado para trabajar fluidamente y garantizar el rendimiento adecuado en las labores de testeo. Su objetivo no es diferente al de llevar a cabo tests de penetración sobre aplicativos Web. Ya sea a través de un sistema en tiempo real o LiveCD, o si se quiere instalar en el disco duro, se destaca por su catálogo de aplicaciones libres y gratuitas especializadas que realizan funciones automáticas o manuales en pruebas de intrusión.

7.2. INVENTARIO DE HERRAMIENTAS POR FASE DE HACKING ÉTICO

A continuación, se relacionan las herramientas informáticas recomendadas para facilitar la automatización de procesos y presentación de resultados durante las distintas actividades que se realizan en la fase de evaluación de un Penetration Test.

Tabla 4. Herramientas para uso en Hacking ético.

Fase	Herramienta	Funcionalidad
Evaluación	Cree.py	Extracción de información de individuos
	Maltego	Footprinting en Internet.
	TheHarvester	
	FOCA	
	McAfee SiteDigger	
	Exif Tool	
	Airmon-ng	Información de las instalaciones e identificación de equipos.
	Airodump-ng	
	Kismet – Newcore	
	inSSIDer	

Fase	Herramienta	Funcionalidad
	Whois	Footprinting externo.
	InterNIC	
	Host	
	Dig	
	Fierce2	Footprinting activo.
	DNSEnum	
	Dnsdict6	
	Nmap	
	SNMPEnum	
	Nmap	Footprinting Interno.
	Alive6	
	SNMPcheck	
	Metasploit	
	Host	
	Dig	
Análisis de vulnerabilidades	OpenVAS	Herramientas automatizadas para las pruebas de vulnerabilidades.
	Nessus	
	NeXpose	
	Retina Network Community	
	Webinspect	Escáner de Aplicaciones Web.
	DirBuster	
	P0f	Prueba de vulnerabilidades de manera pasiva.
	Wireshark	
	Tcpdump	
	Metasploit	
Explotación	Metasploit	Ataques de precisión.
	Wireshark	Sniffing.
	Tcpdump	
	Brutus	Ataques de fuerza bruta.
	THC-Hydra / XHydra	
	Medusa	
	Aircrack-ng	Acceso a radio frecuencias.
	Airmon-ng	
	Airodump-ng	
	Aireplay-ng	
	Karmetasploit	Ataques al usuario.
	Havij	
	SQLmap	
	Pangolin	
Post-explotación	Fgdump	Extracción de hashes de contraseñas en Windows
	Hashdump	
Fuente: El Autor		

7.3. DESCRIPCIÓN DE LAS HERRAMIENTAS

- **Aircrack-ng:** Completo conjunto de herramientas cuyo objetivo es permitir una mejor evaluación de la seguridad para las redes WiFi WEP y WPA/WPA2 permitiendo:

    - Monitorear paquetes.
    - Ejecutar ataques.
    - Verificar las capacidades del hardware y realizar pruebas.
    - Crackear claves.

Entre los paquetes de los cuales se hará uso se encuentran:

    - Aircrack-ng es la herramienta que se usa para crackear las llaves WEP y WPA/WPA2 utilizando dos métodos: PTW (Pyshkin, Tews, Winmann) y FMS/Kore valiéndose de los paquetes capturados con airodump-ng.
    - Aireplay-ng se encarga de realizar ataques que puedan generar tráfico que posibilite el posterior crackeo de las claves a través de aircrack-ng.
    - Airmon-ng tiene una función de gestión del hardware lo cual se refleja a través de la activación/desactivación de las interfaces de red y el modo monitor.

- **THC IPv6 Attack Toolkit:** El objetivo de este conjunto de herramientas es muy claro: aprovechar las debilidades de los protocolos IPV6 e ICMP6 para efectuar ataques que permitan obtener información referente a la red.

Para el presente proyecto, son de especial interés dos herramientas:

    - Alive6 que es capaz de realizar un escaneo para detectar todas las direcciones activas en un segmento de red.
    - Dnsdict6 que parte de entradas de diccionario propias o especificadas por el usuario para enumerar un dominio, y con ello obtener entradas DNS.

- **Brutus Password Cracker AET2:** Es un crackeador de contraseñas, permitiendo probarlas de manera remota hasta obtener la correcta. Fue originalmente pensado para verificar este aspecto en la configuración de routers evitando así el uso de contraseñas por defecto o con una baja fortaleza. Sin embargo, actualmente cuenta con diferentes opciones para autenticación como HTTP, POP3, FTP, SMB y Telnet, entre otros.

- **Cree.py:** Partiendo del concepto de OSINT a través del cual se pretende recolectar la mayor cantidad de información relevante no clasificada y libre en la

web,[20] cree.py se constituye como una potente herramienta de geolocalización partiendo de aquella información disponible a través de OSINT. Además, ofrece grandes ventajas como la presentación de los resultados en mapas, el filtrado según localización y fecha y la opción de exportación para posteriores análisis.

- **Dig:** Herramienta de línea de comandos usada en la administración de redes que consulta los DNS con el fin de obtener información sobre las direcciones de host, registros MX, nameservers y otra información relacionada[21]. Es decir, como parte de la recolección de información permite la agrupación de información de dominio.

- **DirBuster:** Aplica la fuerza bruta en los directorios de un servidor web o de aplicaciones teniendo en cuenta que el proceso de instalación por defecto trae consigo componentes ocultos como páginas y aplicaciones. DirBuster se aprovecha de esto e intenta encontrarlas haciendo uso de 9 listas diferentes productos de la investigación de recursos en Internet y en referencia al uso de archivos y directorios por parte de los desarrolladores de aplicaciones.

- **DNSEnum:** Script cuya función es la de capturar la mayor cantidad de información sobre determinado dominio, descubriendo a su vez los bloques de IP no contiguos[22].

- **Retina Network Community:** Su versión gratuita brinda un manejo potente de las vulnerabilidades presente en todo el contexto de trabajo.

Limitado a 256 IPs, es capaz de realizar gran cantidad de tareas de gran importancia para un Penetration Test como son:

  - Identificación de vulnerabilidades de red.
  - Detección de fallas en la configuración.
  - Detección de parches de seguridad faltantes en Sistemas Operativos, aplicaciones, dispositivos y ambientes virtuales.

- **Exif Tool:** Es una aplicación conformada por una librería PERL y una línea de comandos de mucha utilidad para manipular información contenida en los metadatos de gran cantidad de tipos de archivos. Su gran ventaja permite, por

[20] BRIGHTPLANET. What is OSINT and how can your organization use it?. Disponible en: <http://www.brightplanet.com/2013/04/what-is-osint-and-how-can-your-organization-use-it/>

[21] MEDIATEMPLE. Understanding the dig command. Disponible en: < https://mediatemple.net/community/products/dv/204644130/understanding-the-dig-command>

[22] KALI. dnsenum. Disponible en: <http://tools.kali.org/information-gathering/dnsenum>

ejemplo, sanear toda la información sensible en los archivos de una empresa antes de hacer una publicación de los mismos.

- **Fgdump:** Es un programa centrado en la auditoria de contraseñas en Sistemas Windows, cuya extracción la realiza desde NT Lan Manager (NTLM) y MS Lan Manager (LanMan). Sus capacidades le permiten incluir entre los resultados un histórico de contraseñas en caso de estar disponibles y asimismo exportarlas a un archivo externo. Antes de su ejecución, intenta deshabilitar programas antivirus para proseguir con su funcionamiento y accionar la secuencia de aplicaciones así: pwdump, cachedump y pstgdump.

- **Fierce2:** Liviana herramienta clasificada como un escáner de enumeración el cual permite localización espacios no contiguos de IPs para dominios específicos indicados por el usuario valiéndose de recursos como DNS, Whois y ARIN[23]. Está pensado como un precursor de herramientas de prueba activas.

- **FOCA:** Especializada en el análisis de metadatos, FOCA pretende encontrar información oculta en documentos frecuentemente del tipo ofimático ubicados en la web o a nivel local.
Los datos extraídos se procesan, se unen y se reconocen qué documentos se crearon desde el mismo equipo y además se infieren servidores y clientes relacionados en la organización.

A continuación, se muestran algunas categorías referentes a la información resultante posterior al análisis de documentos:

  - Información de usuario.
  - Rutas lógicas.
  - Versiones de Software.
  - Datos de red.
  - Dominios y Zonas.
  - Roles.

- **McAfee SiteDigger:** Es una herramienta indispensable en la recolección de la información empresarial. Permite la búsqueda a través del cache de Google con el fin de buscar blancos sensibles en la red para un dominio concreto la cual podría ser causal de vulnerabilidades, errores de configuración y seguridad o información confidencial expuesta.

- **Havij:** Es una herramienta automatizada para realizar ataques de Inyección SQL en aplicaciones Web. Con una interfaz intuitiva, basta con ingresar la URL especifica que será blanco de ataque para que el programa la analice, y producto

[23] ALDEID. Fierce. Disponible en: < https://www.aldeid.com/wiki/Fierce>

del proceso se indica si la intrusión ha sido exitosa. Posteriormente, se mostrará la base de datos actual desde la cual se podrá tener acceso a todas las tablas para extraer la información que se desee. El programa incluye un “Admin finder” para encontrar el login de acceso para las opciones de administración.

- **Host:** Herramienta de línea de comandos utilizada para realizar búsquedas de DNS. Su tarea principal es la de convertir nombres en direcciones IPs y viceversa[24].

- **inSSIDer:** Herramienta indispensable para monitorear, detectar problemas y optimizar la red inalámbrica. Entre otros aspectos la aplicación permitirá:

    - Mejorar el rendimiento de la red.
    - Detectar y mostrar la red actual y todas las que se encuentren cerca.
    - Mostrar cómo varía la fortaleza de la señal en diferentes lugares.
    - Detectar el canal que otras redes estén usando para verificar si coincide con la propia red y cambiarlo para obtener mayor rendimiento.

- **Kismet:** Aplicación encargada de detectar redes inalámbricas, realizar sniffing y funcionar como IDS, requiere de hardware con soporte del modo monitor para su adecuado funcionamiento. Su factor diferenciador radica en la detección de redes en forma pasiva recolectando paquetes de datos que además, le permiten identificar redes escondidas[25].

- **Maltego:** La plataforma que ofrece esta herramienta es única al permitir recolectar información empresarial y personal desde diferentes fuentes con el fin de determinar el grado de amenazas a la que se está expuesto. Su perspectiva se basa en la búsqueda de recursos sobre la red o todo internet sin importar la temática de la cual trate, éste tratará de localizarla, añadirla y visualizarla.

- **Medusa:** Su labor se centra en los ataques de fuerza bruta y pretende garantizar que estos sean rápidos, confiables y sigan procesos paralelos. Además, se pretende que el desarrollo de la herramienta sea escalable, por tanto, esta sigue el principio de modularidad. Son de destacar los siguientes aspectos:

    - Soporte para pruebas concurrentes.
    - Especificación personalizada sobre organización de la información objetivo.
    - Capacidad de crecimiento mediante el desarrollo de módulos.

- **Metasploit Community:** La dispersión sobre herramientas para realizar un Penetration Test no es adecuada para garantizar buenos resultados, por tanto,

[24] COMPUTERHOPE. Linux and Unix host command. Disponible en: < http://www.computerhope.com/unix/host.htm>

[25] KISMET WIRELESS. Documentation. Disponible en: < https://www.kismetwireless.net/documentation.shtml>

Metasploit Community Edition ofrece una interfaz gráfica que simplifica las tareas de este tipo de pruebas permitiendo:

- Realizar descubrimiento de la red.
- Verificar vulnerabilidades para exploits específicos.
- Incrementar la efectividad de los escanners de vulnerabilidades como Nessus, Nexpose y otros.

Así también entre otras características se encuentran:

- Permite Mapear la red.
- Integración con otros escáneres de vulnerabilidades.
- Encontrar el exploit correcto a aplicar en una prueba.
- Verificar remediación.

- **Nessus:** Es una herramienta muy completa que permite el escaneo de vulnerabilidades. Su fácil manejo a través de una interfaz Web, brinda la recopilación de amenazas detectadas aprovechando su gran número de plugins lo que posibilita un resumen detallado que brinda una descripción, sugerencia de solución y referencias sobre problemas encontrados de especial atención en un sistema informático

- **OpenVAS:** Es una herramienta muy completa que se constituye como la evolución de Nessus. Integra una interfaz a través de la web con la que se gestionara de manera centralizada las vulnerabilidades presentadas en diferentes sistemas.

- **NeXpose Community:** Es un escáner que gestionar las vulnerabilidades durante todo su ciclo de vida. Una característica bastante representativa y llamativa de la aplicación es su facilidad de integración con Metasploit, lo que permitirá explotar las vulnerabilidades a través de la funcionalidad del otro programa.

- **Nmap:** Se constituye como una herramienta para la exploración de la red, siendo de gran utilidad para las labores de auditoria de seguridad. Los resultados que brinda la ejecución de un análisis pueden incluir los equipos en la red, servicios, sistemas operativos, filtros de paquetes o cortafuegos.

- **P0f:** Aplicación de gran utilidad y que trabaja en un modo pasivo orientado hacia la recopilación de información referente al Sistema Operativo de las máquinas que se encuentran conectadas al sistema, a las que se encuentra conectado el sistema e incluso a aquellas remotas a las cuales no se tiene alcance. Su gran potencia puede arrojar datos como el proveedor de Internet del equipo remoto.

- **Pangolin:** Potente herramienta para evaluar la seguridad en bases de datos haciendo uso de ataques de Inyección SQL. En principio, detecta las vulnerabilidades en aplicaciones web y saca provecho de éstas para realizar el ataque y brindar al usuario toda una gama de opciones para el manejo de la información obtenida; se puede devolver sesiones, bases de datos, credenciales de acceso, extraer privilegios, copias de seguridad, entre otros.

- **SNMPcheck:** Comando de enumeración para dispositivos SNMP que provee una salida legible y en un formato amigable para el usuario que es útil tanto para los Penetration Test como para la monitorización del sistema.

- **SQLmap:** Una de las herramientas de pentesting más utilizadas para automatizar las pruebas relacionadas con ataques de inyección SQL[26]. Algunas de sus características son:

    - Realiza peticiones a partir de parámetros de URL indicada, por cualquier método (GET, POST, cookies).
    - Soporte para la mayoría de sistemas de gestión de bases de datos, soporte para conexión directa a la base de datos y soporte para enumerar de usuarios, contraseñas, hashes, privilegios, roles, bases de datos, tablas y columnas.
    - Reconocimiento automático de formatos de hash de contraseñas y soporte para crackearlos usando ataque basado en diccionarios.

- **THC-Hydra / XHydra:** Compatible con diversidad de protocolos, Hydra realiza ataques de fuerza bruta para intentar descifrar contraseñas de servicios remotos. Lo anterior se realiza con el objetivo de emitir un diagnóstico o concepto sobre las facilidades para obtener acceso a un sistema de manera no autorizada.

- **TheHarvester:** Como parte de la fase de recolección de información de un Penetration Test, esta herramienta brinda funcionalidades muy útiles a la hora de establecer la huella del cliente en Internet con el fin de determinar qué información puede obtener el atacante de la organización. Algunos de los datos que se recolectan a través de la aplicación corresponden a cuentas de correo, subdominios, hosts, nombres de empleados, puertos abiertos y banners desde recursos públicos como buscadores, servidores de llaves PGP y bases de datos[27].

- **Wireshark:** Es el más importante analizador de protocolos de red, siendo un gran aliado para la solución de problemas. Provee de capturas de paquetes comprensivas e informativas. Además, está en favor de un mejoramiento para el

[26] HACKPLAYERS. Top 10 de herramientas de hacking 2015. Disponible en: < http://www.hackplayers.com/2015/09/top-10-de-herramientas-de-hacking-de-2015.html>
[27] KALI. theHarvester. Disponible en: < http://tools.kali.org/information-gathering/theharvester>

desarrollo de otros protocolos de comunicación y es de gran utilidad para la educación en redes.

Herramientas descartadas para el proceso de evaluación

- **SiteDigger:** Herramienta que examina el cache de google para buscar vulnerabilidades, errores y problemas de configuración en sitios web. No se utiliza debido a que la última versión fue liberada en el año 2009. Además, las pruebas se centrarán en encontrar vulnerabilidades en la red empresarial, no sobre el software instalado en los sitios web.

- **ExifTool:** Es una herramienta que permite leer metadatos de archivos con soporte sobre gran variedad de formatos. Sin embargo, para el contexto de las pruebas actuales, no se realizarán análisis de metadatos para archivos, por lo cual no será aplicable en el proceso de evaluación.

- **Kismet:** A pesar de que es una aplicación potente y que permite efectuar gran cantidad de operaciones orientadas hacia la detección, escaneo e intrusión sobre redes inalámbricas se decidió optar por la suite de seguridad que se ofrece a través de aircrack-ng que está disponible en Kali Linux y que adicionalmente ofrece la posibilidad de analizar paquetes, crackear redes y realizar auditoria de redes.

- **InSSIDer:** Permite buscar redes inalámbricas brindando detalles sobre cada una de ellas. Sin embargo, no permite realizar otras tareas de análisis y auditoria, por tanto, se usa de preferencia la suite aircrack-ng.

- **InterNIC:** Portal desactualizado a partir de 2001. Existen alternativas que brindan herramientas informativas mucho más completas como es el caso de domaintools y sus registros whois detallados.

- **Host:** Tanto el comando “host” como “dig” pueden ejecutarse en sistemas operativos Unix, y en sí se usan para la misma funcionalidad. Sin embargo, en algunos casos como la resolución de problemas en DNS es preferible el uso de “dig” debido a que el formato de salida es más detallado mostrando los contenidos de los cuatro campos en la respuesta DNS, pregunta, respuesta, autoridad y secciones adicionales además de contar con más opciones de configuración.

- **Fierce2:** Escaner de dominios DNS, no aplicable para el alcance de las tareas que se efectuarán durante las pruebas de Pentesting para CJT&T Ingeniería de Software.

- **Dnsdict6:** Realiza enumeración de entradas DNS, permitiendo la búsqueda de subdominios invisibles para el público. Su funcionalidad se logra con otras aplicaciones presentes en Kali Linux, por tanto, no se usará durante las pruebas de Pentesting.

- **SNMPENUM y Snmpcheck:** A pesar de que puede ser una excelente herramienta de enumeración para visualizar los programas instalados, puertos a la escucha, dispositivos hardware, servicios en ejecución, entre otros, se prefirió utilizar nmap en razón de la gran cantidad de opciones que brinda para observar que tan expuesto se encontraba cada equipo en la red de la organización.

- **Alive6:** Escaner para detectar todos los sistemas que están en el rango de red. Pertenece a la suite THC-IPv6-Attack-Toolkit de Kali Linux. Se pueden lograr los mismos resultados a través de la aplicación nmap.

- **MetaSploit, NeXpose y otros escáneres de vulnerabilidades:** Por trayectoria de Nessus y el fork de su versión antigua llamado OpenVAS son las opciones de preferencia para realizar el escaneo de vulnerabilidades en tanto ofrece estabilidad, rendimiento, facilidades para generar reportes fiables, filtros e interfaz limpia y clara, soluciones añadidas, auditoria sobre la red, entre otros. Además, éstos integran el framework de Metasploit para realizar dicho proceso.

- **Brutus, hydra y medusa:** No se estarán realizando ataques de fuerza bruta para obtener contraseñas ya sea de aplicaciones web o de servicios internos en ejecución sobre los equipos presentes en la red de comunicaciones de la organización.

- **Karmetasploit:** Permite crear puntos de acceso falsos para capturar contraseñas, recopilar información y realizar ataques contra el navegador de los clientes. No es algo que se busque comprobar sobre las pruebas realizadas. Esto implicaría que los empleados estén involucrados directamente y lo que se quiere es comprobar la seguridad en la red, no evaluar este tipo de situaciones que implicarían ingeniería social.

- **Havij, SQLMap, Pangolin: Herramientas de inyección SQL.** Se usan portales con soluciones de software confiables en sus sitios web como Mantis Bug Tracker, Microsoft Sharepoint o Wordpress entre otros. Por lo tanto, debido a su alto control de errores, no se ha visto la necesidad de utilizar este tipo de escáneres. Ahora, a nivel interno únicamente se manejan las aplicaciones que se encuentran en desarrollo para clientes y el servidor TFS cuyo portal se encuentra protegido y no se encuentran puntos para poder evaluar la seguridad. Sin embargo, si es muy importante que durante la navegación sobre estos sitios internos los datos viajen encriptados para evitar fugas de información.

- **Fgdump:** Herramienta para recuperar contraseñas en Windows, desafortunadamente solo aplica para Sistemas Operativos Windows hasta la versión Vista. Los equipos de la organización cuentan con Windows 7+, por lo cual la aplicación no será de utilidad.

- **Hashdump:** No se efectuarán pruebas con ataques Pass the hash para obtener acceso a un equipo a través de la cuenta de usuario y su respectivo hash.

7.4. EJECUCIÓN DEL PENETRATION TEST

7.4.1. Fase de Planeación y Preparación

Es el punto inicial y fundamental, en el cual de mutuo acuerdo con la organización se decide el grado de profundidad y precisión de pruebas a efectuar, las limitantes y límites y las herramientas operativas y metodológicas que se utilizarán. Una vez se tienen los puntos claros, se firma un acuerdo en el cual se consigne la información esencial teniendo claridad sobre las responsabilidades de cada parte. El resultado se puede encontrar en el Anexo A del presente documento.

Adicional a esto se define lo siguiente:

- Las pruebas se efectúan con el fin de establecer un diagnóstico sobre el nivel de seguridad en la organización.

- Los resultados obtenidos serán la base para las políticas y procedimientos de seguridad a implementar en la organización.

- Las pruebas a realizar se efectuarán exclusivamente en horario no laboral. Si se hace en horario de oficina será con previa notificación a la gerencia.

- Se buscará realizar un escaneo sobre todos los equipos de la red empresarial, sin un rango específico establecido.

- En el caso de explotar alguna vulnerabilidad, verificar la posible escalada de privilegios e informar con antelación a la gerencia. En caso de que información sensible esté comprometida se deberá recibir autorización para el acceso a dichos datos.

- Se autorizan pruebas sobre el sitio web de la organización.

- No se realizan pruebas que impliquen ingeniería social.

7.4.2. Fase de Evaluación

Durante la fase de evaluación se efectuarán las pruebas de penetración correspondientes a los sistemas cuyo nivel de seguridad será evaluado. Para esto, se tomará como base el estándar PTES (Penetration Test Execution Standard), para lo cual se ha definido la siguiente forma de proceder:

- **Recolección de información:** En este punto se realizará un reconocimiento sobre los objetivos de evaluación, esto ayudará a establecer un panorama general que podría ser clave para la producción de planes estratégicos de ataque. Se tendrán en cuenta las siguientes fuentes de información:
    - **OSINT:** Obtención de información de origen público.
    - **Footprint de Internet:** Reconocimiento de información de la compañía que se encuentre disponible desde Internet.
    - **Footprinting:** Reconocimiento activo y pasivo de información correspondiente a la infraestructura física y lógica de la organización desde una perspectiva externa e interna.

- **Escaneo de Vulnerabilidades:** Mediante el uso de aplicaciones de terceros confiables, se realiza un escaneo de los sistemas y las redes para verificar cuales son las posibles vulnerablilidades que podrían ser aprovechadas por un atacante.

- **Análisis de Vulnerabilidades:** Posterior al escaneo, se realiza un análisis sobre las vulnerabiliades priorizando aquellas de mayor impacto, contrastando sobre las posibles medidas que puedan mitigar cada amenaza asociada.

- **Vectores de ataque:** Define como el atacante podría utilizar los puntos vulnerables de la infraestructura organizacional para efectuar una ofensiva sobre los activos más importantes.

- **Explotación:** Hace uso del conocimiento de las vulnerabilidades detectadas sobre los sistemas para explotarlas de manera controlada, con el único fin de verificar y no de afectar los activos de la organización.

7.4.2.1. OSINT: Definida como la inteligencia desde fuentes abiertas, es de gran ayuda para analizar información obtenida desde orígenes o sitios de acceso público. Este proceso tiene como principal objetivo recolectar información que se encuentre actualizada y que sea relevante desde el punto de vista del atacante y la competencia. Se deben establecer criterios de búsqueda estratégicos para que esta fase genere resultados adecuados.

- **Información Corporativa:** La información de un objetivo particular debería incluir aquella disponible a través de sitios de entidades estatales. En este sentido, se define que se deben realizar búsquedas en entidades de este tipo pertenecientes al municipio, departamento y país en busca de información que pueda contener aspectos relevantes con respecto a personas involucradas en la entidad. Tras realizar una búsqueda exhaustiva se realizaron los siguientes hallazgos:

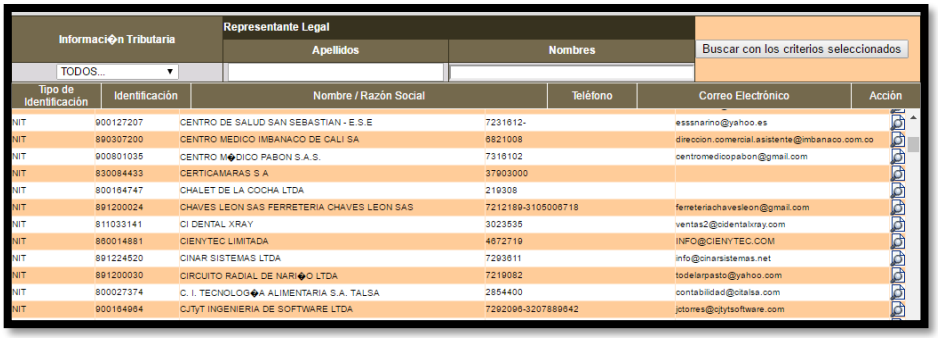
Se realiza búsqueda en Google con el siguiente filtro “cjtyt cámara de comercio pasto”. Se detectó que existe información actualizada en el portal de la Universidad de Nariño.

Figura 1. Búsqueda Corporativa en Google

Fuente: Buscador Google

Se procede al ingreso en esa página, encontrando un registro de proveedores de la Universidad, entre éstos “CJTyT Ingeniería de Software”.

Figura 2. Registro de Proveedores Universidad de Nariño



Fuente: Universidad de Nariño (apolo.udenar.edu.co)

Al dar clic sobre la lupa ubicada al lado derecho del registro, se observa que se abre un documento PDF al cual se puede acceder a través de este enlace, con información sensible como la siguiente:

- NIT de la Empresa.
- Teléfonos.
- Correo electrónico.
- Nombre completo del Representante Legal.
- Identificación del Representante Legal.
- Cuenta Bancaria de la empresa.

Se examina el Registro Único Empresarial y Social de Cámaras de Comercio (RUES), el cual arroja coincidencias al ingresar parte de la razón social de la empresa (“CJT&T”).

Figura 3. RUES CJT&T Ingeniería de Software

Fuente: RUES (www.rues.org.co)

Figura 4. Registro Mercantil CJT&T Ingeniería de Software

Fuente: RUES (www.rues.org.co)

Tras dar clic en el botón “RM”, se arroja información pública sobre la empresa como:

- Número de matrícula.
- NIT.
- Tipo de Organización.
- Cantidad de Empleados.
- Actividad Económica.

En la web de einforma, también se pudo obtener información referente a la empresa como se indica en la siguiente imagen:

Figura 5. Información empresarial desde einforma

Fuente: einforma (www.einforma.co)

- **Información sobre Ubicación:** La ubicación física de la empresa u organización representa un dato fundamental en este proceso de inteligencia. Los sitios públicos frecuentemente se podrían ubicar utilizando los motores de búsqueda.

Tras realizar la búsqueda en los principales motores como Google, Bing, Yahoo y Ask, se obtuvo un resultado relevante en éste enlace y además en la página principal de la empresa, que ayudó a determinar la ubicación física exacta de la empresa.

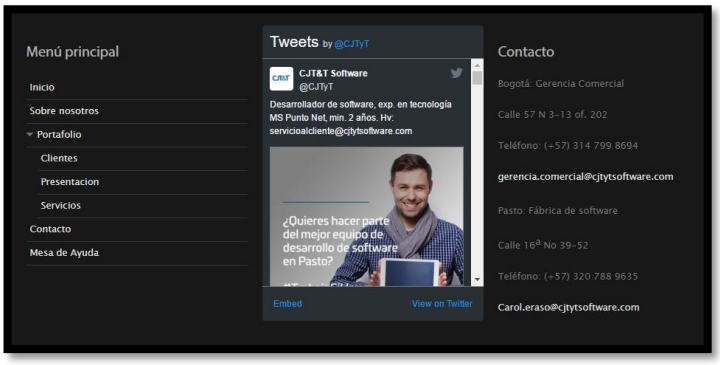
Figura 6. Búsqueda de localización de la empresa en Bing

Fuente: Buscador Bing

Figura 7. Resultado de búsqueda localización de la empresa

Fuente: Información Empresas (www.informacion-empresas.co)

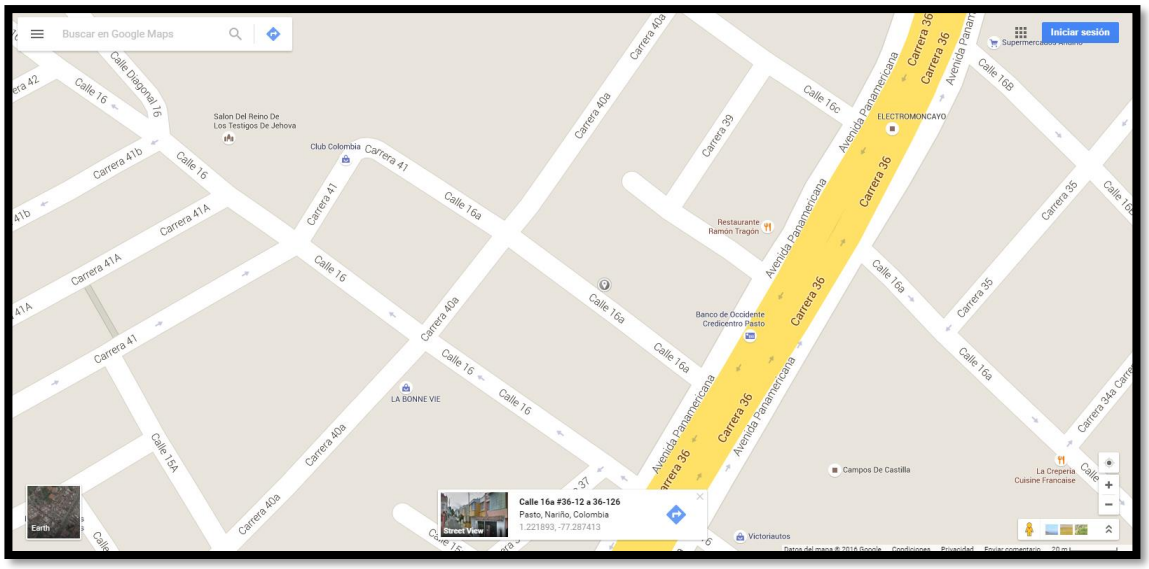
Figura 8. Información de localización de la empresa en la página corporativa



Fuente: Página Corporativa CJT&T (www.cjtytsoftware.com)

Se identifica que la posible dirección sería “Calle 16ª No. 39-52 B/Santa Ana”. Tras realizar la verificación de Google Maps, se señaló una ubicación aproximada como se muestra a continuación:

Figura 9. Geolocalización CJT&T Ingeniería de Software



Fuente: Google Maps

Se observó que existe un registro del sitio en Street View, y al examinar dicha información se pudo navegar y llegar hacia la dirección objetivo.

Figura 10. CJT&T en Street View

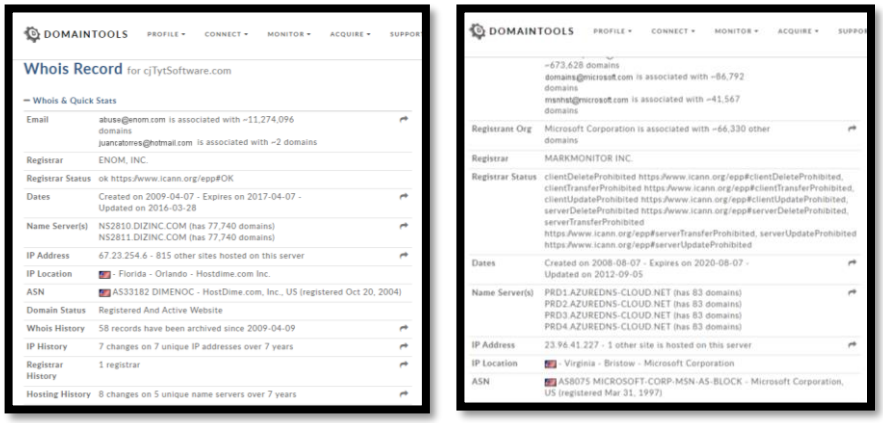
Fuente: Google Street View

- **Ubicación del Centro de Datos:** El descubrimiento sobre blancos estratégicos orientados desde el sitio web de la empresa, documentos públicos donde se pueda encontrar información de ésta, registros de terrenos u otros resultados a través de motores de búsqueda pueden dar claves para identificar objetivos potenciales.

En este punto se analizan los tres sitios web de la empresa que se pudieron encontrar a través de los motores de búsqueda:

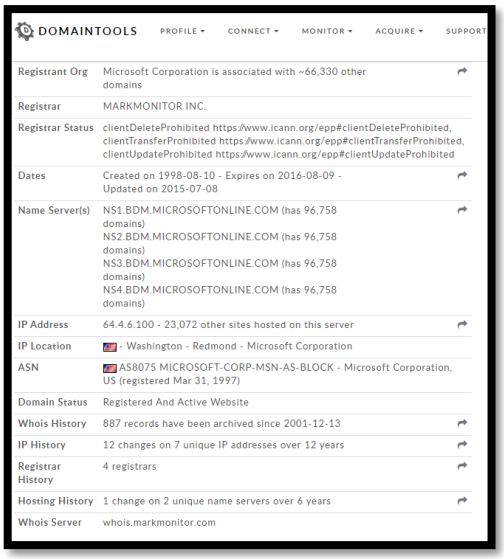
  - http://cjtytsoftware.com
  - http://cjtyt-cloud-jdk.cloudapp.net/
  - https://cjtyt-public.sharepoint.com/

Figura 11. Registros Whois páginas corporativas 1



Fuente: Domaintools (www.domaintools.com)

Figura 12. Registros Whois páginas corporativas 2



Fuente: Domaintools (www.domaintools.com)

En este punto, se pudo determinar que los sitios web públicos de la empresa están hospedados a través de servicios hosting externos los cuáles ubican sus servidores en Estados Unidos. De acuerdo a la información extraída a través de los DNS de las páginas Web se obtuvo que los proveedores son:

- Hostdime
- Microsoft

Ahora, con respecto a documentos públicos los cuales se pudieron identificar revisando los resultados de las búsquedas “cjt&t ingeniería de software pdf” y “cjt&t ingeniería de software doc”, fue posible recopilar los siguientes enlaces relevantes:

- JIISIC: http://jiisic12.inf.pucp.edu.pe/libros/libro-completo-jiisic12.pdf.
- Invitación pública, Nariño Vive Digital: http://contratacion.udenar.edu.co/wp-content/uploads/2014/08/EVALUACION-TECNICA-INVITACION-PUBLICA-N%C2%B0-169-2014.pdf.
- Convocatoria, Nariño Vive Digital: http://www.parquesoftpasto.com/wp-content/uploads/AVISO_DE_CIERRE.pdf.
- Evaluación convocatoria, Nariño Vive Digital: http://www.parquesoftpasto.com/wp-content/uploads/PDCMC_Nar_GEL_003_E3_A7_ActaEvaluacion1.pdf.

De estos enlaces se pudieron identificar los siguientes puntos relevantes:

- La empresa se ha presentado en licitaciones de empresas públicas y privadas como proveedor oferente de equipos de cómputo y licencias de software.
- La empresa presta el servicio de desarrollo de Software a la medida.
- La empresa apoya los procesos de investigación en favor del fortalecimiento de la industria del Desarrollo de Software.

- **Zona horaria:** Tener claridad sobre la zona horaria de la organización puede permitir estimar las horas laborales, con lo cual el equipo de evaluación podría definir el tiempo más idóneo para efectuar sus pruebas.

La página web de la empresa confirma la ubicación de ésta, la cual establece la Gerencia Comercial en la ciudad de **Bogotá** y la Fábrica de Software en la ciudad de **Pasto**. Por tanto, dado el país, se puede determinar que la zona horaria corresponde a **(UTC -05:00) Bogotá, Lima, Quito, Rio Branco.**

- **Reuniones fuera de la oficina:** Se identifica que los sitios web oficiales de la empresa incluyendo sus cuentas en redes sociales no indican ningún tipo de información correspondiente a reuniones recientes o futuras con empleados, proveedores, partners o clientes.

- **Productos y Servicios:** En el portal oficial de la página de la empresa (www.cjtytsoftware.com), sección de servicios se listan aquellos que se ofrecen actualmente:

- Integraciones de software comercial.
- Desarrollo de software a la medida.
- Tercerización de servicios.
- Mantenimiento de aplicaciones de software.
- Migración de aplicaciones de software.

- **Comunicaciones Corporativas:** De acuerdo al portal oficial de la empresa se puede identificar que existen dos números de teléfono correspondiente a dos departamentos de la empresa así:

  - Gerencia Comercial: (+57) 314 799 8694.
  - Fábrica de software: (+57) 320 788 9635.

- **Aperturas de trabajo:** Buscar por ofertas o publicaciones de trabajo a través del sitio corporativo o un buscador de trabajos puede proveer visión de valor sobre cómo trabaja internamente el objetivo. Es una práctica frecuente incluir información con respecto a actuales o futuras implementaciones de tecnología. Recolectar esta información puede proveer visión sobre elementos potenciales de interés para un atacante.

Figura 13. Ofertas de Trabajo de CJT&T Ingeniería de Software

Fuente: Computrabajo (www.computrabajo.com)

Se identifica que la empresa realiza regularmente ofertas de trabajo a través de sus redes sociales y de la página Computrabajo.

- **Perfiles en redes sociales:** Las redes sociales activas y los usuarios que las siguen pueden permitir inferir muchos aspectos con respecto a los empleados, por ejemplo, relaciones, intereses, intercambios, gustos e incluso creencias religiosas. Si el analista se adentra mucho más en este punto, podría ser capaz de determinar el grado de conocimiento o prestigio de la persona en la organización. A continuación, se listan las redes sociales activas de la empresa CJT&T Ingeniería de Software:

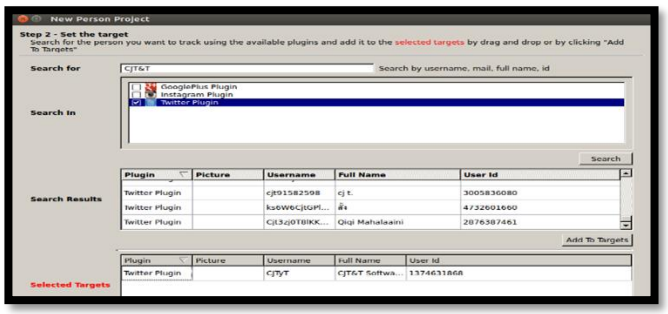
    - Facebook: https://www.facebook.com/cjtytsoftware/
    - Twitter: https://twitter.com/cjtyt/
    - Linkedin: https://www.linkedin.com/company/cjt&t-ingenier%C3%ADa-de-software

- **Cree.py:** Es una herramienta libre que permite automatizar la tarea de recolección de información desde Twitter. Como adición, es capaz de obtener datos de geolocalización.

De esta manera, se realizó la instalación de cree.py en Linux Ubuntu. Para contar con las fuentes más actualizadas se procedió a descargarlo desde su página oficial. Después, se descargó su código fuente y plugins. Posteriormente, se siguen las instrucciones de instalación verificando el cumplimiento de requisitos para finalmente ejecutar el programa.

En este caso, el enfoque se ha centrado únicamente en la red social Twitter dado que es la única que se encuentra activa a nivel empresarial y que es compatible con la aplicación. Se ha realizado la configuración del plugin siguiendo el asistente y accediendo a twitter con una cuenta preexistente. A continuación, se procede a ejecutar el proyecto, donde se ingresan términos claves para que el programa realice su tarea de filtrado. Posterior a esto, se selecciona el perfil deseado y el programa procede con la búsqueda.

Figura 14. Analizando CJT&T en Cree.py



Fuente: El autor

De manera desafortunada, tal y como se observa en la imagen a continuación, dada la escasa actividad de la cuenta las pruebas no han arrojado resultados.

Figura 15. Resultados de la búsqueda en Cree.py

Fuente: El autor

7.4.2.2. Footprint de Internet: El footprint o huella de internet permite obtener información externa y que se encuentre en fuentes de acceso público. Su objetivo es reconocer la infraestructura del objetivo, cuya base permitirá ser insumo para fases posteriores.

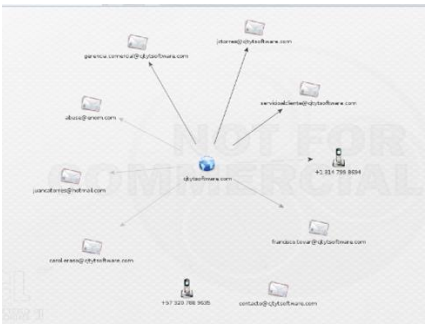
- **Direcciones de correo:** Aunque puede parecer inútil, es un gran punto de inicio para proveer información valiosa sobre el contexto y entorno en que se desenvuelve el objetivo de análisis. Las notaciones, convenciones y otros aspectos relacionados pueden permitir identificar nombres potenciales para uso de manera posterior.

- **Maltego:** Es una herramienta que permite automatizar las tareas de recolección de información de manera inteligente. Posee una versión gratuita y otra comercial. En este caso se hará uso de la versión gratuita para efectuar las pruebas, teniendo claridad sobre algunas limitantes que se supone no serán obstáculo para obtener los resultados deseados.

La gran ventaja de esta aplicación es sin duda la facilidad para agrupar la información recolectada en un formato fácil de entender y manipular, lo que permite ahorrar tiempo efectuando tareas de descubrimiento o mapeo.

Se ha accedido a la interfaz, y una vez allí se ha creado un nuevo grafo. Se ha escogido un escaneo básico para la recolección de correos. Tras esta tarea se ha dado clic en el dominio central y también se ha elegido adicionar la búsqueda de números telefónicos. El resultado se indica a continuación:

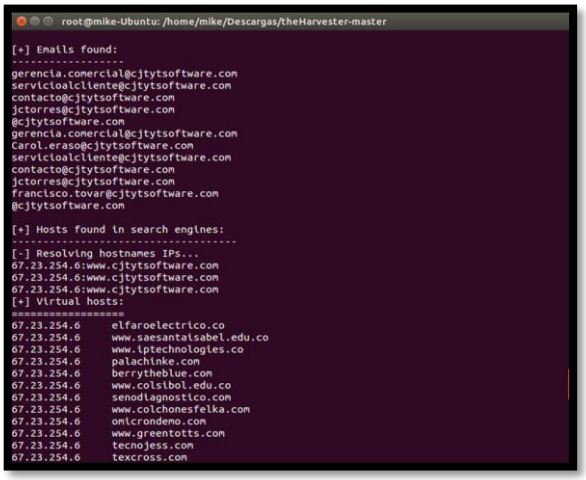
Figura 16. Recolección de correos mediante Maltego



Fuente: El autor

- **TheHarvester:** Para corroborar los resultados recopilados por Maltego, se ha ejecutado el Script TheHarvester que también permite recolectar cuentas de correo y nombres de subdominios desde diferentes fuentes públicas. Es más simple, pero muy efectiva. En la imagen que se muestra a continuación se indican los resultados que ha arrojado la ejecución de este script.

Figura 17. Recolección de correos mediante TheHarvester



Fuente: El autor

- **Información archivada:** Existe gran cantidad de ocasiones en las cuales no es posible acceder a información de un sitio web debido al hecho que el contenido puede no estar disponible desde su fuente original. Estar posibilitado para acceder a copias archivadas de esta información permite acceder a información del pasado.

Figura 18. Página corporativa CJT&T hasta el año 2011

Fuente: Archive.org

Hay muchas formas de acceder a esta información archivada. Esto principalmente significa utilizar los resultados en cache desde Google. Se ha utilizado como recurso alterno la información archivada en la página **archive.org**. A través de esta serie de imágenes, se observa la evolución de la página Web corporativa como una evidencia de posibles cambios recientes en la imagen corporativa, servicios, empleados, entre otros.

Figura 19. Página corporativa CJT&T hasta el año 2014

Fuente: Archive.org

Figura 20. Página corporativa CJT&T hasta marzo del año 2016

Fuente: Archive.org

Figura 21. Página corporativa CJT&T actualmente

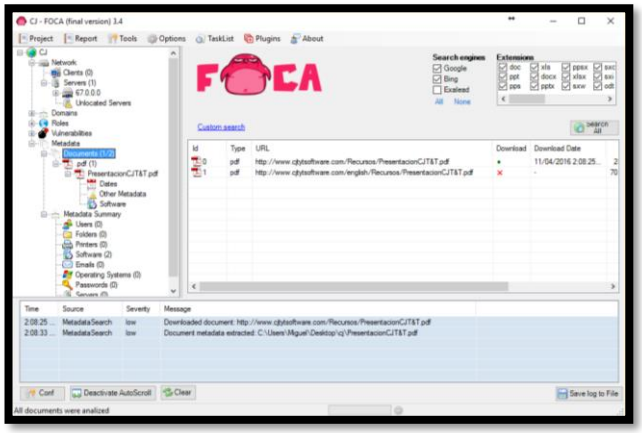
Fuente: CJT&T Ingeniería de Software (cjtytsoftware.com)

- **Datos Electrónicos:** La colección de datos electrónicos en respuesta directa al reconocimiento y recolección inteligente debe ser enfocada en el objetivo de negocio o individuo.

- **FOCA:** Es una herramienta que lee metadatos de un gran rango de documentos y formatos multimedia. Este programa extrae los nombres de usuario relevantes, rutas, versiones de software, detalles de impresión y correos electrónicos. Puede ser ejecutado sin necesidad de descargar archivos individualmente.

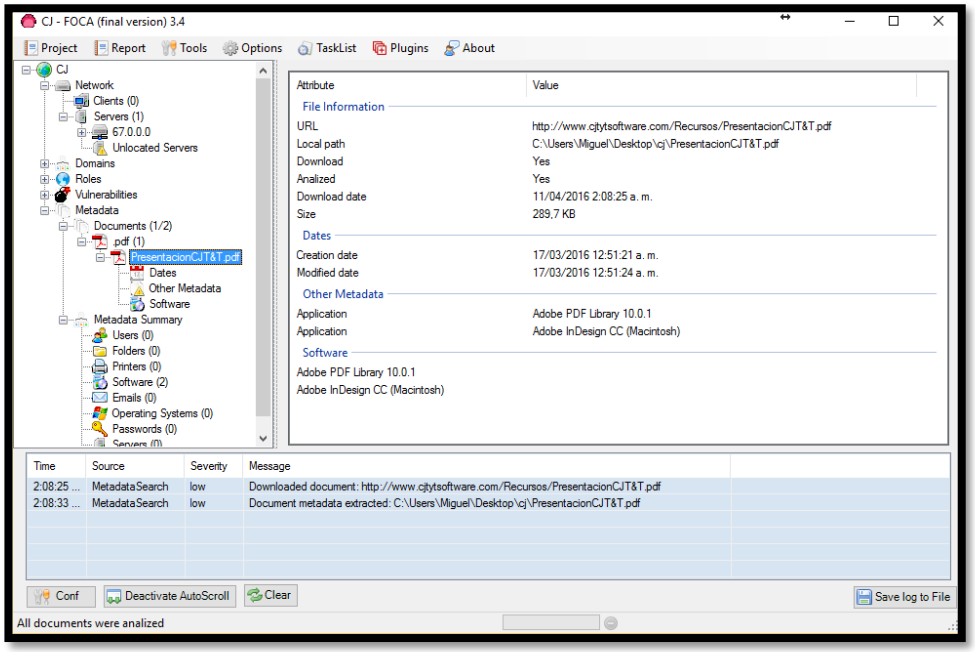
Se realizó la descarga del programa y su instalación. Se crea un nuevo proyecto apuntando hacia el dominio cjtytsoftware.com. Tras realizar la búsqueda únicamente se pudo encontrar un documento PDF el cual al ser analizado no brindó pistas útiles para posteriores fases tal y como se muestra a continuación.

Figura 22. Búsqueda de documentos en el dominio cjtytsoftware.com



Fuente: El autor

Figura 23. Análisis de metadatos a documentos en cjtytsoftware.com



Fuente: El autor

- **Descubrir redes WLAN:** El descubrimiento de redes inalámbricas puede permitir su verificación para determinar su nivel de seguridad posteriormente. Realizar la enumeración consiste en una tarea que debe abarcar la identificación de:

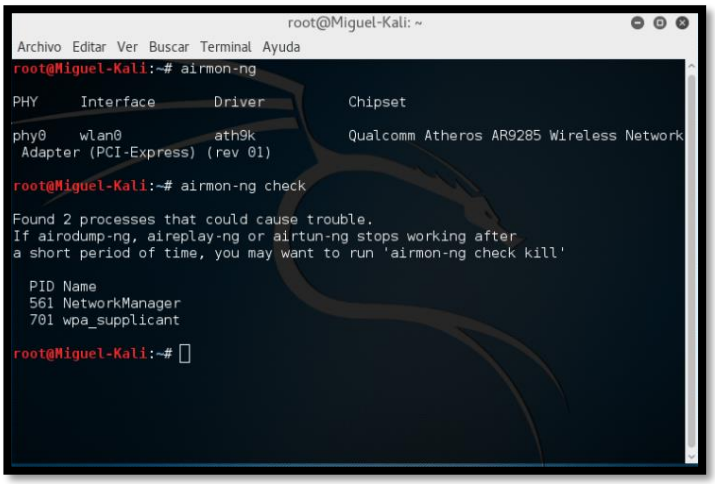
    - WLAN sin protección.
    - WLAN-WEP.
    - WLAN-WPA.
    - WLAN-LEAP.
    - WLAN-802.1x.

Las herramientas requeridas para enumerar esta información se mencionan a continuación:

- **Airmon-ng:** Usado para habilitar el modo monitor en interfaces inalámbricas. De igual manera, es útil para retornar al modo cliente.

En primer lugar, se verifica que el adaptador inalámbrico se encuentre en el modo monitor. Para esto, se debe ingresar el comando airmon-ng sin parámetros para mostrar el estado en el que se encuentran las interfaces.

Figura 24. Verificación de modo monitor tarjeta inalámbrica



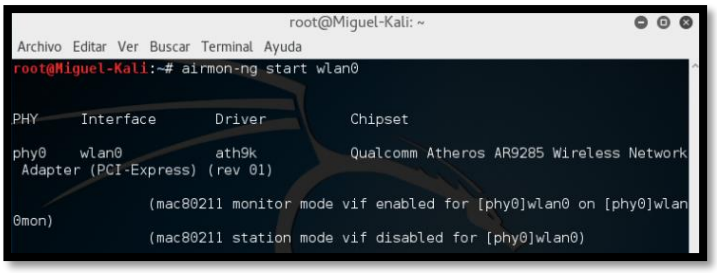
Fuente: El autor

Se denota que la interfaz es wlan0, lo cual significa que aún no se ha activado el modo monitor. Se ejecuta el comando airmon-ng check para verificar si existe algún

proceso que impida el correcto desempeño de la aplicación y si es necesario se ingresa en consola airmon-ng check kill para matar los procesos correspondientes.

Ahora, para activar el modo monitor se ingresa el comando: airmon-ng start wlan0, asumiendo que wlan0 es la interfaz del adaptador inalámbrico.

Figura 25. Activación modo monitor adaptador inalámbrico

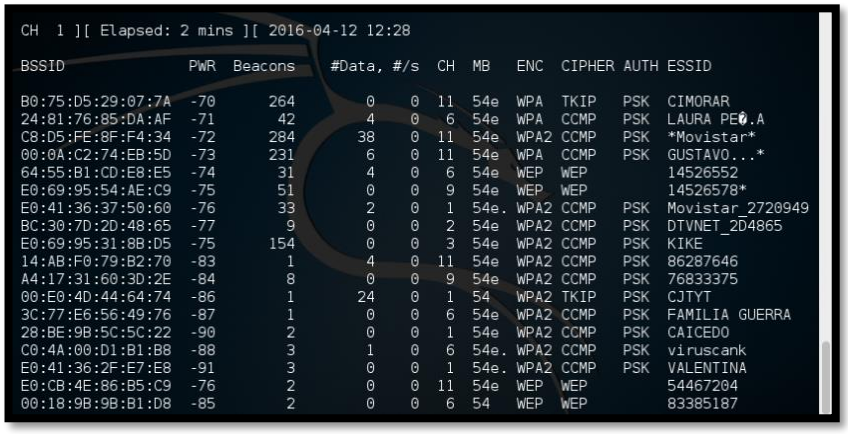


Fuente: El autor

- **Airodump-ng:** Es un sniffer de paquetes que ubica el tráfico en archivos de captura o vectores y muestra la información con respecto a las redes inalámbricas.

Es posible mostrar una lista de los puntos de acceso detectados y una lista de los clientes conectados a través del comando airodump-ng –w output wlan0, considerando wlan0 como la interfaz inalámbrica.

Figura 26. Puntos de acceso inalámbrico y clientes conectados



Fuente: El autor

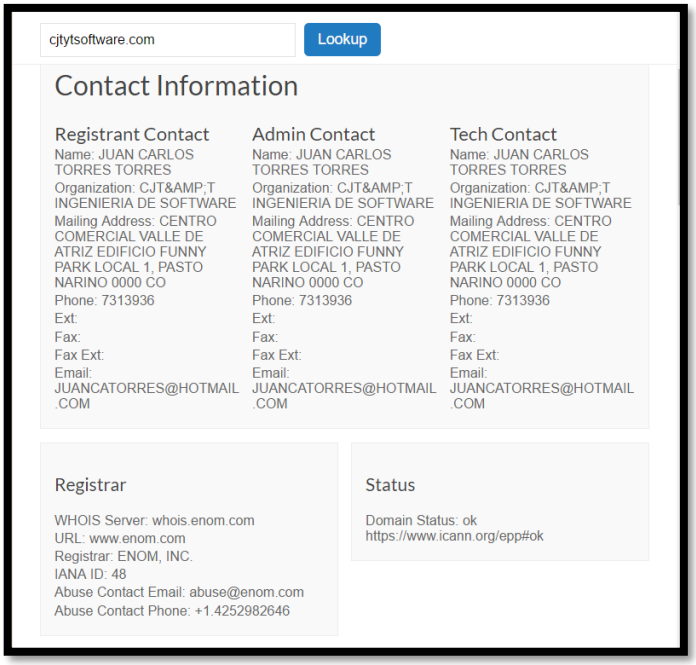
El anterior proceso claramente permite identificar varios puntos importantes sobre las redes inalámbricas como encripción, algoritmo, autenticación y nombre, entre otros, posiblemente insumos importantes para un análisis que se realice durante las etapas siguientes.

7.4.2.3. Footprint externo: Representa la tarea de recolección de respuestas basadas en un objetivo desde la interacción directa con una perspectiva externa. La meta es obtener tanta información del objetivo como sea posible.

En primer lugar, se determina cuál de los servidores WHOIS contiene información útil. Teniendo a mano el dominio objetivo, se localiza la información de registro.

Dada la situación sobre la estructura de la información como un árbol jerárquico, ICANN o IANA pueden permitir el registro autoritativo para todos los dominios de alto nivel como un gran punto de partida para todas las consultas manuales WHOIS posteriores.

Figura 27. Información de Registro de dominio

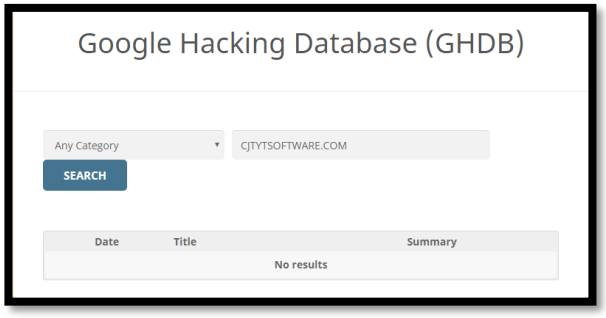


Fuente: ICANN

- **Reconocimiento del sitio:** Siendo un gran indicio sobre vulnerabilidades detectadas a través de diferentes herramientas en Internet, Google Hacking

Database es un importante sitio que permite establecer un reconocimiento activo y pasivo de un portal específico disponible a un solo clic de distancia. Debería representar una prioridad para establecer correcciones a la brevedad posible ante el peligro de información pública sobre debilidades presentes en los sistemas de la organización.

Figura 28. Búsqueda de registros de sitios corporativos en GHD

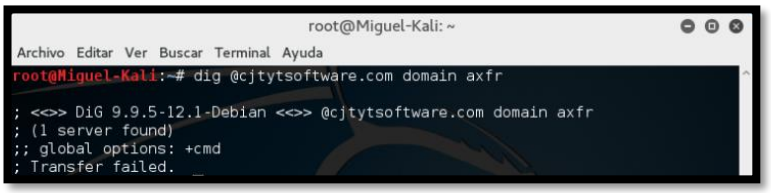


Fuente: Google Hacking Database

- **Footprinting activo:** Siguiendo la misma línea de trabajo se complementan las pruebas realizadas a través de la recopilación de información a través de la interacción directa con el objetivo en la búsqueda de datos relevantes producto del análisis de los DNS.

- **Transferencia de zonas:** Es un tipo de transacción DNS diseñado para replicar las bases de datos conteniendo datos a través de una serie de servidores. Pueden ser completas e incrementales. Hay numerosas herramientas para probar la habilidad de realizar una transferencia de zona DNS, en este caso las comprobaciones se realizaron por medio de “dig”.

Figura 29. Ejecución del comando dig para transferencia de zonas.



Fuente: El autor

La ejecución del comando “dig @nombredeldominio domain axfr”, tiene como objetivo obtener los registros axfr (transferencia de zonas) teniendo como principal dato el nombre del dominio que en este caso corresponde a cjtytsoftware.com. Sin embargo, debido a la seguridad del servidor de alojamiento la solicitud fue rechazada como se indica en la Figura 29.

- **DNS Bruting:** Como es de conocimiento general, los DNS son usados para mapear las direcciones IP desde los nombres de host y viceversa. Por esta razón, se querrá comprobar si su configuración es insegura.

Es importante identificar fallas relacionadas con transferencias de zonas. A pesar de haberlo analizado previamente a través del comando “dig”, no está de más aprovechas las herramientas que proveen un escaneo completo de este punto con un valor añadido. La enumeración de DNS mediante aplicativos especializados no solo servirá para verificar la habilidad de realizar transferencia de zonas, también puede potencialmente descubrir nombres de host adicionales que no son conocidos comúnmente.

- **DNSEnum:** Utiliza como principal recurso los ataques de fuerza bruta a subdominios para enumerar los DNS. Como principales recursos para alcanzar el objetivo se vale de búsquedas inversas, listados de rangos de las redes del dominio y consultas WHOIS. Se ejecutó el comando “dnsenum –enum –f dns.txt cjtytsoftware.com” para analizar el dominio mencionado utilizando el diccionario generado por los creadores del script.

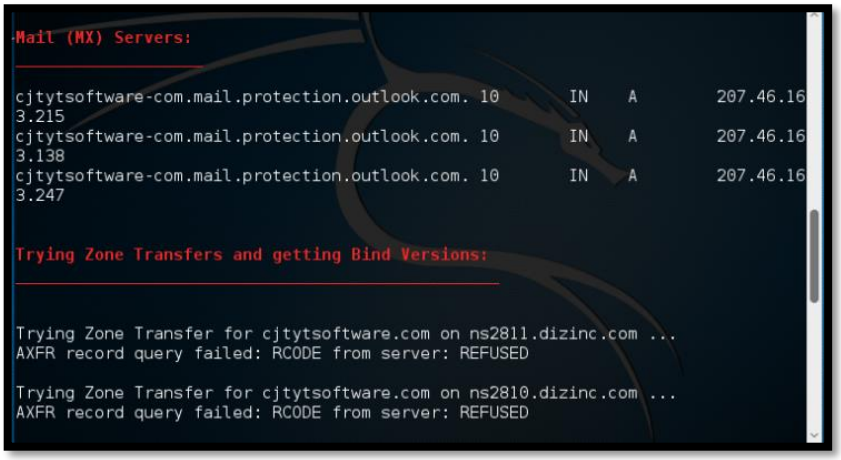
Figura 30. Direcciones de Host y Nameservers a través de DNSEnum

Fuente: El autor

En la Figura 30, se puede observar que se ha descubierto la dirección IP del dominio y los servidores de nombre.

Ahora, se muestran otros ítems entre los cuales se pueden apreciar los servidores MX y el intento por obtener los registros de transferencia de zonas, el proceso de estos últimos no es exitoso dadas las posibles restricciones establecidas por la compañía proveedora.

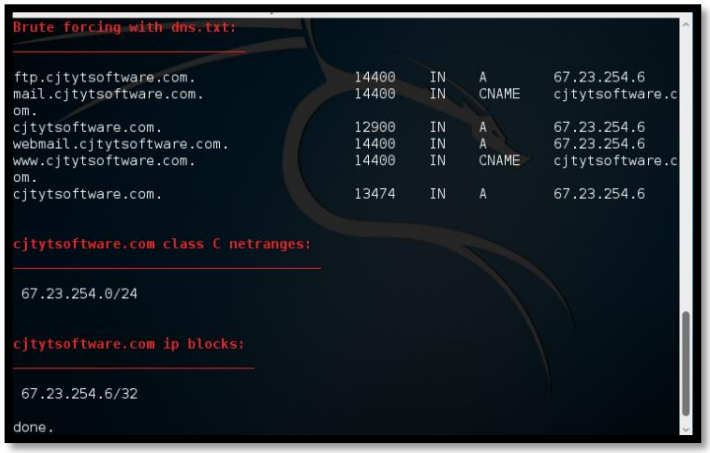
Figura 31. Servidores Correo y Transferencia de zonas DNSEnum



Fuente: El autor

Por último, se revelan datos muy útiles como los subdominios escaneados a través del diccionario indicado como parámetro en el comando.

Figura 32. Subdominios a través de DNSEnum



Fuente: El autor

- **Escaneo de puertos:** Se realiza a través de nmap el cual ofrece gran cantidad de opciones, sin embargo, para el escaneo de puertos se centrará en algunos comandos necesarios para la tarea.

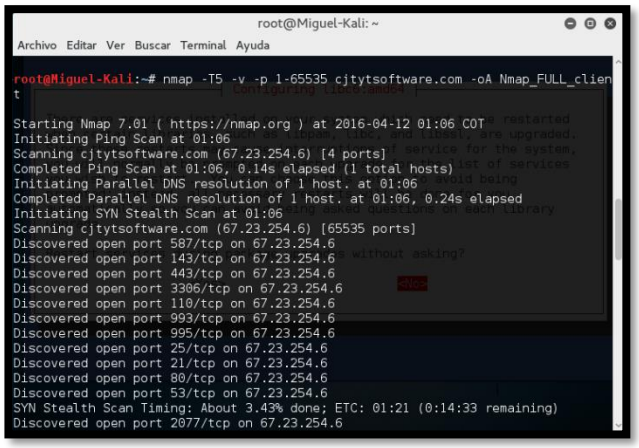
Basado en el dominio se escanearán los puertos TCP en un rango de 1 a 65535.

Figura 33. Escaneo de puertos aplicaciones externas a través de nmap

Fuente: El autor

Los resultados completos producto de este escaneo de puertos se pueden revisar en el Anexo D del presente documento.

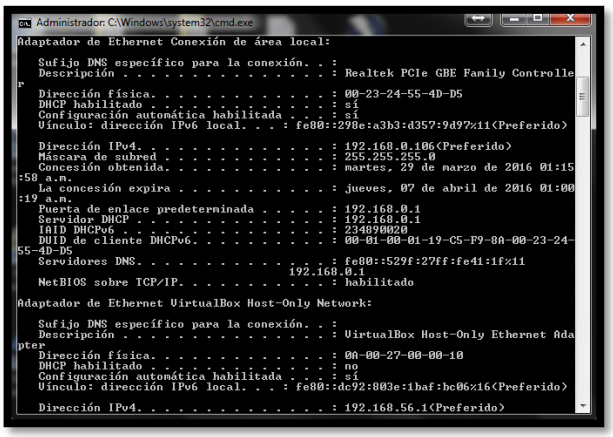
Figura 34. Ejecución escaneo aplicaciones externas a través de nmap



Fuente: El autor

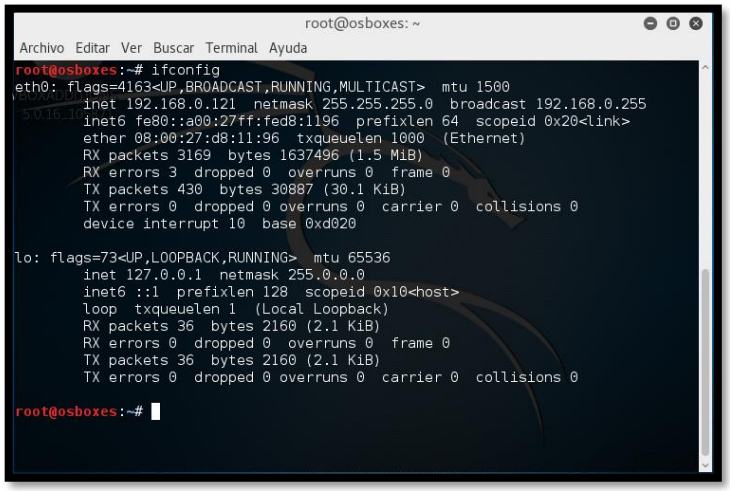
- **Footprint interno:** Previo a ejecutar algún tipo de auditoria o escaneo a través de nmap, es esencial conocer con seguridad cuál es la red que se está analizando. Por esto, una vez se establece conexión a la red interna de la empresa, lo primero que se hace es verificar si existe un servidor DHCP a través del comando ifconfig/ipconfig, con esto se podrá identificar la subred, la puerta de enlace, servidor DNS y nombre de dominio.

Figura 35. Ejecución ipconfig en Windows



Fuente: El autor

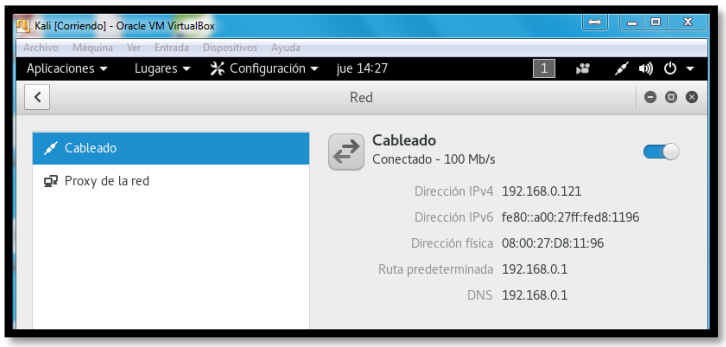
Figura 36. Ejecución ifconfig en Linux



Fuente: El autor

Entre más insumos de información sean tenidos en cuenta se tendrá mucha más certeza sobre el objetivo al cuál irá dirigido el análisis. Ahora, se extrae información desde Network Manager así:

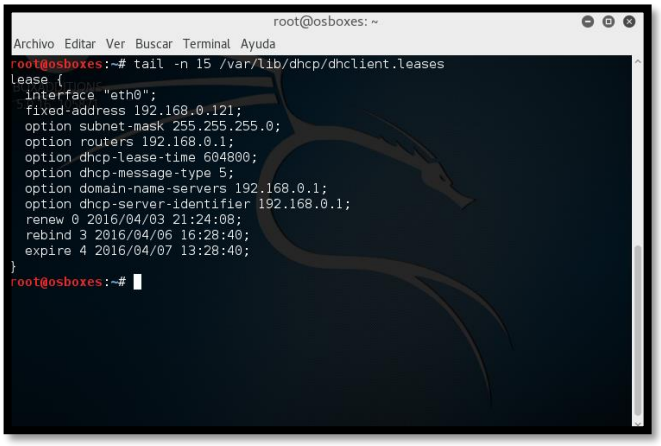
Figura 37. Información de red a través de Network Manager



Fuente: El autor

Para la identificación de servidores DNS se ejecuta el comando “tail –n 15 /var/lib/dhcp/dhclient.leases” como puede corroborar a continuación:

Figura 38. Descubrimiento de Servidor DNS

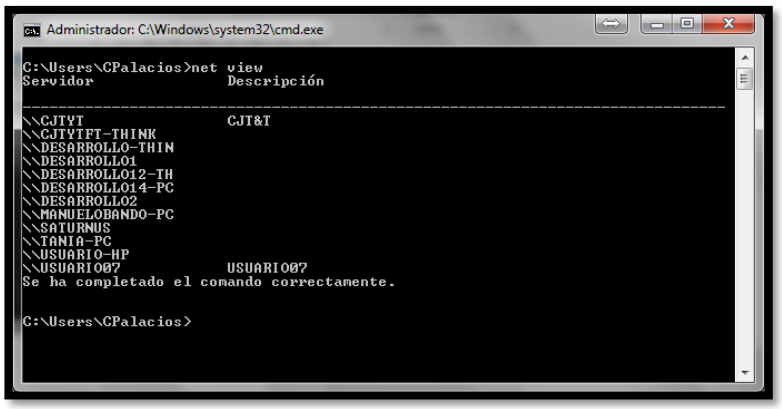


Fuente: El autor

Con esto, se puede determinar que la subred activa sería ***192.168.0.0/24*** con puerta de enlace, servidor DNS y DHCP apuntando a la dirección IP ***192.168.0.1***.

Para complementar este proceso, Windows a través de "netview" ofrece una herramienta invaluable para enumerar otros sistemas Windows en el dominio de broadcast.

Figura 39. Enumeración a través de net view



Fuente: El autor

Se realiza ping a los nombres de host para identificar IP y subredes. A continuación, se indica una recopilación de la información encontrada:

Tabla 5. Recopilación de datos de red

Nombre de host	IP	Subred	Puerta de Enlace
CJTYTFT-THINK	192.168.0.118	192.168.0.0/24	192.168.1.1
DESARROLLO-THINK	192.168.0.106	192.168.0.0/24	192.168.1.1
DESARROLLO1	192.168.0.115	192.168.0.0/24	192.168.1.1
DESARROLLO12-TH	192.168.0.157	192.168.0.0/24	192.168.1.1
DESARROLLO2	192.168.0.101	192.168.0.0/24	192.168.1.1
MANUELOBANDO-PC	192.168.0.185	192.168.0.0/24	192.168.1.1
SATURNUS	192.168.0.125	192.168.0.0/24	192.168.1.1
TANIA-PC	192.168.0.246	192.168.0.0/24	192.168.1.1
USUARIO-HP	192.168.0.121	192.168.0.0/24	192.168.1.1
USUARIO07	192.168.0.86	192.168.0.0/24	192.168.1.1
DESARROLLO14-PC	192.168.0.249	192.168.0.0/24	192.168.1.1
Fuente: El autor			

Figura 40. Ejecución en ping para cada nombre de host

Fuente: El autor

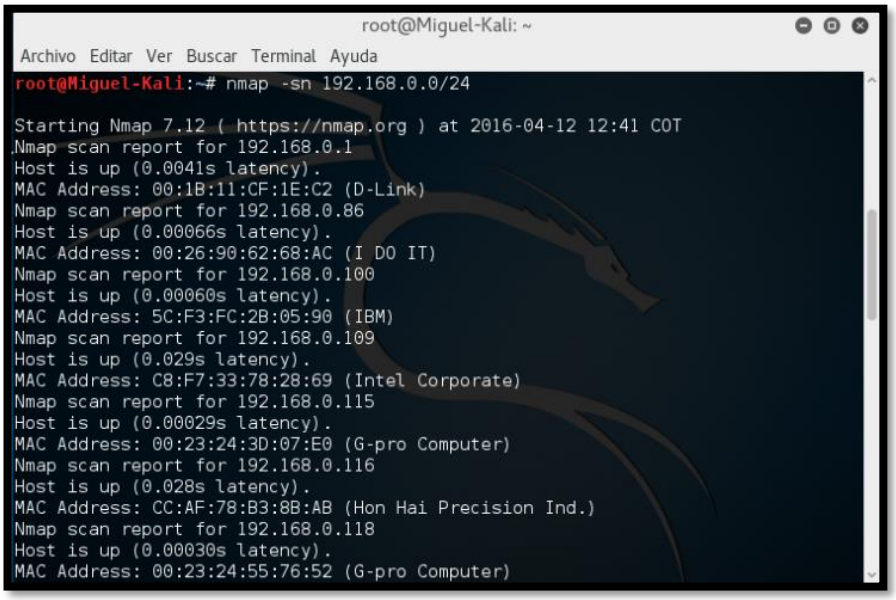
El punto importante de este proceso, es la identificación de la subred a la cual pertenecen los equipos, de esta manera se podrá realizar un escaneo más profundo con nmap.

- **Barridos de ping:** El proceso de huella activa interna comienza por medio de la identificación de sistemas activos a través de un barrido de ping para determinar la respuesta de los hosts.

Así tras ejecutar el comando “nmap –sn subred”, se obtuvieron los resultados que indican los hosts activos en la red. Debido a los cambios realizados en la organización a nivel locativo, se pueden consultar los barridos realizados durante dos periodos de tiempo distintos; en el Anexo E se encuentra la información

correspondiente al escaneo del 12 de abril mientras que en el Anexo I aquel realizado el 12 de mayo. Seguidamente, una evidencia del proceso:

Figura 41. Barrido de ping en la subred 192.168.0.0/24

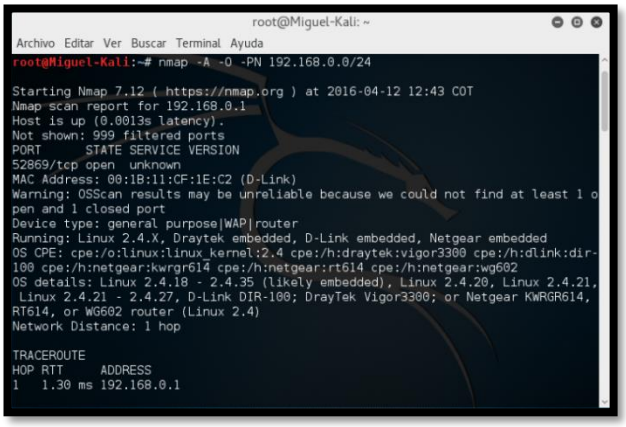


Fuente: El autor

- **Escaneo de puertos:** Un escaneo sobre los puertos en una red puede brindar un claro panorama sobre nuevos vectores de ataque. A través de información como puertos abiertos, traza, sistema operativo, entre otros, se podrá tener material suficiente para detectar vulnerabilidades en los sistemas posteriormente. Este proceso se facilita utilizando la aplicación nmap a través deel comando “nmap –A –O –PN subred”.

Además, debido al traslado de la empresa a otra ubicación se optó por realizar dos escaneos en distintos periodos de tiempo, sus resultados se pueden revisar en el Anexo F para el caso del 12 de abril y en el Anexo J para el 12 de mayo.

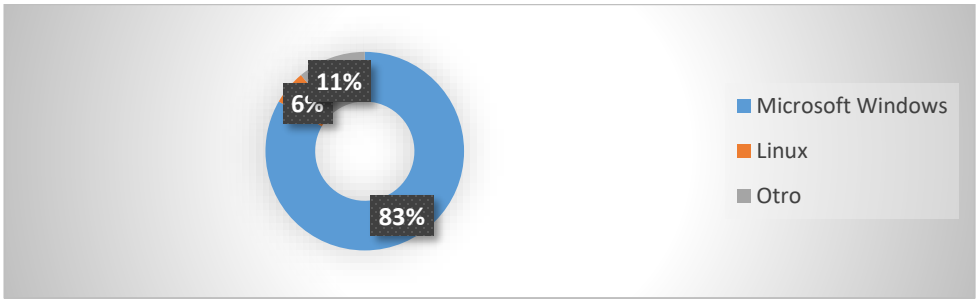
Figura 42. Escaneo de puertos en la subred 192.168.0.0/24



Fuente: El autor

De acuerdo al último escaneo de puertos realizado se pudo comprobar que existe la siguiente proporcionalidad con respecto a los Sistemas Operativos de los hosts activos en la organización:

Figura 43. Relación entre hosts activos y su sistema operativo



Fuente: El autor

El anterior gráfico refleja que en su mayoría prevalece el uso de Microsoft Windows con un 83%. De igual manera, de acuerdo al escaneo realizado a través de nmap se pudo identificar que los servidores también hacen uso de este Sistema en su versión Server. Este es un punto de partida relevante, ya que la identificación de este dato permite inferir que se debe tener mucho cuidado con el tema de las actualizaciones tanto del Sistema Operativo como de las aplicaciones en éste utilizadas debido a las continuas fallas de seguridad que se encuentran en sus productos.

Ahora, prosiguiendo con respecto al análisis de información relacionado con el escaneo de puertos se pudo extraer la siguiente relación entre los puertos y servicios activos con respecto a la cantidad de hosts detectados en la organización.

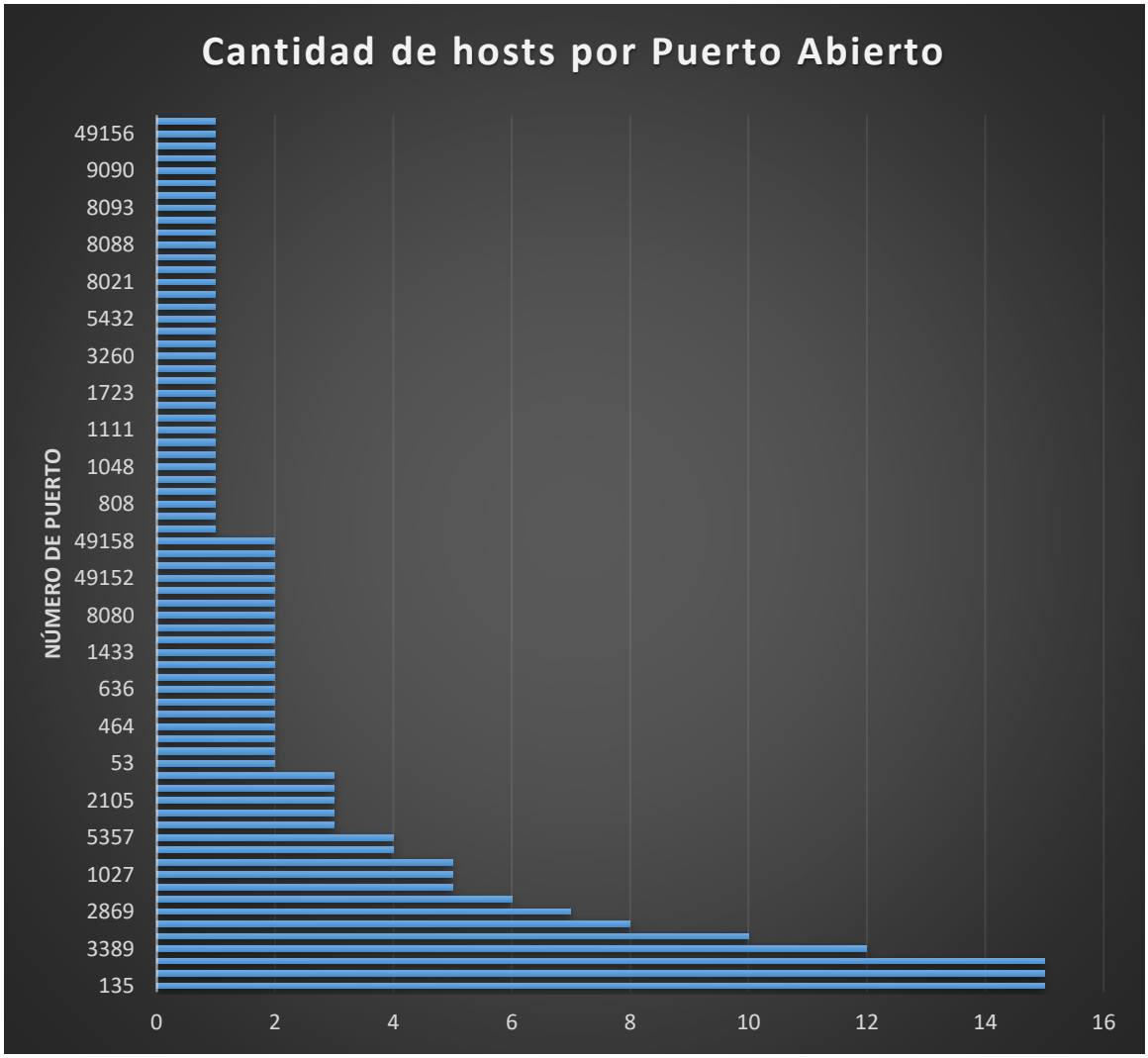
Tabla 6. Frecuencia de Puertos y servicios en los hosts de la organización

Puerto	Servicio	Cantidad de hosts
53	domain	2
80	http	10
81	http	1
88	kerberos-sec	2
135	msrpc	15
139	netbios-ssn	15
389	ldap	2
443	https	8
444	http	1
445	microsoft-ds	15
464	kpasswd5	2
554	rtsp	2
593	ncacn_http	2
636	tcpwrapped	2
808	ccproxy-http	1
1025	msrpc	5
	ssl/NFS-or-IIS	1
1026	msrpc	5
1027	msrpc	5
1028	msrpc	5
1033	msrpc	1
1034	msrpc	1
1048	msrpc	1
1056	msrpc	1
1057	msrpc	2
1060	msrpc	2
1082	msrpc	1
1111	lmsocialserver	1
1152	msrpc	1
1433	ms-sql-s	2
1521	oracle-tns	1
1723	pptp	1
1801	msmq	3
1947	http	1
2030	device2	1
2103	msrpc	3
2105	msrpc	3
2107	msrpc	3

Puerto	Servicio	Cantidad de hosts
2179	vmrdp	4
2869	http	7
3260	iscsi	1
3261	iscsi	1
3268	ldap	2
3269	tcpwrapped	2
3306	mysql	1
3389	ssl/ms-wbt-server	12
5357	http	4
5432	postgresql	1
5555	http	1
8009	ajp13	1
8021	http	1
8080	http	2
8081	http	1
8085	http	1
8088	http	1
8089	http	1
8090	http	1
8093	http	1
8400	http	1
9000	http	2
9001	http	1
9090	http	1
9091	http	1
10243	http	2
49152	http	1
	msrpc	1
49153	http	1
	msrpc	1
49154	http	1
	msrpc	2
49155	msrpc	1
49156	msrpc	1
49157	ncacn_http	2
49158	msrpc	2
49176	msrpc	1
Fuente: El autor		

Desde los datos contenidos en la tabla anterior, se puede dar cabida hacia la generación de un gráfico representativo donde se pueden definir la mayor frecuencia de puertos abiertos en los equipos de la organización.

Figura 44. Cantidad de Host por Puerto Abierto

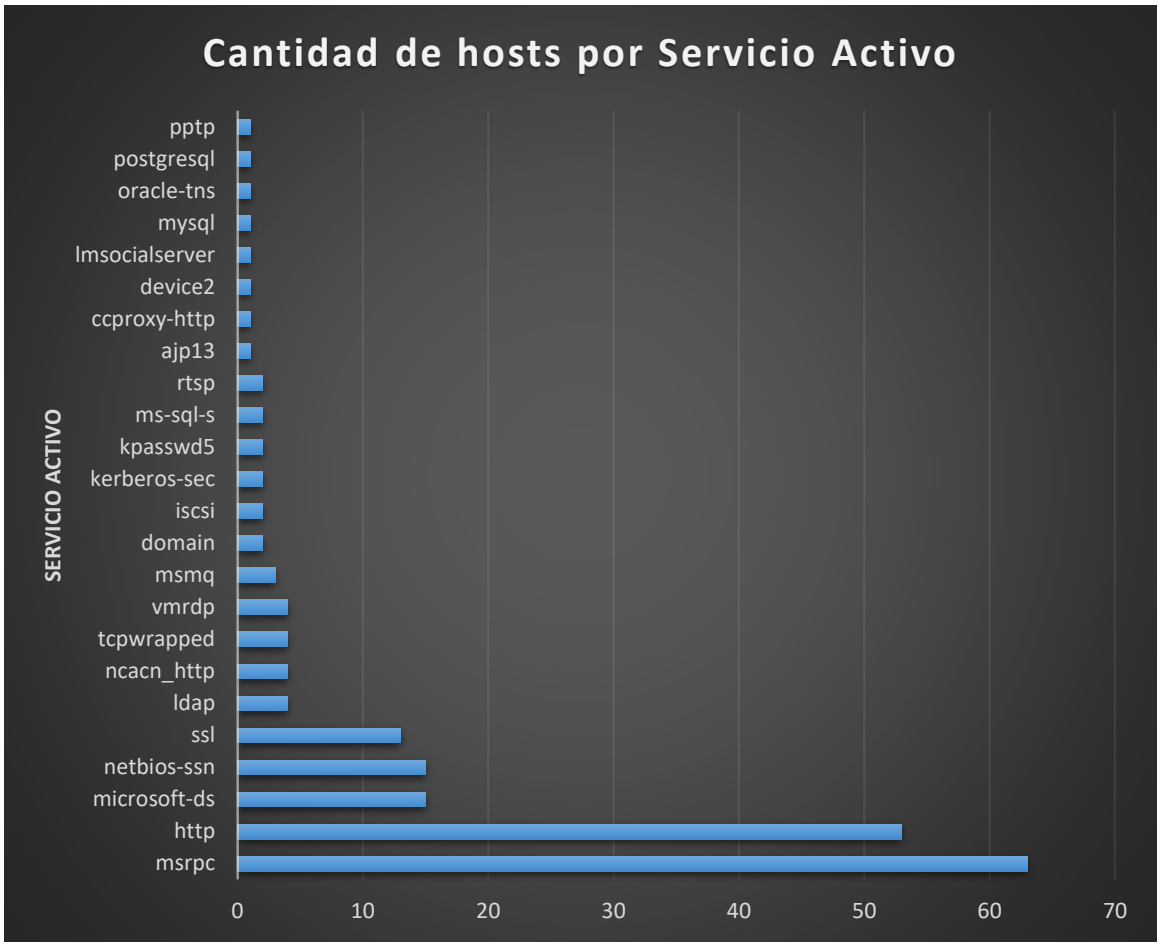


Fuente: El autor.

De aquí se puede analizar que existen 3 puertos cuya frecuencia es mayor sobre el resto: puerto 80, 445 y 135 cuyos servicios activos se han dado a conocer anteriormente.

Ahora, teniendo en cuenta que cada puerto está asignado a un servicio en ejecución, se ha recopilado la información correspondiente a la frecuencia sobre servicios ejecutados en las máquinas de la organización obteniendo los resultados mostrados a través de la siguiente gráfica:

Figura 45. Cantidad de Hosts por Servicio Activo



Fuente: El autor

Aquí, se puede mostrar que los servicios más frecuentes son msrpc y http.

- msrpc: Corresponde a un protocolo de comunicación de procesos de manera remota, generalmente se asigna hacia el puerto 135 y es usado por gran cantidad de servicios.
- http: Su frecuencia se debe a que la mayoría de equipos tienen instalados servidores web por la situación de quehacer diario en la organización siendo la principal actividad el desarrollo de software.

7.4.2.4. Reconocimiento de la red de comunicaciones: En complementación con la enumeración realizada a través de aplicaciones como nmap en Kali Linux y net view que viene integrado en Windows, se procedió a realizar un diagrama de red de la organización el cuál se abarca en los Anexos B y C con el fin de identificar cada uno de los dispositivos interconectados y así poder medir el grado de importancia de cada uno ellos.

Entonces de ahí se obtiene que la empresa cuenta con los siguientes tipos de dispositivos:

- 2 Servidores.
- 11 Equipos de escritorio.
- 12 Equipos pórtatiles.
- 2 switches.
- 2 routers.

Además, es importante mencionar que la empresa cuenta con dos proveedores de Internet: Media commerce y Claro. En consecuencia, tienen dos redes lógicas para cada ISP con las siguientes direcciones: 192.168.0.0/24 y 192.168.1.0/24. La primera red, es utilizada para el departamento operativo y la segunda para el administrativo.

Debido a solicitud expresa de la empresa CJT&T Ingeniería de Software, solamente es de interés aplicar todo el proceso de evaluación en la red 192.168.0.0/24 debido a que es la que realmente está implicada en las tareas operativas.

Es de señalar que se cuenta con configuración de IP estática únicamente para los equipos servidores, los demás equipos utilizan cada router de su segmento como servidor DHCP para solicitar asignación de IP dinámica.

Los servidores mencionados anteriormente tienen como IP 192.168.0.100 y 192.168.0.234 y se han categorizado según su uso como servidores de respaldo y aplicaciones respectivamente. A continuación, se analizan los contenidos que manejan cada uno de ellos y su grado de importancia para la organización.

Servidor de aplicaciones

El servidor tiene instalado el Sistema Operativo Windows 2012. Se pudo observar que cuenta con múltiples aplicaciones web internas que son desplegadas a través de los servicios que proporciona IIS. Así también, se pudo identificar que adicional a esto, se usa como servidor de base de datos alojando entre otros MySQL, SQL Server y Oracle.

Por otro lado, y lo más importante, éste se usa como un servidor de TFS, en el cual se realiza la administración de todos los proyectos para los equipos de desarrollo que conforman la empresa. A través de esté se realiza el almacenamiento y versionamiento de código fuente, creación e interacción sobre incidencias, gestión sobre el proceso de pruebas e integración con diferentes metodologías de desarrollo de Software que se manejen a nivel organizacional.

Se podría considerar que este equipo de cómputo es vital para las operaciones cotidianas y contiene información vital para el funcionamiento de la empresa.

Servidor de respaldo

El servidor de respaldo de la organización cuenta con un gran espacio de almacenamiento. Por el momento, las tareas programadas se encargan de posibilitar la generación de archivos de respaldo que serán resguardados y posteriormente verificados por el personal TI de la organización.

En este servidor únicamente se almacenan las copias de seguridad pertenecientes al servidor de aplicaciones de la empresa.

Por la anterior razón, a pesar de que la empresa podría seguir con sus actividades normales en caso de una posible interrupción en el funcionamiento de este equipo, en un escenario crítico donde el equipo principal es atacado y la información es alterada, los respaldos almacenados en éste serán el único medio para retornar a la normalidad.

Otros equipos

Los equipos de escritorio y portátiles que se indican en el Anexo B y C del presente documento, si bien son importantes para que los empleados puedan desempeñar sus tareas diarias, no contienen información confidencial que pueda estar en riesgo en caso de un ataque informático. Sin embargo, el hecho de no contar con los equipos suficientes para garantizar las actividades de la empresa si implica una afectación directa sobre sus intereses económicos.

Además, es de obligación mencionar que no todos los equipos que se encuentran en el diagrama son de uso continuo, ya que dependen del número de empleados contratados y activos en el periodo de tiempo. Al momento de realizar las pruebas, un total de 11 equipos se encontraron en actividad para la red objetivo de análisis.

Aspectos relevantes

- Al momento de efectuar las pruebas la red no cuenta con un Firewall físico, ni un proxy que filtre las solicitudes entrantes y salientes de Internet.

- Cualquier alteración sobre el servidor de aplicaciones sería catastrófica para la empresa.
- El servidor de respaldo contiene copias de seguridad sobre el sistema operativo y las diferentes bases de datos que se manejan en el servidor de aplicaciones.

- Los otros equipos de la intranet son de uso laboral para el personal de la empresa, en los cuales se ejecutan las tareas cotidianas como desarrollo, Testing y comunicación continua con los clientes a través de aplicaciones de terceros como Skype y Hangouts.

A continuación, en la tabla 7 se realiza un resumen que resalta la importancia de los equipos en la organización.

La escala de medición a usar sobre el nivel de importancia de cada tipo de equipo se encuentra entre los siguientes valores: baja, media y alta.

Tabla 7. Importancia de equipos de cómputo

Tipo de equipo	Información que contiene	Importancia
Servidor de aplicaciones	• Código fuente. • Bases de datos. • Aplicaciones de gestión interna.	Alta
Servidor de respaldo	Copias de seguridad	Alta
Equipos de escritorio Equipos portátiles	• Documentos. • Archivos multimedia. • Código fuente descargado del servidor de aplicaciones.	Media

Fuente: El autor.

7.4.2.5. Fase de Análisis de Vulnerabilidades: Una vez se obtiene claridad sobre los objetivos del ataque en la red Interna se procede a ejecutar un análisis de vulnerabilidades haciendo uso de la herramienta de Software Nessus. El resultado obtenido el 28 de abril ha permitido obtener un panorama sobre las debilidades de los sistemas en la organización clasificada por IP y por severidad de las vulnerabilidades. El reporte respectivo se podrá encontrar en los Anexos G y H del presente documento. A continuación, se realiza un análisis sobre los hallazgos encontrados.

Tabla 8. Severidad de Vulnerabilidades en cada host de la organización

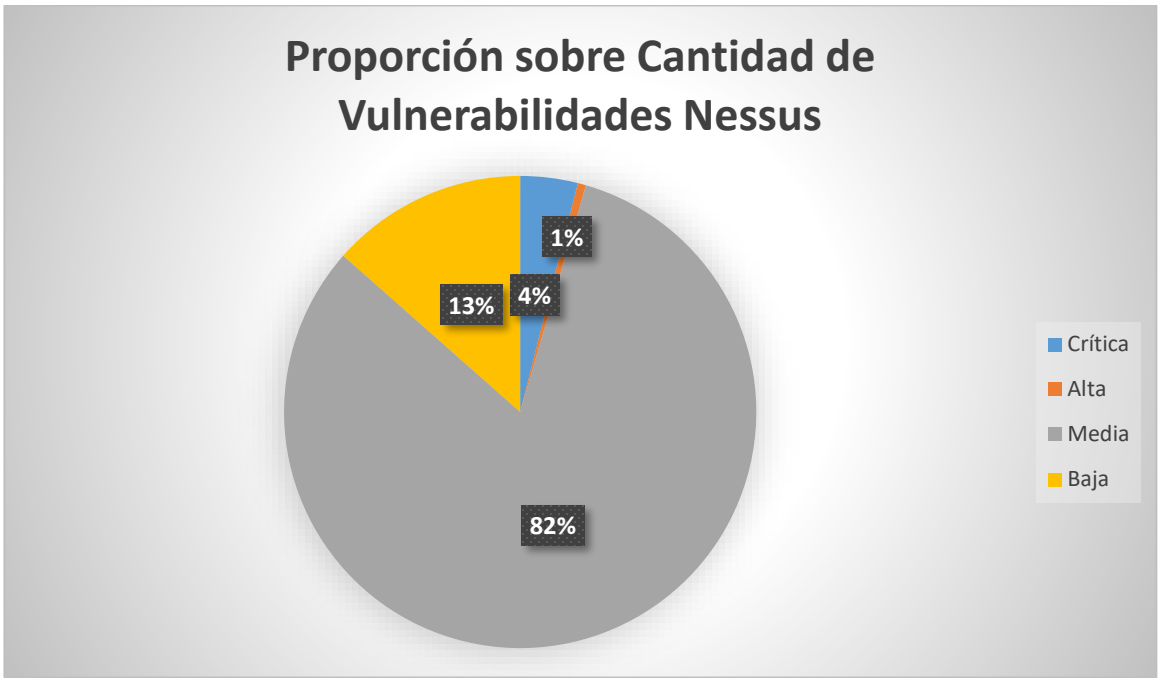
IP	C: Critico	C: Alta	C: Media	C: Baja	C: Informativa
192.168.0.100	2	1	2	2	22
192.168.0.134	2	0	17	1	56
192.168.0.86	1	0	8	1	29
192.168.0.246	1	0	5	0	28
192.168.0.254	1	0	3	1	10
192.168.0.1	0	0	1	1	4
192.168.0.101	0	0	2	1	18
192.168.0.102	0	0	0	1	4
192.168.0.105	0	0	8	1	34
192.168.0.106	0	0	7	2	26
192.168.0.118	0	0	7	1	31
192.168.0.121	0	0	6	0	36
192.168.0.125	0	0	4	0	30
192.168.0.127	0	0	8	2	28
192.168.0.129	0	0	0	0	9
192.168.0.135	0	0	10	2	38
192.168.0.138	0	0	1	0	15
192.168.0.143	0	0	1	0	25
192.168.0.144	0	0	6	1	18
192.168.0.157	0	0	13	2	34
192.168.0.185	0	0	7	1	30
192.168.0.188	0	0	7	1	30
192.168.0.200	0	0	13	2	39
192.168.0.209	0	0	1	0	18
192.168.0.222	0	0	2	0	25
192.168.0.249	0	0	7	1	29
	7	1	146	24	666
Fuente: El autor					

De acuerdo a esta recopilación de resultados se tiene que:

Tabla 9. Cantidad de vulnerabilidades según severidad

Severidad	Cantidad
Crítica	7
Alta	1
Media	146
Baja	24
Fuente: El autor	

Figura 46. Proporción sobre Cantidad de Vulnerabilidades Nessus



Fuente: El autor

La anterior gráfica permite observar que la mayor cantidad de defectos que se presentan en la organización tienen un grado de severidad medio con un 82%. Esto representa una situación bastante preocupante debido al alto grado de exposición de los activos sobre la posible amenaza de un tercero. Es imperante mitigar o eliminar estas vulnerabilidades que representan un riesgo alto sobre las operaciones normales de la empresa dado los carentes medios de protección que actualmente se encuentran implementados.

En este punto, se inicia con el análisis de cada una de las vulnerabilidades encontradas y la propuesta sobre las posibles soluciones para corregir la falla en los sistemas:

Tabla 10. Vulnerabilidades críticas y Soluciones para la organización

Severidad: Crítica			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
79638 - MS14-066	Vulnerabilidad en Canal seguro podría permitir ejecución de	El host de acceso remoto es afectado por una vulnerabilidad de ejecución de código	Microsoft liberó una serie de parches para Windows partiendo de su versión 2003.

Severidad: Crítica			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
	código de manera remota	remoto debido al procesamiento inadecuado de paquetes por el paquete de seguridad del canal seguro. Un atacante puede explotar este problema enviando paquetes especialmente formados a un servidor Windows.	
39364	Credenciales por defecto para el controlador IBM Baseboard Management	El host remoto parece ser un BMC que es usado para proveer administración fuera de banda. El BMC remoto está protegido por una contraseña por defecto.	Reemplazar la contraseña por defecto por una contraseña fuerte.
68931	Configuración de opción sin autenticación de seguridad para IPMI	El servicio IPMI está en escucha en el sistema remoto con la opción "cipher suite zero" habilitada, lo que permite acceso como administrador sin requerir una contraseña. Una vez logueado, un atacante remoto puede realizar variedad de acciones, incluyendo apagar el sistema.	Deshabilitar la opción o limitar el acceso al servicio.
80304	Ejecución de Código Remoto por Vulnerabilidad en el Manejo de Cookies HTTP mediante Allego RomPager	Nessus efectuó un ataque que fue capaz de sobrescribir la ruta de solicitud enviando una cookie manipulada hacia el servidor web.	Actualizar a una imagen actualizada del firmware (RomPager 4.34).
82828	Vulnerabilidad en HTTP.sys podría causar ejecución de código remoto	La versión de Windows que se ejecuta en el host está afectada por una vulnerabilidad en la pila del protocolo HTTP debido a parseo inadecuado de las solicitudes HTTP. Esta situación puede permitirle al atacante remoto	Microsoft libero un conjunto de parches para Windows disponibles a través de Update.

Severidad: Crítica			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
		ejecutar código arbitrario con privilegios de System.	
Fuente: El autor			

Tabla 11. Vulnerabilidades altas y Soluciones para la organización

Severidad: Alta			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
80101	Divulgación de hash de contraseñas	El host remoto soporta IPMI v2.0. Este protocolo es afectado por una vulnerabilidad de divulgación de información debido al soporte de autenticación RAKP.	No existen parches para la vulnerabilidad. Para mitigar se recomienda: • Deshabilitar IPMI a través de la LAN si no es necesario. • Usar contraseñas fuertes para limitar el éxito de ataques de diccionario fuera de línea. • Usar Listas de Acceso de Control o redes aisladas para limitar el acceso a las interfaces de administración IPMI.
Fuente: El autor			

Tabla 12. Vulnerabilidades medias y Soluciones para la organización

Severidad: Media			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
51192	Certificado SSL no es de confianza	El certificado X.509 del servidor no tiene una firma de una CA pública conocida. Lo anterior puede causar dificultades en la verificación de la autenticidad e identificación del servidor web haciendo más fácil efectuar un ataque MIM en contra el host remoto.	Comprar o generar un certificado adecuado para el servicio.

Severidad: Media			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
57582	Certificado SSL autofimado	La cadena del certificado X.509 para el servicio no está firmada por un CA reconocido. Si el host remoto es un host público en producción, esto anula el uso de SSL debido a que cualquier persona podría establecer un MIM en contra del host remoto.	Comprar o generar un certificado adecuado para el servicio.
65821	Soporte para Suites de cifrado SSL RC4	El host remoto soporta el uso de RC4 en una o más suites de cifrado. El cifrado RC4 falla en su generación de bytes de transmisión, disminuyendo la aleatoriedad. Si el texto plano es encriptado repetidamente y un atacante está habilitado para obtener muchos textos cifrados, el atacante puede derivar el texto plano.	Reconfigurar la aplicación afectada para evadir el uso de cifrado RC4. Se recomienda el uso de TLS 1.2 con AES-GCM sujeto al soporte del servidor web y el navegador.
57608	Firmado SMB deshabilitado	El firmado no es requerido en el servidor remoto SMB. Un atacante remoto anónimamente puede explotar esta situación para conducir un ataque MIM en contra del servidor SMB.	Forzar firmado de mensajes en la configuración del host.
18405	Debilidad Servidor de Protocolo en Escritorio Remoto de Windows	La versión remota del Servidor de Protocolo en el Escritorio Remoto de Windows es vulnerable a un ataque MIM. El cliente RDP no hace esfuerzo para validar la identidad del servidor cuando se está configurando una encriptación. Un atacante con la habilidad de interceptar tráfico desde el servidor RDP puede establecer encriptación con el cliente y servidor sin ser detectado. Un ataque MIM de esta naturaleza puede permitir al atacante obtener información sensible transmitida	Forzar el uso de SSL como una capa de transporte del servicio si está soportado o seleccionar la opción de permitir conexiones solamente desde computadores ejecutando escritorio remoto con autenticación a nivel de red.

Severidad: Media			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
		incluyendo credenciales de autenticación.	
57690	Nivel bajo de encriptación en Servicios de Terminal	La terminal de servicios remota no está configurada para usar criptografía fuerte.	Cambiar encriptación RDP a nivel alto o compatible con FIPS
58453	Servicios de Terminal no usa Autenticación a nivel de red	La terminal de servicios remota no está configurada para usar autenticación a nivel de red. NLA usa el protocolo CredSSP que permite proporcionar un servidor fuerte de autenticación que provee la capacidad de protección en contra de ataques MIM.	Habilitar NLA en el servidor remoto RDP a través de la pestaña “Remoto” de la configuración del sistema en Windows.
45411	Certificado SSL con nombre de host incorrecto	El nombre común del certificado SSL presentado en el servicio es de una máquina diferente.	Comprar o generar un certificado adecuado para el servicio.
26919	Acceso de Usuario Local para Cuenta de Invitado en SMB	El host remoto permite loguearse como invitado usando una cuenta aleatoria.	Cambiar la configuración de red o deshabilitar la cuenta de invitado si es aplicable.
90510	Actualización de Seguridad para protocolos remotos SAM y LSAD	El host remoto Windows es afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Administrador de cuentas de seguridad y la autoridad local de seguridad debido al inadecuado nivel de negociación en la autenticación sobre canales de llamadas de procedimientos remoto.	Parches disponibles a través de actualizaciones de Windows.
20007	Detección de Protocolo SSL versión 2 y 3	El servicio remoto acepta conexiones encriptadas usando SSL 2 y 3. Estas versiones de SSL son afectadas por varias fallas que un atacante puede aprovechar para conducir ataques MIM o desencriptar comunicaciones entre el	Usar TLS 1.1 o versiones más recientes.

Severidad: Media			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
		servicio afectado y los clientes.	
35291	Firmado de Certificado SSL usando un algoritmo débil de hashing	El servicio remoto usa una cadena en el certificado SSL que ha sido firmada usando un algoritmo débil de hashing que es susceptible a colisiones.	Contactar al CA para emitir nuevamente el certificado.
78479	POODLE	El host remoto es afectado por una vulnerabilidad de divulgación de información MIM conocida como POODLE. La vulnerabilidad se debe a la manera en que SSL 3.0 maneja los bytes de relleno cuando desencripta mensajes usando bloques cifrados en modo CBC. El atacante podría desencriptar un byte seleccionado de un texto cifrado en un mínimo de 256 intentos si están habilitados para forzar a la aplicación a enviar la misma información sobre conexiones SSL 3.0 creadas recientemente.	Deshabilitar SSLv3.
50686	Reenvío IP habilitado	El host remoto tiene habilitado el reenvío IP. Un atacante puede explotar esta situación para rutear paquetes a través del host y potencialmente evitar firewalls, filtros o barreras.	Deshabilitar el reenvío IP a menos que los dispositivos correspondan a un router.
12217	Divulgación de información remota por Snooping de Cache en Servidores DNS	El servidor DNS remoto responde a consultas desde dominios de terceros que no tienen el conjunto de bits de recursión. Esto puede permitir al atacante determinar que dominios han sido recientemente resueltos a través de su servidor de nombres y entonces identificar los hosts que recientemente ha visitado.	Contactar al vendedor del software DNS para una solución.

Severidad: Media			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
24244	Errores personalizados no configurados en Microsoft .NET	El servidor web remoto ASP.NET está configurado para mostrar mensajes de error detallados, lo que puede guiar hacia la divulgación de potencial información sensible sobre la instalación remota o sobre las aplicaciones.	Configurar el servidor para que la opción “customErrors mode” se encuentre establecida en “On” en vez de “Off”.
42263	Servidor Telnet no encriptado	El host remoto está ejecutando un servidor Telnet sobre un canal no encriptado. Esto no es recomendado debido a que datos sensibles son transferidos en texto plano. Esto permite al atacante remoto espiar una sesión Telnet para obtener credenciales u otra información sensible y modificar tráfico intercambiado entre cliente y servidor.	Deshabilitar el servicio Telnet y usar SSH.
26928	Soporte para Suites de Cifrado SSL débiles	El host remoto soporta el uso de cifrado SSL que ofrece encriptación débil.	Reconfigurar la aplicación afectada para evitar el uso de cifrado débil.
42873	Soporte para Suites de Cifrado SSL con fortaleza media	El host remoto soporta el uso de cifrado SSL que ofrece encriptación con fortaleza media, lo que se puede considerar como llaves con longitud entre 56 y 112 bits.	Reconfigurar la aplicación afectada para evitar el uso de cifrado con fortaleza media.
71174	Vulnerabilidad CSS por el encabezado de la referencia HTTP de RomPager	El servidor remoto está afectado por una vulnerabilidad XSS. Este servidor no sanea adecuadamente el valor del encabezado de referencia generando una página de error 404.	Actualizar RomPager a la versión 4.51 o superior.
81606	Soporte para EXPORT_RSA en suites de cifrado con llaves menores o iguales a 512 bits	Un atacante puede factorizar un módulo RSA de 512 bits en un periodo corto de tiempo. Así, podría ser capaz de	Reconfigurar el servicio para remover el soporte de EXPORT_RSA.

Severidad: Media			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
		degradar la sesión para usar EXPORT_RSA.	
81777	Servicio MongoDB sin autenticación detectado	MongoDB, un sistema de base de datos orientado hacia documentos, está escuchando en el puerto remoto y está configurado para permitir conexiones sin autenticación. Un atacante remoto puede entonces conectarse al sistema de base de datos con el objetivo de manipular documentos, colecciones y bases de datos.	Habilitar autenticación o restringir acceso al servicio MongoDB.
83738	Soporte para EXPORT_DHE en suites de cifrado con llaves menores o iguales a 512 bits	A través de criptoanálisis, un tercero puede encontrar la llave secreta compartida en un periodo corto de tiempo. Así, podría ser capaz de degradar la sesión para usar EXPORT_DHE	Reconfigurar el servicio para remover el soporte de EXPORT_DHE.
83875	Módulos SSL/TLS Diffie Hellman menores o iguales a 1024 bits	A través de criptoanálisis, un tercero puede estar habilitado para encontrar la llave secreta compartida en un corto periodo de tiempo. Esto permitiría al atacante recobrar el texto plano o potencialmente violar la integridad de las conexiones.	Reconfigurar el servicio para usar un único módulo Diffie-Hellman con 2048 bits o superior.
90317	Algoritmos débiles SSH soportados	Se detectó que el servidor SSH remoto está configurado para no usar cifrado o usar cifrado Arcfour (RC4).	Contactar al proveedor o consultar la documentación del producto para remover los cifrados débiles.
90318	Descubrimiento de token por vulnerabilidad XSRF en Apache Tomcat	El servidor Apache Tomcat es afectado por una vulnerabilidad de divulgación de información en la página de inicio de las aplicaciones de administración. Un atacante sin autenticarse podría obtener un token válido XSRF durante el redireccionamiento emitido cuando se solicita /manager o	Actualizar Apache Tomcat a la versión 7.0.68, 8.0.32, 9.0.0.M3 o posterior.

Severidad: Media			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
		/host-manager. Este token puede ser utilizado por un atacante para construir un ataque XSRF.	
Fuente: El autor			

Tabla 13. Vulnerabilidades bajas y Soluciones para la organización

Severidad: Baja			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
30218	Nivel de encriptación de Servicios de Terminal no es Compatible con FIPS-140	La configuración de encriptación utilizada por los servicios de terminal remotos no es compatible con FIPS-140	Cambiar el nivel de encriptación RDP a “4. Compatible con FIPS”
69551	Cadena de certificados SSL contiene llaves RSA menores que 2048 bits	Al menos uno de los certificados X.509 enviado por el host remoto tiene una llave que es menor que 2048 bits. De acuerdo a los estándares de la industria establecidos por el Foro CA/B, certificados que sean emitidos posterior a Enero 1 de 2014 deben tener al menos 2048 bits.	Reemplazar el certificado en la cadena que tenga una llave RSA con menos de 2048 bits en longitud con una llave más extensa, y re emitir cualquier certificado firmado por el certificado antiguo.
11197	Divulgación de información por relleno en tramas de controladores múltiples Ethernet (Etherleak)	El host remoto usa un controlador de dispositivo de red que rellena las tramas Ethernet con datos que podrían variar de un paquete a otro, probablemente tomados desde la memoria del kernel, memoria del sistema localizada en el controlador del dispositivo o un buffer de hardware en la interfaz de la tarjeta de red.	Contactar al proveedor del controlador del dispositivo de red por una solución.
10663	Detección del Servidor DHCP	El script contacta al servidor DHCP remoto y trata de devolver información sobre el	Aplicar filtro para mantener esta información fuera de la red y eliminar las

Severidad: Baja			
Código	**Vulnerabilidad**	**Descripción**	**Solución**
		diseño de red. Algunos servidores DHCP proveen información sensible como el nombre de dominio NIS, o información del diseño de red como la lista de los servidores web en la red, entre otros. Esta información podría ser usada por un atacante para familiarizarse con la red asociada.	opciones que no están en uso.
34324	FTP soporta autenticación de texto plano o sin cifrar	El servidor FTP remoto permite que el nombre de usuario y contraseña sean transmitidos en texto plano, lo que podría ser interceptado por un sniffer de red o un ataque MIM.	Cambiar a SFTP o FTPS. En el último caso se debe configurar el servidor para que las conexiones de control se encuentren encriptadas.
70658	Modo de cifrado CBC habilitado en el Servidor SSH	El servidor SSH está configurado para dar soporte a encriptación CBC. Esto podría permitir a un atacante recobrar un mensaje en texto plano a partir de un texto cifrado.	Contactar al vendedor o consultar la documentación del producto para deshabilitar la encriptación a través del modo de cifrado CBC y habilitar la encriptación con modo de cifrado CTR o GCM.
71049	Algoritmos MAC débiles en SSH habilitados	El servidor SSH remoto está configurado para permitir los algoritmos MAC MD5 o 96-bit los cuales son considerados débiles.	Contactar al proveedor o consultar la documentación del producto para deshabilitar los algoritmos MAC MD5 y 96-bit.
Fuente: El autor			

Posterior a este escaneo, se procedió a utilizar la herramienta OpenVAS debido a los cambios presentados en la infraestructura de la red empresarial. A continuación, se presentan los resultados correspondientes al proceso efectuado el 12 de mayo cuyo reporte se encuentra en el Anexo K de este documento.

Asimismo, se realiza un análisis sobre la relación de vulnerabilidades y su nivel de severidad que será de gran ayuda como punto comparativo para determinar el panorama de seguridad individualizado sobre los hosts activos de la organización.

Tabla 14. Severidad de Vulnerabilidades OpenVAS

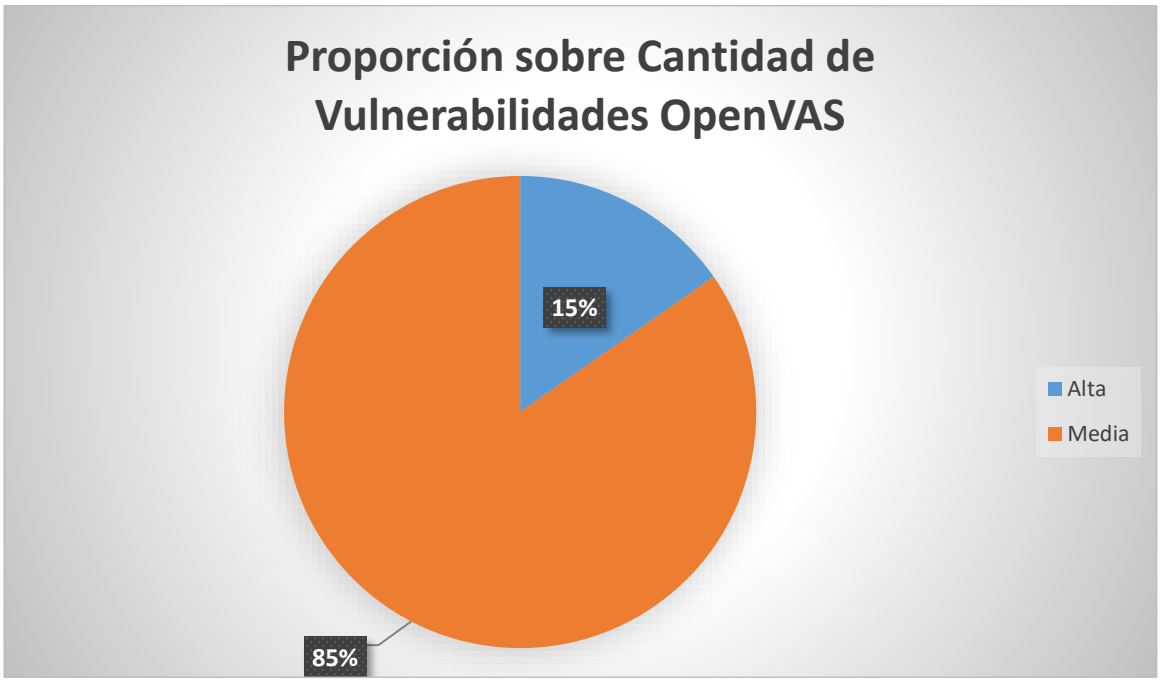
IP	C: Alta	C: Media	C: Informativa
192.168.0.134	9	26	3290
192.168.0.17	1	5	61
192.168.0.11	1	5	12
192.168.0.107	1	4	25
192.168.0.117	1	3	33
192.168.0.200	0	6	42
192.168.0.103	0	11	34
192.168.0.222	0	4	27
192.168.0.105	0	3	25
192.168.0.18	0	3	23
192.168.0.106	0	1	17
192.168.0.13	0	1	16
192.168.0.1	0	0	9
	13	72	3614
Fuente: El autor			

De acuerdo a esta recopilación de resultados se tiene que:

Tabla 15. Cantidad de vulnerabilidades según severidad OpenVAS

Severidad	Cantidad
Alta	13
Media	72
Fuente: El autor	

Figura 47. Proporción sobre Cantidad de Vulnerabilidades OpenVAS



Fuente: El autor

De acuerdo a la anterior gráfica se observa que la mayor cantidad de defectos que se presentan en la organización tienen un grado de severidad medio con un 85%. No difiere mucho del anterior análisis representando un gran riesgo que debe atenderse de manera inmediata.

Ahora, de acuerdo al reporte generado por OpenVAS a continuación se recopilan las vulnerabilidades más importantes producto del hallazgo en el escaneo mencionando sus posibles soluciones.

Tabla 16. Vulnerabilidades altas y soluciones OpenVAS.

Severidad: Alta		
Vulnerabilidad	**Descripción**	**Solución**
MS15-034 HTTP.sys Vulnerabilidad de Ejecución de código remoto	Esta vulnerabilidad podría causar que el atacante ejecute código arbitrario con consecuentes acciones en el contexto del usuario final.	• Ejecutar actualizaciones desde Windows Update en el Sistema Operativo.
Vulnerabilidades multiples no	Un ataque exitoso de este tipo podría permitir que un tercero	• Actualizar a la versión más reciente o aplicar los

Severidad: Alta		
Vulnerabilidad	**Descripción**	**Solución**
especificadas en Oracle MySQL-05 Abril16 (Windows)	autenticado de manera remota afecte la seguridad del sistema.	parches publicados por Oracle para MySQL.
Vulnerabilidad de Denegación de servicio en Apache Tomcat -Junio15 (Windows)	Un ataque exitoso aprovechando esta vulnerabilidad podría permitir la denegación de servicio de los sistemas afectados.	• Actualizar Apache Tomcat a las versiones 6.0.44, 7.0.55, 8.0.9 o posterior.
Agora CGI Cross Site Scripting	Teniendo en cuenta que Agora es una aplicación orientada al comercio electrónico, se ha detectado que debido a inconvenientes o pobre validación en los datos de entrada sería posible ejecutar código a través de un ataque XSS exponiendo la confidencialidad de los datos del usuario.	• Actualizar la versión 4.0e de Agora o una más reciente.
Vulnerabilidad de omisión de autenticación por sesión nula en Microsoft Windows SMB/NETBIOS NULL	La explotación de esta vulnerabilidad podría permitir que el atacante utilice los archivos o directorios compartidos para causar que el sistema falle.	• Deshabilitar el uso de sesiones nulas, remover los archivos compartidos o protegerlos con una contraseña.
Fuente: El autor		

Tabla 17. Vulnerabilidades medias y soluciones OpenVAS.

Severidad: Media		
Vulnerabilidad	**Descripción**	**Solución**
Cifrado débil en SSL	Se ha detectado un servicio que utiliza cifrado débil, lo que podría implicar colisiones comprometiendo la confidencialidad de la información del usuario.	• La configuración del servicio debería ser cambiada para evitar el soporte de cifrados débiles.
Detección de protocolos obsoletos SSLv2 y SSLv3	El atacante podría aprovecharse de conocer fallas criptográficas en los protocolos obsoletos para obtener acceso a información sensible que se transfiere desde una conexión segura.	• Deshabilitar los protocolos obsoletos. • Habilitar protocolos TLSv1+.

Severidad: Media		
Vulnerabilidad	**Descripción**	**Solución**
Vulnerabilidad de divulgación de información en cifrado CBC del protocolo POODLE SSLv3	Aprovechar esta falla podría permitir que un ataque MiM sea exitoso y permita obtener acceso a datos en formato plano.	• Obtener las últimas actualizaciones por parte del proveedor. • Se recomienda deshabilitar SSL v3
Vulnerabilidad de enumeración de usuarios en mensaje de error al realizar autenticación en MySQL	Su explotación podría permitir obtener nombres de usuario válidos que podrían servir como insumo para un posterior ataque de fuerza bruta u otros.	• Instalar las últimas actualizaciones del producto.
Oracle MySQL múltiples vulnerabilidades no especificadas-01 Abri16 (Windows)	La explotación de estas fallas compromete directamente la confidencialidad, integridad y disponibilidad de la información contenida en las bases de datos MySQL.	• Instalar las últimas actualizaciones del producto.
Oracle MySQL multiples vulnerabilidades no especificadas-02 Abril16 (Windows)		
Oracle MySQL múltiples vulnerabilidades no especificadas-06 Abril16 (Windows)		
Vulnerabilidad CSRF de filtrado de Token en Apache Tomcat-Feb16 (Windows)	Su éxito permite que los atacantes remotos superen la protección contra ataques CSRF utilizando un token.	• Actualizar Apache Tomcat a la versión 7.0.68, 8.0.32, 9.0.0.M3 o posterior.
Vulnerabilidad de fijación en sesión de Apache Tomcat -Feb16 (Windows)	Esto permitiría que el atacante secuestre u obtenga datos de sesiones web aprovechando el uso del campo “requestedSessionSSL” para una petición no consensuada o involuntaria.	• Actualizar Apache Tomcat a la version 7.0.66, 8.0.32, 9.0.0.M3 o posterior.
Vulnerabilidad de omisión del administrador de seguridad Apache Tomcat-Feb16 (Windows)	Un ataque exitoso de este tipo podría permitir a usuarios remotos autenticados omitir el administrador de seguridad, por lo cual no se tendrían restricciones para realizar	• Actualizar Apache Tomcat a la versión 7.0.68, 8.0.32, 9.0.0.M3 o posterior.

Severidad: Media		
Vulnerabilidad	**Descripción**	**Solución**
	cualquier acción sobre los datos de aplicaciones o posible denegación de servicio.	
Vulnerabilidad de omisión del administrador de seguridad Apache Tomcat 01 -Feb16 (Windows)	La explotación de la vulnerabilidad podría permitir que usuarios remotos autenticados omitan las restricciones del administrador de seguridad para ejecutar código arbitrario con el cual podrían leer solicitudes HTTP y eventualmente descubrir identificadores de sesión.	• Actualizar Apache Tomcat a la versión 6.0.45, 7.0.68, 8.0.32, 9.0.0.M3 o posterior.
Vulnerabilidad de denegación de servicio en Apache Tomcat - Mar15	El atacante podría efectuar un ataque de denegación de servicio a través de la transmisión de cantidad ilimitada de datos, lo cual guiaría hacia el consumo desmesurado de recursos.	• Actualizar Apache Tomcat a la versión 6.0.42, 7.0.55, 8.0.9 o posterior.
Vulnerabilidad de omisión del administrador de seguridad en Apache Tomcat - Junio15 (Windows)	A través de la omisión de autenticación en algunas secciones de administración se podría obtener información sensible.	• Actualizar Apache Tomcat a la versión 6.0.44, 7.0.58, 8.0.16 o posterior.
Vulnerabilidad de divulgación de directorio en Apache Tomcat - Feb16 (Windows)	La explotación exitosa sería la causante de que atacantes remotos puedan determinar la existencia de un directorio en el servidor.	• Actualizar Apache Tomcat a la versión 6.0.45, 7.0.67, 8.0.30, 9.0.0.M3 o posterior.
Vulnerabilidad limitada de directorio transversal en Apache Tomcat - Feb16 (Windows)	Esta vulnerabilidad podría permitir a los atacantes remotos que se encuentren autenticados en el servidor a omitir las restricciones del administrador de seguridad y listar un directorio padre.	• Actualizar Apache Tomcat a la versión 6.0.45, 7.0.65, 8.0.27 o posterior.
Vulnerabilidad de elevación de privilegios en Microsoft SQL Server (2984340) - Remota	El atacante remoto podría causar una denegación de servicio o elevación de privilegios a causa de la vulnerabilidad en el servidor de base de datos SQL Server.	• Ejecutar Windows Update e instalar las actualizaciones específicas para el producto o descargarlas directamente desde la página web del proveedor.
Usar una solicitud de búsqueda LDAP	Es posible descubrir información LDAP debido a que el directorio	• Remover la compatibilidad pre Windows 2000.

Severidad: Media		
Vulnerabilidad	**Descripción**	**Solución**
para devolver información desde el Directorio de Servicios NT	base del servidor remoto está configurado como nulo lo que puede permitir enumerar información sin necesidad de tener ningún privilegio sobre la estructura de directorios.	
Enumeración de Servicios DCE	Estos servicios pueden ser enumerados a través del puerto 135 realizando las consultas adecuadas. Esto podría permitir obtener más conocimiento sobre el equipo remoto.	• Filtrar el tráfico entrante desde este puerto.
Error en el manejo de llaves temporales al degradar la opción exportar RSA OpenSSL (FREAK)	El host tiene OpenSSL instalado por lo cual podría ser muy probable que sea vulnerable a un ataque MiM.	• Correcciones establecidas por el proveedor.
OpenSSL TLS 'DHE EXPORT' Vulnerabilidad de omisión MiM LogJam	El poder explotar esta vulnerabilidad exitosamente podría permitir a un atacante MiM degradar la seguridad de una sesión hacia 512 bits permitiendo que sea menos complicado romper la encripción y monitorear o manipular las cadenas encriptadas.	• Correcciones establecidas por el proveedor.
Vulnerabilidad de descubrimiento de llave privada en servidor Microsoft RDP	Al explotar esta vulnerabilidad, el atacante podría tener acceso a información sensible del usuario.	• Debido a que no existen soluciones por parte del proveedor, por el momento se recomienda deshabilitar las características del producto, eliminarlo o reemplazarlo por otro.
12Planet Chat Server one2planet.infolet.InfoServlet XSS	El host remoto contiene un CGI que es vulnerable a ataques XSS con lo cual se podrían obtener las credenciales de usuarios legítimos del sitio.	• Actualizar a la versión más reciente del producto.
Información por defecto de página de bienvenida en Microsoft IIS	El atacante podría obtener información sensible que podría guiarlo para plantear vectores para próximos ataques.	• Deshabilitar las páginas por defecto en la configuración del servidor.
Contenedor de archivos por	Los archivos por defecto deben ser eliminados ya que podrían ayudar al atacante a determinar	Eliminar los archivos por defecto.

Severidad: Media		
Vulnerabilidad	**Descripción**	**Solución**
defecto en Apache Tomcat servlet/JSP	la versión de Tomcat que se encuentra ejecutándose en el equipo remoto y proveer otro tipo de información adicional.	
Fuente: El autor		

7.4.2.6. Análisis sobre las vulnerabilidades encontradas: De acuerdo a los análisis de vulnerabilidades automatizados realizados a través de las herramientas Nessus y OpenVAS se pudo identificar sus causas las cuales se pueden observar en la siguiente tabla:

Tabla 18. Causa de las vulnerabilidades encontradas

Vulnerabilidad	Causa
Vulnerabilidad en Canal seguro podría permitir ejecución de código de manera remota	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Credenciales por defecto para el controlador IBM Baseboard Management	Configuración por defecto en aplicaciones.
Configuración de opción sin autenticación de seguridad para IPMI	Mala configuración de aplicaciones
Ejecución de Código Remoto por Vulnerabilidad en el Manejo de Cookies HTTP mediante Allego RomPager	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad en HTTP.sys podría causar ejecución de código remoto	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Divulgación de hash de contraseñas	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Certificado SSL no es de confianza	Mala configuración de aplicaciones
	Carencia de controles criptográficos
Certificado SSL autofimado	Mala configuración de aplicaciones
	Carencia de controles criptográficos
Soporte para Suites de cifrado SSL RC4	Mala configuración de aplicaciones
	Carencia de controles criptográficos

Vulnerabilidad	Causa
Firmado SMB deshabilitado	Mala configuración de aplicaciones
	Carencia de controles criptográficos
Debilidad Servidor de Protocolo en Escritorio Remoto de Windows	Mala configuración de aplicaciones
	Carencia de controles criptográficos
Nivel bajo de encriptación en Servicios de Terminal	Mala configuración de aplicaciones
	Carencia de controles criptográficos
Servicios de Terminal no usa Autenticación a nivel de red	Mala configuración de aplicaciones
Certificado SSL con nombre de host incorrecto	Carencia de controles criptográficos
Acceso de Usuario Local para Cuenta de Invitado en SMB	Mala configuración de aplicaciones
Actualización de Seguridad para protocolos remotos SAM y LSAD	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Detección de Protocolo SSL versión 2 y 3	Carencia de controles criptográficos
Firmado de Certificado SSL usando un algoritmo débil de hashing	Carencia de controles criptográficos
POODLE	Carencia de controles criptográficos
Reenvío IP habilitado	Mala configuración de aplicaciones
Divulgación de información remota por Snooping de Cache en Servidores DNS	Mala configuración de aplicaciones
Errores personalizados no configurados en Microsoft .NET	Mala configuración de aplicaciones
Servidor Telnet no encriptado	Mala configuración de aplicaciones
	Carencia de controles criptográficos
Soporte para Suites de Cifrado SSL débiles	Carencia de controles criptográficos
	Mala configuración de aplicaciones
Soporte para Suites de Cifrado SSL con fortaleza media	Carencia de controles criptográficos
	Mala configuración de aplicaciones
Vulnerabilidad CSS por el encabezado de la referencia HTTP de RomPager	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Soporte para EXPORT_RSA en suites de cifrado con llaves menores o iguales a 512 bits	Carencia de controles criptográficos
	Mala configuración de aplicaciones

Vulnerabilidad	Causa
Servicio MongoDB sin autenticación detectado	Mala configuración de aplicaciones
Soporte para EXPORT_DHE en suites de cifrado con llaves menores o iguales a 512 bits	Carencia de controles criptográficos
	Mala configuración de aplicaciones
Módulos SSL/TLS Diffie Hellman menores o iguales a 1024 bits	Carencia de controles criptográficos
	Mala configuración de aplicaciones
Algoritmos débiles SSH soportados	Carencia de controles criptográficos
Descubrimiento de token por vulnerabilidad XSRF en Apache Tomcat	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Nivel de encriptación de Servicios de Terminal no es Compatible con FIPS-140	Carencia de controles criptográficos
	Carencia sobre control de vulnerabilidades técnicas
Cadena de certificados SSL contiene llaves RSA menores que 2048 bits	Carencia de controles criptográficos
Divulgación de información por relleno en tramas de controladores múltiples Ethernet (Etherleak)	Mala configuración de aplicaciones
	Carencia sobre control de vulnerabilidades técnicas
Detección del Servidor DHCP	Mala configuración de aplicaciones
FTP soporta autenticación de texto plano o sin cifrar	Mala configuración de aplicaciones
	Carencia sobre control de vulnerabilidades técnicas
	Carencia de controles criptográficos
Modo de cifrado CBC habilitado en el Servidor SSH	Mala configuración de aplicaciones
	Carencia sobre control de vulnerabilidades técnicas
	Carencia de controles criptográficos
Algoritmos MAC débiles en SSH habilitados	Mala configuración de aplicaciones
	Carencia sobre control de vulnerabilidades técnicas
	Carencia de controles criptográficos
MS15-034 HTTP.sys Vulnerabilidad de Ejecución de código remoto	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas

Vulnerabilidad	Causa
Vulnerabilidades múltiples no especificadas en Oracle MySQL-05 Abril16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad de Denegación de servicio en Apache Tomcat -Junio15 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Agora CGI Cross Site Scripting	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad de omisión de autenticación por sesión nula en Microsoft Windows SMB/NETBIOS NULL	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Cifrado débil en SSL	Carencia de controles criptográficos
Detección de protocolos obsoletos SSLv2 y SSLv3	Carencia de controles criptográficos
Vulnerabilidad de divulgación de información en cifrado CBC del protocolo POODLE SSLv3	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad de enumeración de usuarios en mensaje de error al realizar autenticación en MySQL	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Oracle MySQL múltiples vulnerabilidades no especificadas-01 Abri16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Oracle MySQL multiples vulnerabilidades no especificadas-02 Abril16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Oracle MySQL múltiples vulnerabilidades no especificadas-06 Abril16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad CSRF de filtrado de Token en Apache Tomcat-Feb16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad de fijación en sesión de Apache Tomcat -Feb16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas

Vulnerabilidad	Causa
Vulnerabilidad de omisión del administrador de seguridad Apache Tomcat-Feb16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad de omisión del administrador de seguridad Apache Tomcat 01 -Feb16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad de denegación de servicio en Apache Tomcat - Mar15	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad de omisión del administrador de seguridad en Apache Tomcat -Junio15 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad de divulgación de directorio en Apache Tomcat - Feb16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad limitada de directorio transversal en Apache Tomcat -Feb16 (Windows)	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Vulnerabilidad de elevación de privilegios en Microsoft SQL Server (2984340) – Remota	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
Usar una solicitud de búsqueda LDAP para devolver información desde el Directorio de Servicios NT	Mala configuración de aplicaciones
Enumeración de Servicios DCE	Mala configuración de aplicaciones
Error en el manejo de llaves temporales al degradar la opción exportar RSA OpenSSL (FREAK)	Mala configuración de aplicaciones
	Carencia de controles criptográficos
OpenSSL TLS 'DHE EXPORT' Vulnerabilidad de omisión MiM LogJam	Mala configuración de aplicaciones
	Carencia sobre control de vulnerabilidades técnicas
	Carencia de controles criptográficos
Vulnerabilidad de descubrimiento de llave privada en servidor Microsoft RDP	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas
12Planet Chat Server one2planet.infolet.InfoServlet XSS	Defectos de productos de Software.
	Carencia sobre control de vulnerabilidades técnicas

Vulnerabilidad	Causa
Información por defecto de página de bienvenida en Microsoft IIS	Configuración por defecto en aplicaciones.
Contenedor de archivos por defecto en Apache Tomcat servlet/JSP	Configuración por defecto en aplicaciones.
Fuente: El autor	

De acuerdo a la información consignada en la anterior tabla se destacan las siguientes situaciones:

- **Defectos de productos de Software:** Las vulnerabilidades pueden ser causadas por defectos en las Aplicaciones que se encuentran instaladas en los equipos.

- **Carencia sobre control de vulnerabilidades técnicas:** Directamente relacionada con la anterior causa, la dirección y el personal de TI debe prever que existan defectos en las aplicaciones, por lo cual debe encargarse de gestionar los medios para tener control sobre éstas ya sea a través de herramientas propias o externas.

- **Configuración por defecto en aplicaciones:** Algunas vulnerabilidades pueden ser causadas debido a la falta de gestión o conocimiento por el personal de TI en la instalación de aplicaciones en las cuales permanecen las configuraciones por defecto que pueden ser causantes de graves problemas de seguridad.

- **Mala configuración de aplicaciones:** Las aplicaciones pueden ser configuradas, sin embargo, sus parámetros pueden ser inadecuados implementando opciones que impliquen brechas en la seguridad de los equipos informáticos.

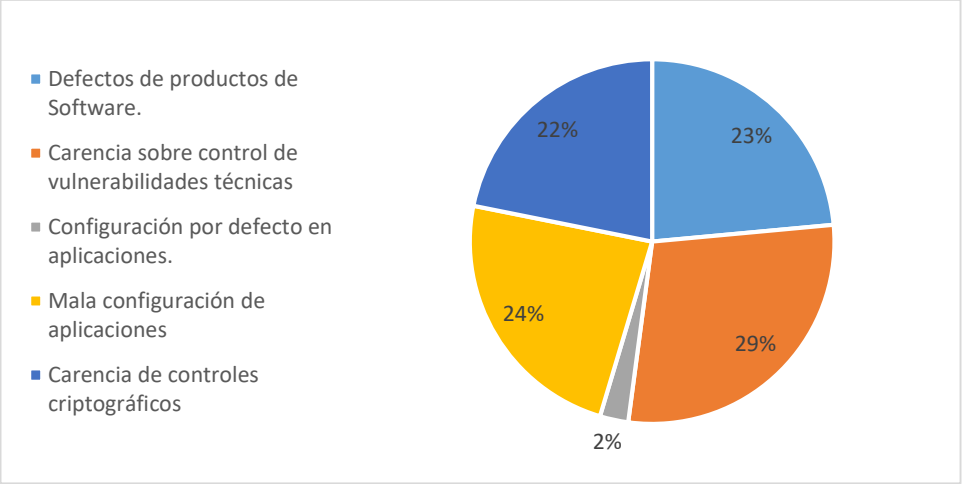
- **Carencia de controles criptográficos:** Sin duda, entre las más frecuentes causantes de las vulnerabilidades, se identificó que no existen controles criptográficos o éstos no corresponden con los adecuados causando que la información que se envíe no esté encriptada, se utilicen algoritmos de encriptación inadecuados, se usen opciones obsoletas, entre otros.

Tabla 19. Proporción Causas y Vulnerabilidades

Causa	Cuenta	Proporción Cuenta Cant. Vulnerb.	Frecuencia Relativa	Porcentaje
Defectos de productos de Software.	28	0,41	0,24	23,53
Carencia sobre control de vulnerabilidades técnicas	34	0,50	0,29	28,57
Configuración por defecto en aplicaciones.	3	0,04	0,03	2,52
Mala configuración de aplicaciones	28	0,41	0,24	23,53
Carencia de controles criptográficos	26	0,38	0,22	21,85
Total	119	1,75	1,00	100,00
Fuente: El autor				

En la gráfica que se muestra a continuación se puede confirmar de una manera más amigable el porcentaje sobre las causas más frecuentes con respecto a las vulnerabilidades encontradas.

Figura 48. Gráfica Proporción entre Causas y Vulnerabilidades



Fuente: El autor

De acuerdo a las vulnerabilidades y causas analizadas sobre el contexto, se podrían establecer las siguientes amenazas con sus respectivas categorías de control que serían el insumo para establecer políticas y procedimientos eficientes en miras a la protección de los activos de información de la organización.

Tabla 20. Relación entre amenazas y controles

Amenaza	Categoría del Control	Control
Denegación de servicio.	Gestión de Capacidad	Para lograr un rendimiento y desempeño óptimos es necesario monitorizar cuidadosamente el uso de recursos en los equipos para hacer las modificaciones y proyecciones necesarias que permitan determinar cambios en el futuro con respecto a la capacidad de los mismos.
Difusión de software dañino.	Controles contra códigos maliciosos	Ante la realidad de contar con un entorno susceptible ante códigos maliciosos, es necesario blindarse a través de la implementación de controles preventivos, correctivos y planes de recuperación complementados por la sensibilización de los usuarios.
Errores de mantenimiento / actualización de programas.	Gestión de las vulnerabilidades técnicas.	Realizar un reconocimiento activo de las vulnerabilidades técnicas de los sistemas es importante para evaluar su impacto y tomar las medidas que se consideren más adecuadas.
Interceptación de información.	Políticas y procedimientos de transferencia de información	Se formulan políticas, procedimientos y controles para la protección de la información que se transfiere de manera física y lógica.
	Acuerdos sobre transferencia de información	Se generan acuerdos que integren criterios de transferencia segura de la información entre usuarios internos y externos a la organización.
	Mensajería electrónica	El masivo uso de sistemas de información de mensajería instantánea o correo electrónico hace que se deba tener en cuenta medios de protección para la información.
	Política de uso de los controles criptográficos	Desarrollar e implementar política de regulación sobre uso de controles criptográficos para proteger la información. Además se garantiza que las herramientas utilizadas son seguras y que fortalecen la privacidad del usuario u organización.
Manipulación de programas.	Uso de programas utilitarios privilegiados	No se permite la instalación de software que tenga la capacidad de anular los sistemas y controles establecidos a las aplicaciones.

Amenaza	Categoría del Control	Control
	Control de accesos a códigos fuente de programas	El acceso al código fuente de las aplicaciones es controlado y gestionado.
Vulnerabilidades de los programas.	Gestión de las vulnerabilidades técnicas.	Realizar un reconocimiento activo de las vulnerabilidades técnicas de los sistemas es importante para evaluar su impacto y tomar las medidas que se consideren más adecuadas.
	Restricciones sobre la instalación de Software.	Se recopilan reglas que definen procesos que permiten materializar el hecho de contar únicamente con Software aceptable instalado en los equipos.
	Seguridad de las aplicaciones del sistema	Se validan escenarios y datos de prueba óptimos para garantizar su tratamiento, el comportamiento de las aplicaciones y el rendimiento de las mismas.
Fuente: El autor		

7.4.2.7. Vectores de Ataque: De acuerdo al análisis de las vulnerabilidades detectadas en los activos de la empresa, se han podido plantear los siguientes vectores de ataque:

- **Uso de configuración por defecto en las aplicaciones instaladas en el sistema:** No es conveniente establecer configuraciones por defecto en las aplicaciones que se instalen en los sistemas de la organización debido a que puede implicar un grave riesgo de seguridad. Un atacante podría aprovechar estos datos conocidos para acceder a los sistemas de manera privilegiada y manipular la información ahí contenida o modificar las configuraciones establecidas para reemplazarlas por otras que sean vulnerables para tener facilidades de acceso permanente.

- **Configuración inadecuada de aplicaciones instaladas en el sistema:** Desde este caso y perspectiva se pueden analizar las siguientes situaciones:

    - Opciones de configuración con parámetros incorrectos o inseguros.
    - Configuración de opciones que no son utilizadas en las aplicaciones.
    - Configuración de aplicaciones para escuchar sobre puertos conocidos

- **No se ha establecido o se ha definido una política débil para la gestión de contraseñas**, lo cual podría facilitar el éxito de ataques de fuerza bruta o de diccionarios para descifrar las contraseñas.

- **Gestión de aplicaciones en servidores y estaciones de trabajo de la organización:** La organización podría estar expuesta si se presentan las siguientes condiciones:

    - No se ha establecido un inventario de aplicaciones y Sistemas Operativos.
    - Existen carencias o inexistencia con respecto a la gestión de vulnerabilidades técnicas.
    - No se ha establecido una política de actualizaciones.
    - Soporte para opciones obsoletas o inseguras.
    - Apertura de puertos innecesarios.
    - Uso de Software obsoleto.
    - Uso de protocolos u opciones de seguridad débiles.

- **Ataques Man in the middle:** Se observan e interceptan los mensajes entre dos actores con el fin de manipularlos a voluntad según los intereses del atacante.

- **Ataques de diccionario:** Se utiliza como insumo un diccionario de datos para probar todas las palabras contenidas en él con el fin de poder descubrir contraseñas. Este ataque es efectivo donde no existen políticas de contraseñas debido a que los usuarios tienden a utilizar palabras fáciles de recordar entre su información confidencial.

- **Ataques de fuerza bruta:** A diferencia de los ataques de diccionario, la fuerza bruta pretende probar todas las combinaciones posibles hasta que exista una coincidencia que encuentre las credenciales correctas y permita obtener el acceso.

- **Ataques de Elevación de privilegios:** Aprovechamiento de vulnerabilidades en aplicaciones para enviar solicitudes que desencadenan condiciones anormales que permiten al atacante acceder al sistema con derechos de superusuario.

- **Envío de información no encriptada:** La información de autenticación o mensajes sin encriptar podría implicar que ante una interceptación del tráfico sea posible para el atacante observar la información sensible en formato plano.

- **Interceptación de tráfico de red:** El uso de sniffers podría permitir que un atacante analice el tráfico de red detectando información sensible o patrones de comportamiento de los usuarios en la organización.

- **Autenticación en las aplicaciones:** Se considera como un blanco de ataque la posibilidad de contar con aplicaciones que:

    - No usen Autenticación segura.
    - No cuenten con un sistema de autenticación.

- **Inconsistencias a nivel de aplicación o de seguridad** mostrando información que no corresponde a los certificados (nombres presentados en una máquina son diferentes)

- **Colisiones sobre algoritmos de encriptación** por uso de cifrados no seguro como MD5 o SHA1.

- **Manejo de errores personalizados en aplicaciones web** para evitar información detallada que pueda exponer información sensible de la aplicación.

- **Ingeniería Social:** La ingeniería social centra su interés en aquellas personas que puedan intervenir en el flujo de información sensible para mediante artimañas o tácticas de manipulación o simple observación obtener cierto beneficio. Estas personas se destacan por su gran conocimiento en relaciones humanas para aprovecharse de la confianza, voluntad o incluso miedo de los otros con el fin de recabar información sensible lo más detallada posible.

- **Ataques XSS:** Orientado hacia aplicaciones web, este ataque permite la inyección de código en determinada petición lo cual permitiría al atacante manipular información sensible con el fin de satisfacer sus intereses o comprometer la integridad y disponibilidad de los sistemas de la organización.

- **Uso de criptoanálisis con intenciones maliciosas:** El criptoanálisis es el proceso inverso a la criptografía consistente en reconstruir un mensaje cifrado en texto simple valiéndose de diferentes métodos, se podría decir que se constituye en el arma enemiga de la criptografía. Su principal meta es descubrir su código o clave de cifrado.

- **Ataques CSRF:** Petición legítima que obliga a realizar una petición sin que el usuario tenga pleno conocimiento de ello. El atacante juega con la confianza del usuario para explotarla sobre un sitio conocido.

- **Información sensible expuesta a nivel público:** Datos confidenciales o sensibles de los usuarios o de la red como los DNS se encuentran disponibles al público, lo cual puede brindar al atacante un panorama suficiente para familiarizarse con los sistemas de la organización y establecer planes u objetivos de ataque.

7.4.2.8. Fase de Explotación: A continuación, se relacionan las vulnerabilidades encontradas en los equipos pertenecientes a la red de la organización que son explotables, indicando el procedimiento a realizar para poder lograrlo.

- **MS15-034 HTTP.sys: Vulnerabilidad ejecución de código remoto y denegación de servicio**

Escáner que detectó la falla: OpenVAS.
Identificador CVE asociado: CVE-2015-1635.
Descripción: Las condiciones de la vulnerabilidad podrían causar la ejecución de código remoto. Sin embargo, se comprobó que enviando una solicitud especialmente manipulada se ocasionó un ataque de denegación de servicio. Se reporta afectación para las aplicaciones que se encuentran desplegadas en el Servidor IIS en los siguientes puertos: 80, 443, 8081, 8089, 8989, 9000 y 9001.

Comando a ejecutar: wget –header="Range: bytes=x-18446744073709551615" http://<servidor>:<puerto>/recurso, donde x es la cantidad de bytes a enviar

- **Agora CGI Cross Site Scripting**

Escáner que detectó la falla: OpenVAS.
Identificador CVE asociado: CVE-2001-1199.
Descripción: La falta de validaciones de entrada en esta aplicación podría causar que se efectúe un ataque XSS exponiendo datos sensibles del usuario.
Comando a ejecutar: Detectando el sitio donde se encuentra desplegada la aplicación se procede a armar un enlace ingresando como parámetro un script javascript. La falta de validaciones de entrada causará la ejecución del código contenido entre las etiquetas.

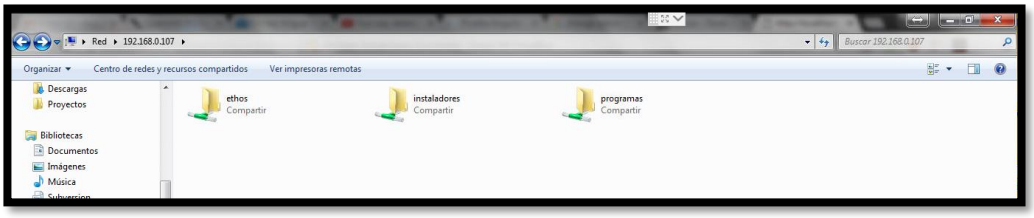
http://<servidor>:<puerto>/store/agora.cgi?cart_id=<script>alert(document.cookie)</script>&xm=on&product=HTML

- **Microsoft Windows SMB/NETBIOS, vulnerabilidad de omisión de autenticación por sesión nula**

Escáner que detectó la falla: OpenVAS.
Identificador CVE asociado: CVE-1999-0519.
Descripción: La autenticación para recursos compartidos de un equipo en red no tiene establecida una contraseña, ésta es nula o por defecto.

A continuación, se puede observar que se accedió a los recursos compartidos de uno de los equipos pertenecientes a la red empresarial sin necesidad de autenticación.

Figura 49. Explotación omisión autenticación de recursos en red.



Fuente: El autor

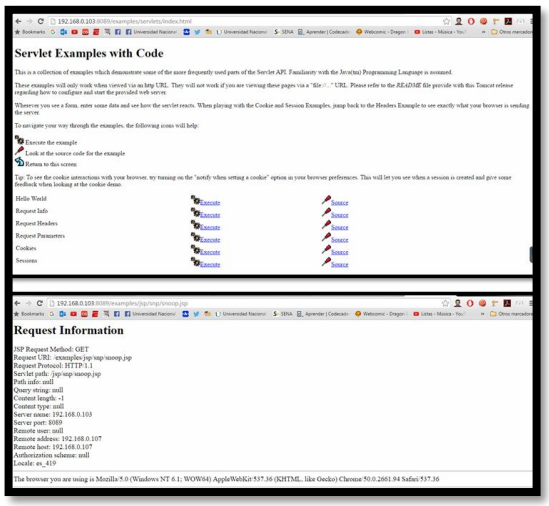
- **Apache Tomcat servlet/JSP container default files**

Escáner que detectó la falla: OpenVAS.
Descripción: Se encontraron archivos por defecto en el directorio donde se encuentra instalado el Servidor Apache Tomcat en las siguientes rutas:

- /examples/servlets/index.html
- /examples/jsp/snp/snoop.jsp
- /examples/jsp/index.html

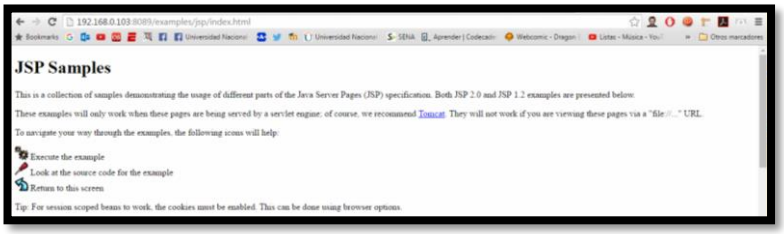
Lo anterior, podría permitir que un atacante determine la versión exacta del servidor que está ejecutándose proveyendo información útil para la construcción de vectores de ataque.

Figura 50. Archivos por defecto en Apache Tomcat



Fuente: El autor

Figura 51. Archivos por defecto en Apache Tomcat



Fuente: El autor

- **12Planet Chat Server one2planet.infolet.InfoServlet XSS**

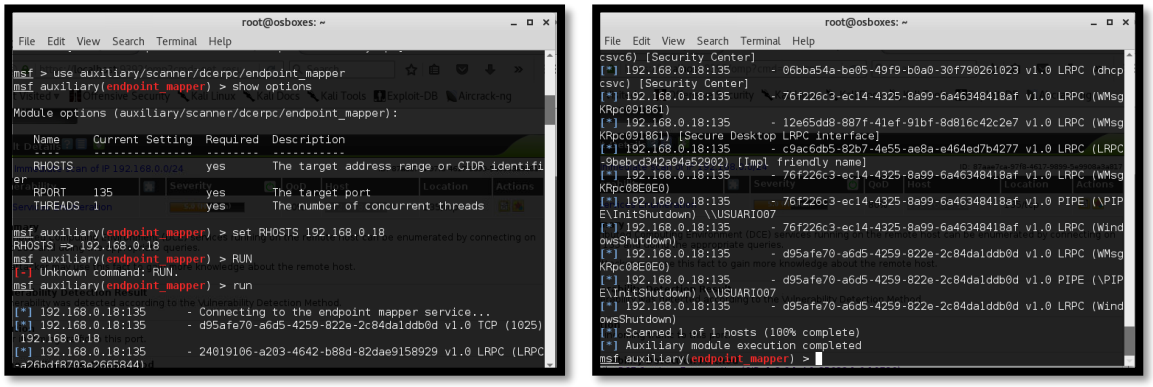
Escáner que detectó la falla: OpenVAS.
Identificador CVE asociado: CVE-2004-0678.
Descripción: La ejecución de una versión vulnerable de esta aplicación, podría permitir que el atacante construya enlaces con scripts maliciosos dirigidos hacia el usuario final.

Comando a ejecutar: Detectando el sitio donde se encuentra desplegada la aplicación se procede a armar un enlace ingresando como parámetro un script javascript. La falta de validaciones de entrada causará la ejecución del código contenido entre las etiquetas.
http://<servidor>:<puerto>/servlet/one2planet.infolet.InfoServlet?page=<script>alert("hy")</script>

- **Enumeración de servicios DCE**

Escáner que detectó la falla: OpenVAS
Descripción: En varios de los equipos de la organización se detectó que el puerto 135 se encuentra abierto, así, es posible detectar los servicios DCE que están ejecutándose permitiendo obtener mayor conocimiento sobre el host remoto. En este sentido, se pudo comprobar la gran cantidad de información arrojada a través de metasploit haciendo uso de sus módulos auxiliares.

Figura 52. Enumeración de Servicios DCE.



Fuente: El autor

- **Vulnerabilidad de divulgación de información por configuración de página de bienvenida por defecto en Microsoft IIS**

Escáner que detectó la falla: OpenVAS
Descripción: Los servidores de la organización ejecutan el servidor web Microsoft IIS el cuál debido a la configuración establecida por defecto se encuentra sujeto o expuesto a una vulnerabilidad de divulgación de información.
En la imagen a continuación se observa que al intentar acceder al servidor web a través de un navegador éste muestra la página de bienvenida por defecto.

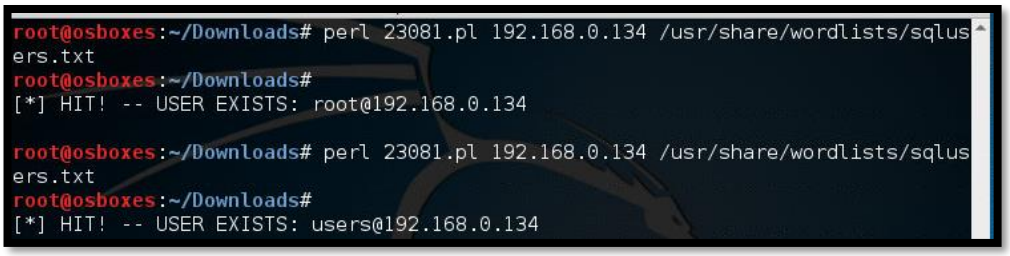
Figura 53. Configuración por defecto página de bienvenida IIS.

Fuente: El autor

- **Vulnerabilidad de enumeración por mensaje de error durante la autenticación de usuarios en MySQL**

Escáner que detectó la falla: OpenVAS
Descripción: El servidor está ejecutando MySQL y la versión de Software que se encuentra instalada es vulnerable permitiendo enumerar los usuarios existentes a pesar de que exista un error en la autenticación para efectuar posteriores ataques de diccionario o fuerza bruta. Seguidamente, se puede observar la ejecución de un exploit que ejemplifica la situación expuesta partiendo de un diccionario simple con nombres de usuario comunes. El exploit se encuentra disponible públicamente a través del siguiente enlace: https://www.exploit-db.com/exploits/23081/.

Figura 54. Enumeración de cuentas MySQL



Fuente: El autor

- **Protección de sitios de la empresa:** Como insumo para las siguientes fases se tomó la clonación de los sitios de la organización mediante el Software HTTrack. Durante este proceso no se presentó ninguna restricción desde los servidores web. Es sumamente importante que se realicen las configuraciones pertinentes para evitar que esto ocurra.

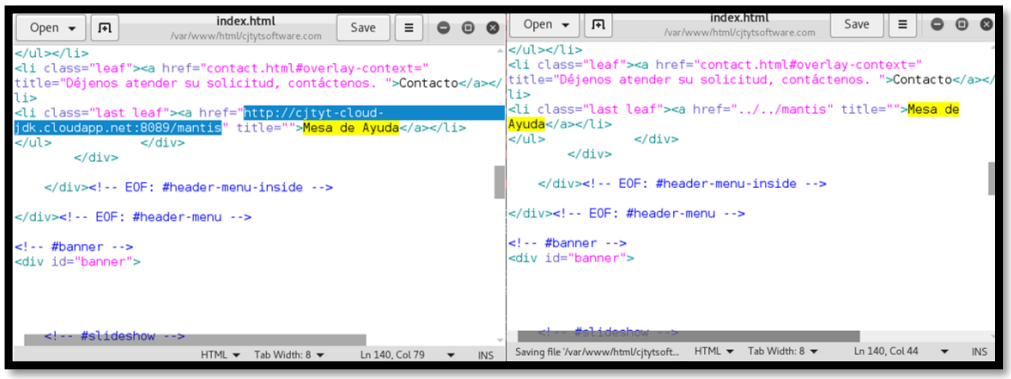
- **Ataque de Phising:** Se clona un sitio conocido de la empresa y a través de un ataque Man in the middle se intentará redireccionar el tráfico dirigido a la IP original para que se visualice la copia falsa guardada en el equipo atacante. Con esto se pretenderá obtener credenciales de acceso que los usuarios ingresen en la pantalla de Login.

Como se mencionó anteriormente, haciendo uso de la herramienta HttCrack se realizó la copia de los sitios web que corresponden a la empresa:

Página principal: http://cjtytsoftware.com/
Mesa de ayuda: http://cjtyt-cloud-jdk.cloudapp.net:8089/mantis/login_page.php.

Estos sitios estarán desplegados en un servidor Apache perteneciente al equipo atacante. Se modificará el enlace hacia la mesa de ayuda con el fin de que lleve a la víctima hacia la copia local y no hacia el sitio original.

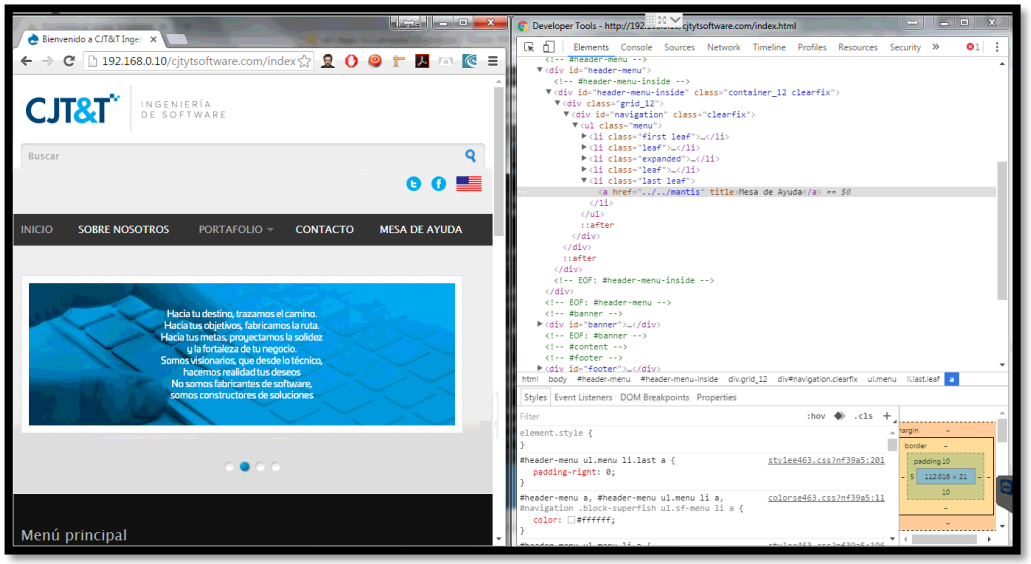
Figura 55. Modificación del Formulario



Fuente: El autor

Se puede observar la página clonada la cual se encuentra en el servidor Apache del equipo atacante y a la que se puede acceder a través de la red de la organización. A través de la inspección del sitio se puede observar el enlace modificado.

Figura 56. Evidencia de puesta en marcha de la página falsa



Fuente: El autor

Asimismo, a continuación, se demuestra que el enlace lleva hacia la copia local de la pantalla de Login de la mesa de ayuda.

Figura 57. Evidencia de puesta en marcha de la página falsa, mesa de ayuda

Fuente: El autor

Posteriormente, se aplicó un ataque DNS Spoofing facilitado por la herramienta Ettercap. Para efectuar el anterior ataque se modifica el archivo etter.dns para ingresar los registros DNS que apliquen de acuerdo al objetivo. En este caso, se efectuó la siguiente configuración teniendo en consideración que la dirección del equipo atacante es **192.168.0.10** y responde a una máquina virtual de un equipo ubicado en la red empresarial:

Se configura el archivo DNS de Ettercap, agregando el sitio que será atacado.

Figura 58. Modificación etter.dns

Fuente: El autor

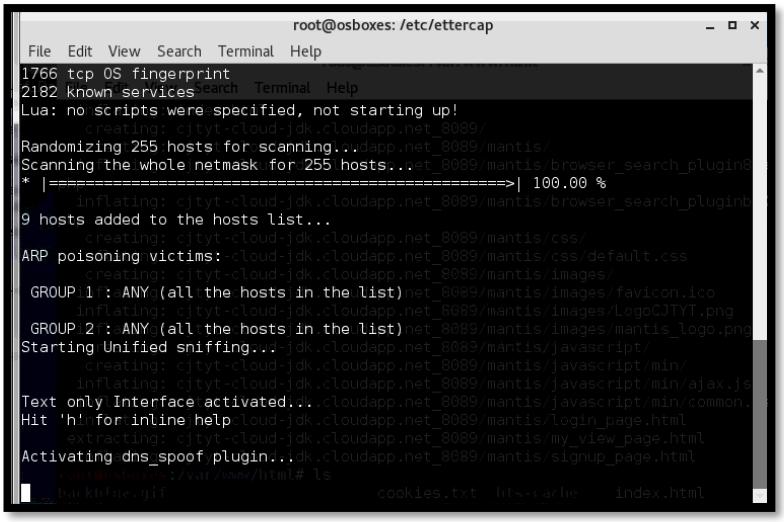
Ahora, se procede a ejecutar el ataque DNS Spoofing haciendo uso del comando **“ettercap -Tqi eth0 –P dns_spoof –M arp”**, asumiendo que “eth0” es la interfaz que tiene acceso a la red de la organización a través del equipo atacante.

Figura 59. Comando para ejecutar el Ataque DNS Spoofing

Fuente: El autor

Posterior a la ejecución del comando, ettercap hace un escaneo de la red, verifica los hosts activos, inicia el proceso de sniffing unificado y procede a activar el ataque de DNS Spoofing, tal como se indica a continuación:

Figura 60. Ejecución del Ataque DNS Spoofing



Fuente: El autor

Ahora, desde el equipo víctima se procede a intentar acceder a la página web de la organización y posteriormente a la mesa de ayuda con éxito. Con el fin de

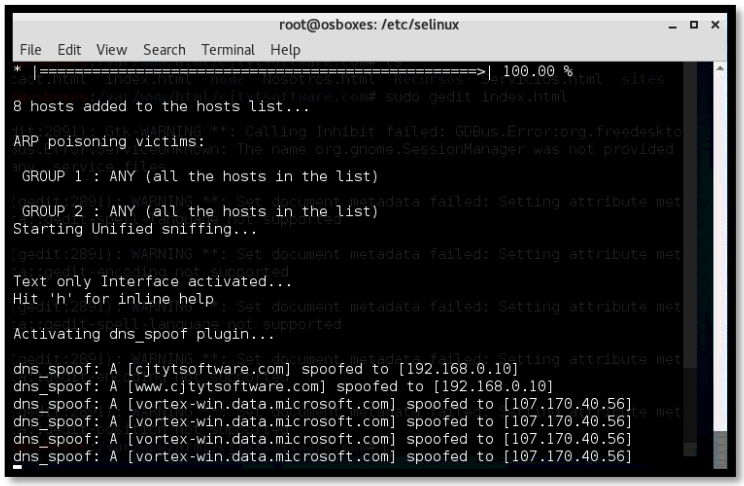
diferenciar la URL original de la correspondiente al ataque, se observa que su comportamiento es diferente.

Figura 61. Acceso a la página falsa de la mesa de ayuda

Fuente: El autor

Se identifica desde la consola que efectivamente una petición hacia el sitio ha sido recibida y suplantada hacia la IP del equipo atacante.

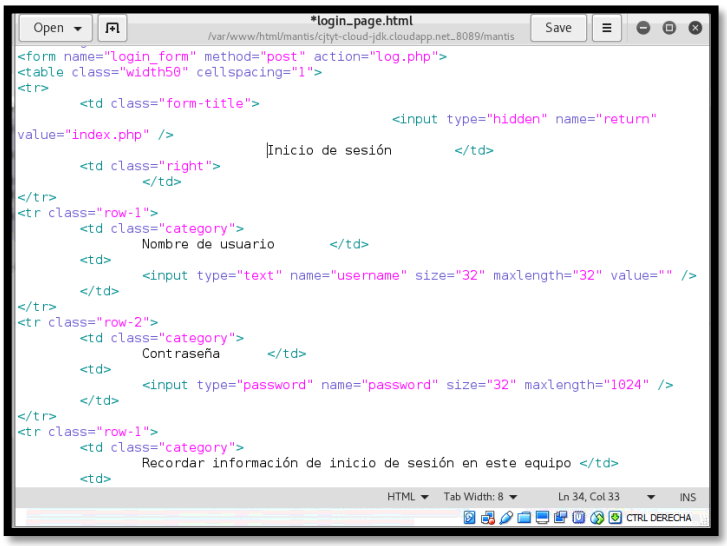
Figura 62. Log de Peticiones Ettercap



Fuente: El autor

Como parte final del ataque se modificará el formulario de la página de la mesa de ayuda para que almacene en un archivo plano las credenciales de acceso que el usuario utiliza. La petición POST se dirigirá hacia el archivo “log.php”.

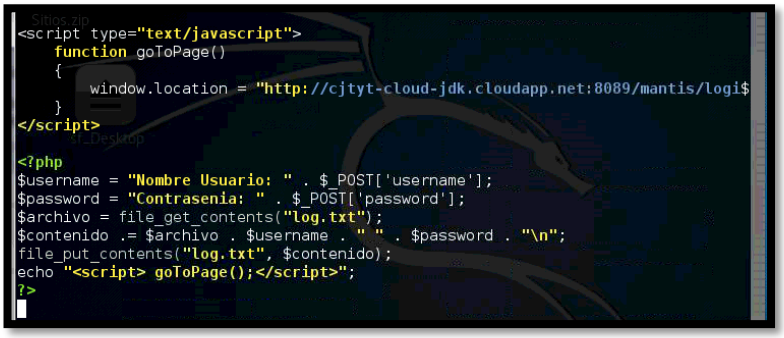
Figura 63. Modificación Formulario de Acceso



Fuente: El autor

A continuación, los contenidos del archivo “log.php” en el cual se observa que se reciben los datos de acceso desde el formulario y se loguean en un archivo de texto para posteriormente redireccionar al usuario a la página original.

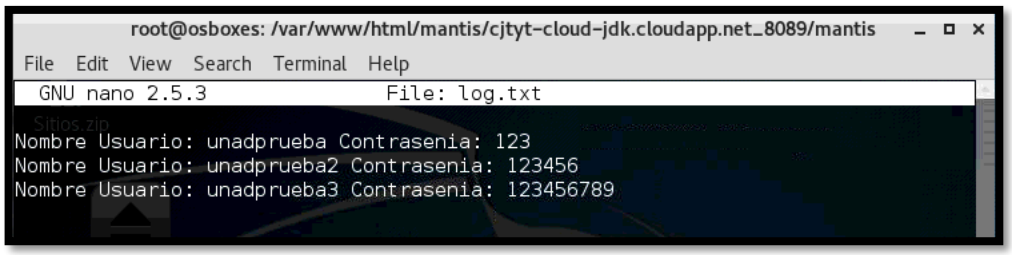
Figura 64. Página PHP para logueo de peticiones



Fuente: El autor

A continuación, se observa el resultado tras realizar tres intentos en la página falsa.

Figura 65. Log de datos de acceso



Fuente: El autor

Análisis de tráfico: Se realiza un ataque de ARP Spoofing redireccionando todo el tráfico desde determinado objetivo hacia servidores o routers para verificar si éste está cifrado o si por el contrario se puede observar información sensible en formato plano viajando por la red.

En primer lugar, se ingresa a la terminal el comando “echo 1 > /proc/sys/net/ipv4/ip_forward” para habilitar el redireccionamiento IP, esto con el objetivo de mantener la conexión a Internet y así evitar que la víctima descubra el ataque fácilmente.

Figura 66. Activación de redireccionamiento IP

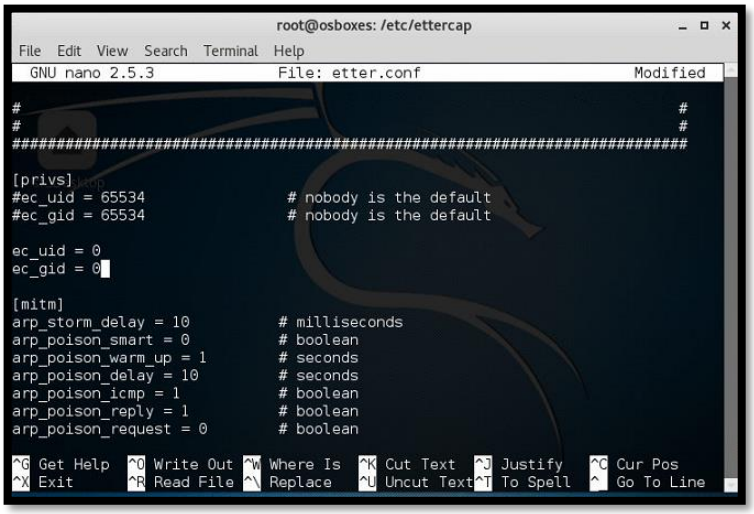
Fuente: El autor

Posteriormente, se procederá a revisar el archivo de configuración de la aplicación “Ettercap”, herramienta con la cual se efectuará el ataque. La ruta de dicho archivo corresponde a “/etc/ettercap/etter.conf” en la distribución Kali Linux.

En este archivo se realizarán dos acciones:

- Cambiar los parámetros “ec_uid” y “ec_gid” a 0, con el fin de permitir a la aplicación tener acceso de superusuario.

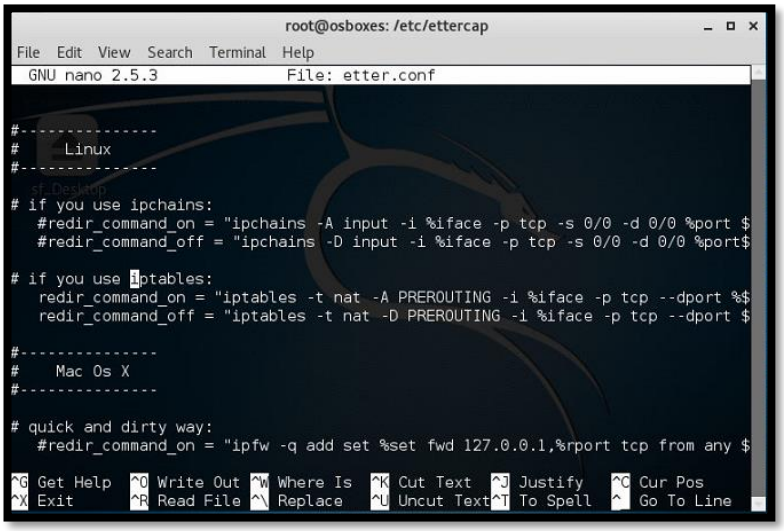
Figura 67. Super usuario para Ettercap



Fuente: El autor

- Se habilita la regla iptables para “Ettercap”.

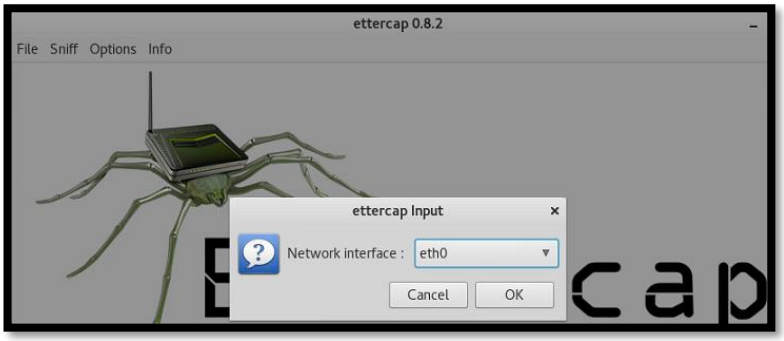
Figura 68. Reglas Iptables en Ettercap



Fuente: El autor

Ahora, se ejecuta el comando “ettercap -G” en consola para abrir la interfaz gráfica de la aplicación desde la máquina atacante. Se procede a seleccionar la opción “Unified sniffing” en el menú “Sniff”. Paso siguiente, se selecciona la interfaz de escucha.

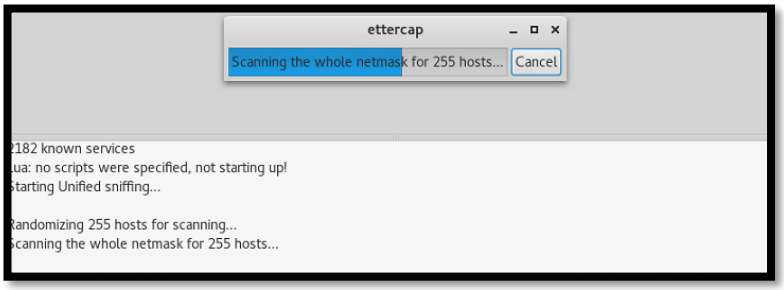
Figura 69. Interfaz de entrada en Ettercap



Fuente: El autor

Una vez se seleccionan la interfaz de entrada, se procede a realizar el escaneo de los hosts presentes en la red. Para esto, se selecciona la opción “Scan for Hosts” ubicada en el menú “Hosts”. Posterior a este paso, se da clic en el mismo menú en la opción “Host lists” donde se encontrará la lista con los resultados del escaneo en la red.

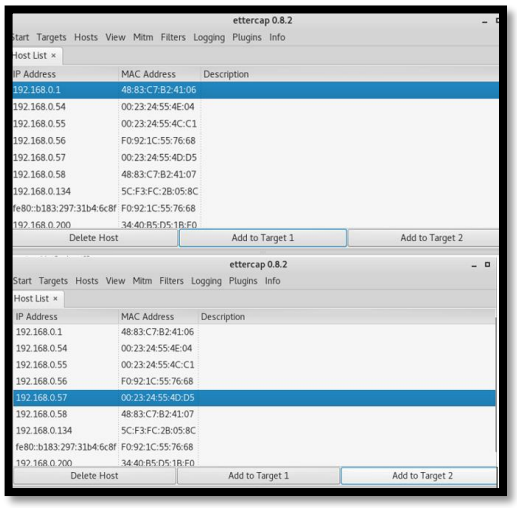
Figura 70. Escaneo de hosts en la red a través de Ettercap



Fuente: El autor

Con los resultados del escaneo, en la pantalla de lista de equipos se añaden los objetivos del ataque teniendo en cuenta que el “Objetivo 1” será la puerta de enlace (192.168.0.1) y el “Objetivo 2” el equipo víctima (192.168.0.57).

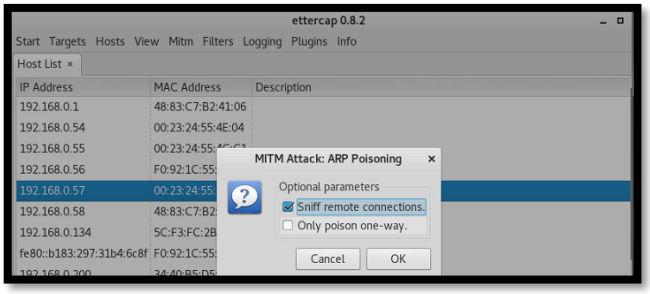
Figura 71. Especificación de Hosts Objetivo en Ettercap



Fuente: El autor

Una vez se definen los objetivos del ataque, se activa el ataque Man in the middle especificando que se realiza sniffing a conexiones remotas.

Figura 72. Activación ataque Man in the middle

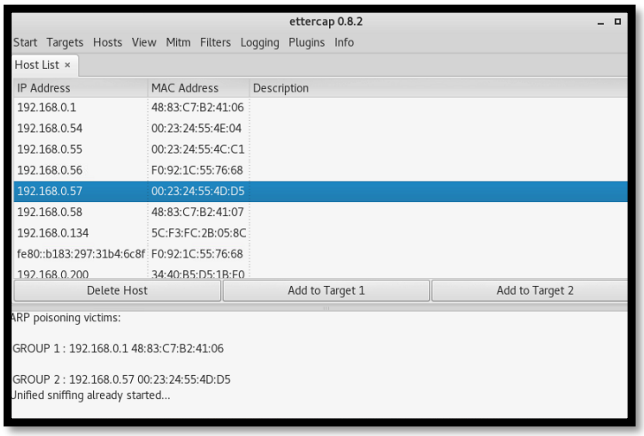


Fuente: El autor

La aplicación mostrará en su log los grupos que corresponden a víctimas del ataque según la configuración que ya se ha establecido en los pasos anteriores. Por último,

para iniciar con el envenenamiento de ARP en la víctima y router se procede a dar clic en el menú “Start” y su opción “Start Sniffing”.

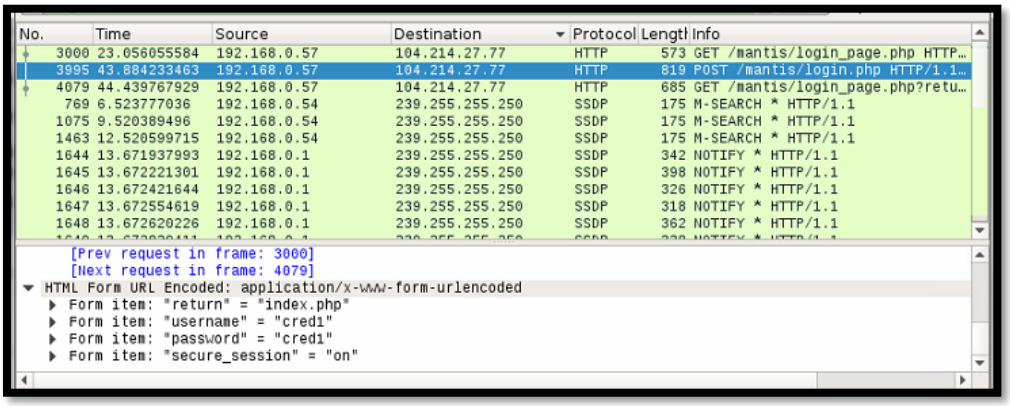
Figura 73. Inicio del Sniffing en Ettercap



Fuente: El autor

Por efecto del redireccionamiento será posible observar el tráfico entrante y saliente hacia y desde el equipo víctima en el equipo atacante. Para ello se hará uso de Wireshark. Se procedió a navegar en la mesa de ayuda de la organización a través de Internet e ingresar datos en el formulario de Login. Posteriormente, se detuvo el análisis de tráfico y se procedió a revisar las capturas. El hallazgo fue una petición POST en la cual se pudo observar las credenciales de acceso usadas para intentar el ingreso al sistema. El archivo con el escaneo completo se puede encontrar en el Anexo L del presente documento.

Figura 74. Análisis de tráfico con Wireshark



Fuente: El autor

7.5. FORMULACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

7.5.1. Información General

Razón Social: CJT&T Ingeniería de Software.

Tipo de Negocio: Desarrollo de Software a la medida.

Sector Comercial: Sector Terciario, prestación de servicios.

Misión: Ofrecemos servicios para el uso y aprovechamiento de la tecnología informática, brindamos soluciones con calidad, eficiencia y efectividad. Optimizamos procesos empresariales con la constante investigación de las bondades que permite la tecnología informática.

Visión: CJT&T en el año 2017, más que una empresa será una familia integrada por miembros comprometidos, motivados y entregados a la causa de posicionar la compañía como la mejor. Los clientes encontrarán, no un proveedor, sino un aliado en quien confiar sus inversiones en tecnología de información; la sociedad tendrá un referente de honestidad, transparencia y compromiso total con la construcción de una mejor región.

Alcance: Basado sobre las pruebas de penetración llevadas a cabo de manera interna y externa en la empresa CJT&T Ingeniería de Software, estas políticas son aplicables para empleados, clientes y proveedores.

Sus fundamentos permiten garantizar buenas prácticas para que los activos de información sean operados de manera segura respetando las leyes estatales y reglamentos internos.

Responsables: La implementación y notificación del presente documento en la organización es el gerente. La actualización de las políticas de seguridad informática estaría a cargo de personal capacitado en el área disciplinar; también se podría encargar esta tarea al Departamento de Tecnologías de la Información (TI) según sean detectadas necesidades de seguridad desde distintos segmentos de la organización.

7.5.2. Objetivos

Brindar a empleados, clientes y proveedores de CJT&T Ingeniería de Software el compendio de información necesaria que les sirva como insumo y herramienta para ser capaces de proteger los activos de información de la organización.

Mantener un documento actualizado donde se integren y sea posible controlar todas las actividades referentes a la seguridad física y lógica de los activos de información de la organización.
Posterior a la implantación de las Políticas de Seguridad informática se pretende que la empresa:

- Cuente con un medio para garantizar una mayor protección de sus activos a través de la cohesión del personal que estará involucrado en diversas responsabilidades que serán claves para el aseguramiento de la máxima seguridad.
- Socialice cada punto relevante con los actores implicados en la seguridad de los activos de la organización.
- Establezca una comunicación permanente entre todos los actores intervinientes en el proceso de seguridad con el fin de establecer un canal común y eficiente.
- Genere un sentido de pertenencia que refleje el compromiso de empleados, clientes y proveedores.

7.5.3. Notificación de Violación a la Seguridad: Todo el personal debe notificar problemas de seguridad que sean detectados. Preferiblemente la comunicación de estos acontecimientos se debe reportar por medio electrónico al correo de la gerencia. Sin embargo, si los sistemas no están activos el incidente debe ser comunicado por escrito o personalmente. La gerencia será la encargada de tomar las medidas pertinentes para que el incidente presentado sea solucionado en el menor tiempo posible.

El incumplimiento sobre los lineamientos establecidos en el presente documento y que pueda comprometer la seguridad de la organización por parte de empleados, clientes o proveedores derivará en fuertes sanciones de tipo disciplinario en concordancia con la aceptación de las condiciones prescritas.

7.5.4. Base de Datos: El Software que se encuentre interactuando entre las diferentes dependencias de la organización y que esté relacionado con sus procesos de negocio indudablemente manejará un gran de volumen de datos sensibles y confidenciales. Por esta razón se deben tener en cuenta las siguientes observaciones:

- Preferiblemente se debe manejar un mismo Sistema de Gestión de Bases de Datos (SGBD) con el fin de centralizar mecanismos de protección en caso de presentarse algún tipo de falla.

- Es preciso que se establezca el principio de mínimo privilegio. Así, se definirán roles asociados a las necesidades de cada sistema de información y en caso de requerir accesos, se deberá solicitar previamente al administrador del sistema quien será el encargado de evaluar la situación y aceptar o rechazar el registro o modificación de permisos/privilegios.

- Deben existir políticas de respaldo para las bases de datos de acuerdo a su grado de criticidad, así como su frecuencia de actualización llevando un registro detallado sobre cada evento y procurando por su almacenamiento seguro.

- Para facilitar las tareas de auditoria a nivel de base de datos se deben establecer los mecanismos que permitan centralizar el almacenamiento de registros históricos sobre las transacciones relevantes, facilitando la posterior labor de análisis de información.

- Se garantiza la ejecución de rutinas para optimizar las bases de datos garantizando su integridad y confiabilidad, así como la de los sistemas de información que las utilizan.

7.5.4.1. Política de Respaldo:

- Bases de Datos: Para protección de la información generada en los procesos de la organización, el servidor de base de datos implementa un sistema de disco duro espejo a raíz de lo cual la información se almacena simultáneamente en dos unidades de disco, pretendiendo de esta manera evitar una posible pérdida de información en caso de fallas.

El personal de TI realizará semanalmente copias de seguridad de las bases de datos las cuales serán almacenadas en discos ópticos (CD / DVD) con características de no re-escribibles para evitar la modificación de la información en estos incluida y adicionalmente en un disco duro externo provisto por la organización con el fin de evitar que la degradación de los discos ópticos pueda afectar la disponibilidad e integridad de la información. Estos se guardarán en la oficina de gerencia custodiada bajo llave. Los discos ópticos se etiquetan con marcador permanente o por medio impreso indicando la fecha de inicio y fecha de fin del respaldo (B. IN: MM/DD/YY – FN: MM/DD/YY).

Por otro lado, es obligatorio realizar la verificación sobre las copias de seguridad generadas. De manera que, para facilitar este proceso, se llevará a cabo sobre un Equipo especial dispuesto específicamente para esta tarea; se solicitará apoyo de los proveedores de sistemas de información en caso de considerarse necesario.

- Sistemas Operativos y Aplicaciones: Debido a la importancia de contar con un ambiente adecuado para el desarrollo de aplicaciones, al momento de realizar una instalación limpia del Sistema Operativo y contar con un ambiente funcional de trabajo se procederá a generar una imagen del disco duro con el fin de que sirva de insumo posterior para su restauración en caso de presentarse alguna eventualidad. El almacenamiento de esta imagen se realizará en un disco duro externo o si es posible en la unidad de almacenamiento del mismo equipo en una partición diferente a la que contiene el Sistema Operativo.

7.5.5. Frecuencia de Evaluación de las Políticas: Las políticas de seguridad informática serán evaluadas cada año en razón de las nuevas necesidades detectadas por la organización en articulación con las diferentes áreas que la conforman guiadas por el líder de TI, la gerencia y la asesoría de un experto en Seguridad Informática.

7.5.6. Política de Legalidad

7.5.6.1. Licenciamiento: Todo el Software propietario que sea utilizado por la organización deberá estar soportado por los respectivos documentos físicos o digitales que garanticen su legitimidad. Aquellas aplicaciones que no sigan esta regla deberán ser eliminadas de manera inmediata de cualquier equipo de la organización en el que se encuentren instaladas.

7.5.6.2. Autorización en Instalación de Software: La instalación de Software en los equipos informáticos de la organización debe estar regulada por el personal de TI, por tal manera, se prohíbe de manera estricta que se realice cualquier acción sin previa autorización, sin importar, si este ha sido adquirido de manera legal por el propio usuario. Las aplicaciones de distribución libre o gratuita serán únicamente instaladas con el consentimiento previo del personal encargado.

7.5.7. Políticas de Seguridad Física

7.5.7.1. Acceso Físico

- Se dispondrá de un espacio exclusivo donde se ubicarán los equipos de telecomunicaciones, así como servidores de la organización.

- Se garantiza que el acceso físico a los equipos de telecomunicaciones y servidores de la organización está totalmente restringido en un cuarto bajo llave. Únicamente la gerencia y el líder del área de TI podrán acceder a dicho espacio cuando sea necesario. Si fuera necesario que otra persona ingresará a esta locación lo hace con la debida autorización previa de los líderes anteriormente mencionados los cuales supervisarán cualquier acción que se realice.
- Se lleva un registro físico y lógico sobre el acceso al cuarto de servidores, en el cuál se indican datos personales, fecha y hora de ingreso y salida y motivo por el cual se ingresa al espacio.

- Únicamente el personal autorizado podrá manipular los recursos en el cuarto de servidores. Toda acción realizada debe ser reportada a través de la hoja de vida de los equipos y si fuera necesario moverlos, cambiarlos o retirarlos se debe registrar la actividad en el formato de entradas y salidas y adicional a ello notificar a la gerencia y líder del área de TI.

- La información en medio físico se archivará en un cuarto exclusivo para la custodia de esta información. Se incluirá en carpetas tipo AZ marcadas con el tipo de registros.

7.5.7.2. Protección Física

- **Mantenimiento de los Equipos:** Se realiza mantenimiento periódico de los equipos para asegurar su disponibilidad e integridad permanente, teniendo en cuenta:

    - Los servidores deben recibir limpieza al menos una vez por semana para evitar afectaciones por contaminación ambiental.
    - En caso de no presentar fallas, se realiza mantenimiento preventivo a los equipos de cómputo cada 3 meses.
    - Solo personal autorizado brinda mantenimiento y lleva a cabo reparaciones en los equipos de cómputo.

- Antes de realizar cualquier tipo de tarea de mantenimiento preventivo o correctivo se elimina toda información confidencial, realizando copias de respaldo de la información crítica.
- Se lleva a cabo un registro de hallazgos y de fallas potenciales o inminentes en todo mantenimiento preventivo y correctivo realizado.
- El registro mencionado anteriormente se consigna en el Formato de Hoja de Vida del Equipo.

7.5.7.3. Instalaciones

- **Infraestructura**

  - Se implementan estándares vigentes para realizar el cableado estructurado en la red de la organización.

  - Se segmentan las redes en la medida de lo posible para evitar colisiones a causa de un dominio de broadcast que involucre una excesiva cantidad de equipos.

  - Se debe contar con planos actualizados de la instalación eléctrica de la organización.

  - Se debe contar con los diagramas de red actualizados.

- **Suministro Eléctrico**

Se debe garantizar que las instalaciones eléctricas de la organización se encuentran en buen estado.

Se dispone de una o varias UPS con capacidad suficiente para soportar los equipos de telecomunicaciones y servidores con el fin de prevenir el riesgo de daño físico. Las instalaciones eléctricas y equipos de soporte son revisados anualmente para garantizar que se encuentran en un estado adecuado para su operación efectiva.

- **Control Ambiental**

Se debe contar con sistemas de extinción contra incendios en cada uno de los cuartos de la organización. El cuarto de servidores deberá contar con un extintor de soporte adicional como medida de prevención ante una posible falla del primero.

7.5.7.4. Inventario

Se lleva un inventario detallado sobre los equipos de cómputo y de telecomunicaciones que se encuentra en la organización.

Se lleva un inventario detallado sobre las aplicaciones de Software autorizadas para instalación y sobre aquellas que actualmente se encuentran instaladas en cada uno de los equipos de cómputo.

7.5.7.5. Recursos de los usuarios

- **Uso de Recursos:** A continuación, se presenten las obligaciones de los empleados de la organización con respecto a la seguridad relacionada con los equipos a su cargo o de los cuales tengan que hacer uso debido a la ejecución de alguna de sus responsabilidades:

  - Los equipos de cómputo sólo deben usarse para actividades de trabajo y no para otros fines.

  - Debe respetarse y no modificar la configuración de hardware y software establecida por el área de TI.

  - No deben usarse CDs, USB u otros medios de almacenamiento en cualquier equipo a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos y que su uso corresponda para efectos estrictamente laborales.

  - No se permite fumar, comer o beber mientras se está usando un equipo de cómputo.

  - Cualquier falla en los equipos debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

  - La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente a la gerencia o área de TI.

- **Retiro de Recursos:** Cuando un empleado deja de laborar en la organización, éste debe entregar sus recursos al área encargada la cual verificará la correcta devolución. Asimismo, e deben retirar todos sus accesos o medios para el ingreso a los recursos de la organización.

- **Derechos de autor y Propiedad Intelectual:** Todos los productos resultantes de la construcción de Software realizado por los empleados durante su vinculación con la organización son de propiedad exclusiva de CJT&T Ingeniería de Software, por tal razón amparada en los derechos de autor y propiedad intelectual está prohibida su copia o almacenamiento en medios físicos y digitales externos, así como su distribución o comercialización. Para garantizar este compromiso, durante la vinculación del empleado se especificará un acuerdo de confidencialidad que tenga en cuenta lo anteriormente expuesto.

7.5.8. Políticas de Seguridad Lógica

7.5.8.1. Red

- El uso de la red en la organización satisface el objetivo de servir como medio de intercambio de información en el contexto laboral entre empleados, clientes y proveedores. Queda totalmente prohibido el uso de las redes informáticas de la empresa como medio de entretenimiento o para transacciones personales de los empleados.

- En concordancia con las políticas aquí documentadas, la organización no es responsable por el tráfico que circula sobre la red. Cualquier movimiento inusual es total responsabilidad del empleado.

- El acceso a recursos compartidos en cada uno de los equipos de la red informática debe requerir un proceso de autenticación. Asimismo, dicho acceso debe realizarse con previo consentimiento del responsable del equipo.

- En la red interna no existen archivos compartidos cuya información pueda afectar esta política.

- El análisis de la red es una acción estricta de administradores, por tanto, el personal de la empresa no está autorizado para utilizar aplicaciones asociadas a esta tarea ni a efectuar acciones relacionadas.

- En caso de que los administradores de la red detecten uso no aceptable de los recursos, se suspenderá inmediatamente al equipo fuente de dicho tráfico. El empleado involucrado a cargo de estos recursos deberá justificar esta situación; en consideración de esto se realizará la reconexión.

7.5.8.2. Servidores

- **Configuración:** Los administradores de la red deberán garantizar la correcta implementación sobre configuración de seguridad en los servidores que se encuentran en la red informática velando por que se cumplan las siguientes condiciones:

- La configuración realizada a los servidores restringe el acceso a recursos como directorios, y aplicaciones que están en contacto con los usuarios. Los permisos serán adaptados de acuerdo a las responsabilidades de los empleados.

- Se deberá velar por reinicios programados de los servidores periódicamente, preferiblemente en un periodo no mayor a un mes para evitar la saturación de recursos que puedan causar una denegación de servicio.

- Se debe depurar los logs del servidor mensualmente de manera que se garantice su integridad y disponibilidad en caso de que algún evento requiriese de su revisión.

- La configuración del servidor debe ser revisada trimestralmente para verificar que se encuentra adaptada a las necesidades de la organización.

- Se evaluará de manera precisa si el servidor ofrece servicios a la red que requieren o no de acceso a Internet.

- **Correo electrónico:** La organización maneja un servicio externo de correo electrónico provisto por Microsoft. Así, se deben tener en cuenta las siguientes pautas:

- El servicio de correo electrónico que se proporciona a los empleados sólo debe usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la organización.

- El personal del área de TI estará encargado de asignar cuentas de usuario a los empleados en el tiempo posterior a su vinculación y de retirarlas cuando dejen la empresa. Para esto, se asignará una contraseña por defecto a su nueva cuenta la cual deberá modificarse en el primer ingreso.

- Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la organización, se debe ejercer

cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de CJT&T Ingeniería de Software sin la debida aprobación.

- Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio de almacenamiento.

- **Bases de Datos**

  - A menos de que represente problemas de funcionamiento o seguridad, la información contenida en las bases de datos no debe ser eliminada del sistema.

  - Los administradores de bases de datos son los únicos facultados para otorgar accesos a los empleados de la organización.

  - Las contraseñas asignadas a las cuentas de usuario únicamente podrán ser modificadas por los administradores de bases de datos. El empleado que lo requiera deberá realizar la solicitud formal por medio escrito o digital para mantener un seguimiento sobre el usuario afectado en cuestión.

7.5.8.3. Recursos de Cómputo

- Seguridad: El personal del área de TI es el único autorizado para instalar herramientas de software y hardware en los equipos para reforzar la seguridad.

El área de TI estará encargada de capacitar u orientar a los empleados cuando sea requerido sobre las medidas de seguridad y herramientas incorporadas en sus equipos asignados.

- Soporte: El personal del área de TI estará encargado del soporte solicitado por los empleados de la empresa en referencia a dificultades en sus dispositivos tecnológicos.

El personal encargado de soporte deberá contar con la autorización para acceder de manera física o remota a los equipos de los empleados con el único objetivo de solucionar los problemas solicitados.

Se deberá auditar de manera periódica los sistemas y servicios en la red informática con el fin de verificar si existen archivos o configuraciones no autorizadas o inválidas que podrían poner en riesgo la seguridad informática en la organización.

Reportar los incidentes de seguridad a la gerencia con sus respectivos soportes y evidencias en caso de ser posible, con el fin de que ésta tome las medidas pertinentes al caso.

- Gestión de Capacidad y Renovación: Los empleados deberán reportar necesidades a nivel de capacidad de hardware en caso de que sus funciones conlleven superar las características específicas de la capacidad instalada con el fin de asignarle un nuevo equipo en caso de estar disponible u ordenar la compra sobre uno que se adapte a sus requerimientos.

Es necesario que se defina la vida útil de las estaciones de trabajo, servidores y equipos de telecomunicaciones para definir un plan de renovación que no impacte de manera excesiva las operaciones de la organización.

7.5.8.4. Antivirus

Es responsabilidad del área de TI instalar una herramienta de Antivirus con consola administrable, la cual debe mantenerse actualizada semanalmente. Si se detecta la presencia de un virus u otro agente potencialmente peligroso tanto en la red como en los equipos, se debe notificar inmediatamente al área de TI, la cual pondrá el equipo en cuarentena hasta que el problema sea resuelto. El personal de TI es el responsable de hacer escaneos semanales para toda la red, y el empleado de hacerlo en su equipo asignado.

7.5.8.5. Control de Acceso: Se incluye este ítem con el fin de impedir el acceso no autorizado a sistemas de información, bases de datos y servicios de información implementando seguridad en el acceso mediante técnicas de autenticación y autorización.

Al registrar el acceso de cada usuario en su interacción con los sistemas informáticos, se busca obtener mayor control sobre sus acciones, reforzando la seguridad mediante el registro de eventos llevados a cabo.

De igual manera, y no menos importante se recomienda la concientización de los usuarios para que conozcan cuál es su papel frente al uso de contraseñas y equipos.

- Se deberá asignar credenciales de acceso a todo empleado que requiera interacción con los sistemas de la organización. En dicho registro se tendrá en cuenta las responsabilidades del empleado con el fin de determinar los permisos

que se deberán otorgar y revocar con respecto al acceso de sistemas, bases de datos y servicios de información.

- Las credenciales de acceso son personales e intransferibles en toda circunstancia y deben regirse sobre buenas prácticas de seguridad. Además, no debe ser escrita en documentos de común acceso.

- El registro de usuario en el sistema requiere que el empleado proporcione datos básicos personales como nombres y apellidos, número de identificación y teléfono.

- Preferiblemente, el nombre de las cuentas de usuario debe incluir el primer nombre, seguido por el carácter punto (.) y finalmente seguido por el primer apellido del empleado. En caso de que coincida con un nombre de usuario ya creado, se utilizará el segundo apellido.

- La clave de acceso debe tener como mínimo 6 caracteres, ser de fácil recordación, no estar basadas en palabras de fácil identificación o relacionadas con información personal del usuario, ser alfanumérica y utilizar combinación de letras mayúsculas y minúsculas y números.

- El sistema debe permitir el cambio de contraseña cuando el Software o el operario lo soliciten. Además, se debe denegar la nueva contraseña como la actual.

- El software solicita el cambio de la clave de acceso al primer ingreso y solicitará de nuevo el cambio cada 30 días. Los usuarios con permisos especiales deben cambiar su clave en un periodo no mayor a 30 días. Adicionalmente, se debe cambiar la contraseña si se tiene indicio de vulnerabilidad de esta o del sistema.

7.5.8.6. Responsabilidades personales

- Los empleados se hacen responsables de toda la actividad relacionada con el uso de sus credenciales de acceso.

- Está prohibido utilizar los accesos de otro empleado, incluso aunque se hubiera recibido su autorización para hacerlo.

- En caso de sospecha sobre uso de las cuentas del empleado por parte de terceros no autorizados, se debe cambiar de manera inmediata la contraseña. El administrador de la red tiene la obligación de autorizar este cambio y ejecutarlo en el menor tiempo posible.

- Si los sistemas no solicitan el cambio de contraseñas, el usuario tiene la obligación de realizar el cambio según los tiempos definidos en la política de control de acceso.

- El almacenamiento de información en los equipos asignados se realiza de manera temporal; esta información es confidencial, por lo cual se deberán establecer las medidas de protección y velar por su cumplimiento buscando guardar la máxima reserva. Además, se debe comprender que ante un cambio de funciones o dimisión de las actividades la empresa ésta se eliminará bajo supervisión del personal encargado.

7.5.8.7. Uso apropiado de recursos

- El uso de recursos está diseñado exclusivamente para actividades relacionadas con la organización.

- No está permitido instalar o almacenar aplicaciones o información no relacionada con las funciones del empleado a nivel laboral.

- Está prohibido ingresar información ofensiva en los sistemas o la red de la organización que afecte su reputación o la de los empleados, clientes o proveedores.

- La información empresarial a cargo del empleado debe ser preservada en el desempeño de sus funciones. Por tanto, no está permitido que ésta sea manipulada de ninguna forma.

7.5.9. Seguridad Perimetral: Se encarga de definir los recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Con esto se logra definir directrices de confianza, permitiendo el acceso o restricción de determinando usuarios internos o externos a los servicios de la organización. Es importante determinar puntos claves desde el punto de vista físico y lógico que permitan definir comportamientos durante un ataque interno o externo así:

- Si un servicio se encuentra implicado en un ataque interno o externo se debe suspender su acceso rechazando las conexiones entrantes y salientes.

- Definir el tráfico de red permitido y restringirlo o filtrarlo garantizando el cumplimiento de esta restricción.

- Tener claridad sobre los puntos de interconexión de la red interna con Internet. En lo posible centralizarlo para tener salida desde un único punto.

- Implementación de monitorización y auditoria del tráfico interior y exterior.

- Implementar el ocultamiento de información sensible como nombres de los sistemas, tipos de dispositivos de red, cuentas de usuario, SSID, entre otros.

7.5.9.1. Cortafuegos: Es necesario establecer un control físico para controlar puertos y conexiones. Así, el cortafuegos o firewall será una solución tipo hardware que permitirá definir las reglas relacionadas con el flujo de datos desde y hacia determinados puertos en clientes y servidores.

- El equipo debe garantizar disponibilidad total para las actividades diarias de la empresa y ser fuente de continuidad en caso de que ocurra algún tipo de fallo en sus componentes físicos o lógicos.

- Se deberá definir de acuerdo a las necesidades de la organización reglas referentes al flujo de datos que determinen las acciones a tomar: bloquear, permitir e ignorar.

- El tráfico anormal debe ser bloqueado por el Firewall para evitar que existan afectaciones en la seguridad de la red informática organizacional.

- Se debe controlar desde el cortafuego el máximo número de conexiones establecidas desde determinado origen bloqueándolas con el fin de hacer frente a ataques de denegación de servicio

- Se debe controlar el tráfico saliente para evitar que se trate de enviar información hacia el exterior para aplicaciones que no se encuentran autorizado para ello.

7.5.9.2. Conectividad a Internet: El servicio de Internet será proporcionado con el único objetivo de proporcionar un apoyo a las actividades laborales. Su uso debe ser responsable y coherente con lo establecido en las normas del presente documento.

- Está prohibido el acceso directo a servicios de Internet directamente, mediante modem externo o conexiones móviles.

- Está prohibida la configuración de proxys ajenos a la empresa para navegar en Internet.

- La transferencia de información desde o hacia Internet debe realizarse únicamente en el caso de relacionarse con actividades laborales.

7.5.9.3. Red Inalámbrica (WIFI)

- La red inalámbrica se restringe únicamente para personal administrativo de la empresa. Las demás dependencias cuentan con acceso a Internet mediante medios de transmisión cableado.

- Se debe registrar cada uno de los equipos autorizados para hacer uso de la red inalámbrica a través de su dirección MAC.

- Para la conexión a la red inalámbrica se utilizará autenticación segura WPA2. Asimismo, las contraseñas de acceso serán de cambio trimestral.

- Los intentos de conexión hacia la red inalámbrica desde equipos diferentes a la dependencia autorizada para ello serán penalizados según el reglamento interno de la empresa.

- No se debe realizar sniffing a la red inalámbrica sin autorización. Los responsables tendrán implicaciones sujetas al reglamento interno y se aplicarán las leyes vigentes de delitos informáticos a nivel nacional.

- La red inalámbrica de la empresa hará uso del estándar IEEE 802.11b/g/n, por lo cual el hardware de los clientes que establecerán conexión debe estar certificado para ello.

- Dado el tamaño de la red empresarial se dará soporte únicamente para el protocolo TCP/IPV.4.

- En caso de presentarse problemas de rendimiento de la red en las diferentes dependencias de la empresa; se limitará el ancho de banda equitativamente para asegurar su correcto desempeño.

7.6. FORMULACIÓN DE PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA

Los procedimientos de seguridad informática permiten definir cómo se va a materializar lo especificado en las políticas, es decir de qué manera se protegerán los activos de información de la organización.

Notificación de Incidente de Seguridad: Los empleados de CJT&T Ingeniería de Software que detecte un inconveniente en la Seguridad de la organización deberá seguir este procedimiento para notificarlo a la gerencia:

- Recopilar la mayor cantidad de información y evidencia con respecto al incidente detectado.
- Verificar la conectividad a Internet de la red interna de la organización.
- Si existe acceso a Internet, se notifica de manera inmediata a la gerencia sobre el incidente de seguridad utilizando únicamente el servicio de correo empresarial, adjuntando los soportes correspondientes.
- En caso de que el servicio de Internet no se encontrara disponible, el empleado hace comunicación verbal y / o escrita sobre el incidente. La gerencia le proporciona una unidad de almacenamiento para protegerlas evidencias digitales en caso de que estas existan.

Asignación, reasignación y retiro de recursos informáticos: Posterior a la vinculación y cese del puesto de trabajo de un empleado de la organización se deben realizar tareas específicas con respecto a la asignación de recursos informáticos que le permitan ejercer sus funciones. Por tanto, se recomienda seguir los siguientes procedimientos:

Asignación de recursos

- Una vez se tiene plena claridad sobre las funciones a ejercer por parte del empleado que se integra a la organización, se procede a asignarle un equipo informático.
- Se actualiza la hoja de vida del equipo indicando el nuevo responsable.
- Se realiza un inventario de los componentes de hardware y software entregados.
- Se verifica el estado de la máquina.
- Se indica al nuevo empleado sus responsabilidades con respecto a los activos de información de la organización.

Retiro de recursos

- El empleado realiza la entrega de su antiguo equipo.
- Se verifica el estado del equipo por parte del personal del área de TI.
- Si el equipo se encuentra en buen estado se procede a guardarlo de manera adecuada en el almacén de la organización. Si, por el contrario, se encontraran fallos relacionados con manipulación inadecuada del equipo, el empleado deberá hacerse responsable de los costos que impliquen las reparaciones.
- Se registran los eventos en la hoja de vida del equipo antiguo.

Reasignación de recursos

- Si el empleado por alguna razón es reasignado y sus funciones cambian y además, estas funciones requieren de equipos con diferentes características, se evaluará en razón del cargo las necesidades con respecto a hardware y software.
- Se sigue el procedimiento de **"Retiro de recursos".**
- Se sigue el procedimiento de **"Asignación de recursos"**.

Alta y baja de usuarios: Los sistemas de información o servicios que requieran de la administración de credenciales de acceso deberán seguir el siguiente procedimiento de alta y baja de usuarios. Éste aplica para todos los empleados de la organización.

Alta de usuarios

- El empleado comunica al área de TI el sistema para el cual requiere realizar el registro de usuario.
- El área de TI determina si de acuerdo a las funciones desempeñadas, el empleado se encuentra autorizado para obtener una cuenta en el sistema solicitado.
- Si está autorizado, el empleado deberá proporcionar sus datos personales para efectuar el registro.
- De acuerdo a sus funciones, se asigna determinado perfil o rol a la cuenta.
- Las credenciales de acceso de la nueva cuenta serán entregadas mediante el correo electrónico empresarial. En caso de tratarse del alta de un usuario en el servicio de correo, se entregarán los datos al correo personal del empleado.
- El área de TI, almacena un registro en su sistema de gestión de cuentas de usuario.
- Los mensajes de correo electrónico con las credenciales de acceso deberán borrarse en un periodo no mayor a 7 días por motivos de seguridad.
- Posterior al primer uso, el usuario deberá cambiar la contraseña de la cuenta asignada, siguiendo la política de contraseñas presente en este documento.

Baja de usuarios

- Posiblemente por cese de trabajo del empleado se requiera dar de baja las cuentas de usuario.
- Se realiza una consulta en el sistema de gestión de cuentas de usuario de acuerdo a la información personal del empleado.
- Se procede a inactivar todas las cuentas asignadas al empleado por un periodo de 7 días.

- Se confirma la baja definitiva y se procede a eliminar toda la información de las cuentas del empleado.

Respaldo de Datos y Aplicaciones: Establecer medios de respaldo es fundamental para garantizar la integridad y disponibilidad de los sistemas ante cualquier posible situación crítica que pudiera ocurrir. Así, a continuación, se definen aquellas actividades necesarias para velar por que esto ocurra:

Respaldo de Base de Datos: De manera semanal se seguirá el siguiente procedimiento de respaldo.

- Se utiliza la herramienta de administración de base de datos según el SGBD para facilitar la tarea de respaldo.
    - SQL Server: SQL Management Studio.
    - Oracle: Toad for Oracle.
    - MySQL: Toad for MySQL
    - Administración Web: Webadmin.
- Se realiza la copia del archivo de respaldo generado en el disco duro externo.
- Se realiza la copia del archivo de respaldo generado en el disco óptico.
- Se marca el disco óptico de acuerdo a la semana que aplique el respaldo con el siguiente formato: (B. IN: MM/DD/YY – FN: MM/DD/YY).
- Se registra el éxito del proceso en el formato físico o lógico de copias de seguridad.
- Se almacena el disco óptico en una caja fuerte para evitar que personal no autorizado pueda tener acceso a las copias de seguridad.
- Se registra el proceso de archivo de la nueva copia de seguridad en el formato de entradas y salidas de la caja fuerte.

Respaldo de Sistema Operativo y Aplicaciones

- El empleado reporta al área de TI que existen inconvenientes con su equipo de cómputo.
- El área de TI designa un encargado para formatear el equipo. Si es necesario se realiza formato de bajo nivel.
- Se instalan las aplicaciones que sean necesarias para las funciones del empleado.
- Se realiza una imagen de respaldo del disco duro, se sugiere el uso de Norton Ghost o Acronis para realizar esta tarea.
- Se registra este proceso en la hoja de vida del equipo.

Discos Duros Espejo

- Verificar la incorporación de una controladora RAID en la placa base del servidor objetivo del mirroring.
- Instalar un disco duro con la misma capacidad que el que se pretende respaldar.
- Activar la controladora RAID de la placa base a través de la BIOS.
- Comprobar la detección y configuración de los dos discos duros.
- Se accede a la configuración de la controladora RAID y se selecciona la opción “Create Array” o “Define LD” indicando los discos duros relacionados y habilitando el modo RAID 1.

Instalación de Software en Equipos de Cómputo: Los empleados de la organización podrían requerir instalar Software en sus equipos para suplir ciertas necesidades. Sin embargo, es necesario que para acometer esta meta se sigan los pasos descritos a continuación:

- Identificar el tipo de Software a instalar.
- Notificar al área de TI los datos referentes al Software por correo electrónico o mensajería instantánea.
- En caso de ser Software propietario y que la empresa no cuente con las licencias de uso, se procederá a evaluar la pertinencia de adquisición de dichas licencias.
- El área de TI determina si autoriza o no la instalación del Software.
- Un delegado del área se dirige hacia el equipo asignado al empleado e ingresa con cuenta de administrador. Posterior a esto ejecuta los archivos previamente vacunados e instala la aplicación.

Registro de acceso: En el caso de acceso sobre áreas que tienen restricciones debido a que los activos ahí localizados son sensibles, se debe llevar un registro detallado del ingreso y salida de personas sobre dicho espacio así:

- Se solicita autorización para el ingreso al área restringida a la gerencia.
- En caso de ser otorgada, se asigna una persona que supervise las actividades del solicitante.
- Al ingresar al recinto, el supervisor registrará la entrada en el formato de acceso donde consignará los datos personales del solicitante.
- En el caso de que la intervención del solicitante altere de alguna manera los equipos del recinto, se debe registrar las afectaciones en el formato de hoja de vida.
- Al finalizar la actividad, se realiza la salida del recinto, se registra la salida en el formato de acceso.
- El supervisor procede a cerrar el cuarto restringido con llave y las retorna a la gerencia.

Registro de entradas y salidas: Cuando un activo cambia de localización en la organización, esta actividad debe ser registrada. Para esto, se realiza lo siguiente:

- El empleado o contratista solicita la autorización para al ingreso, relocalización o salida de un activo a la gerencia verbalmente o por notificación escrita o digital.
- La gerencia remite respuesta sobre autorización o negación de la solicitud.
- En caso de estar autorizado el empleado o contratista registra el tipo de acción a realizar en el formato de entradas y salidas.
- En caso de ser una entrada, se registra la acción, el personal implicado, la localización del activo y la fecha en que se realiza el movimiento.
- En caso de ser una relocalización, se registra la salida en el formato de entradas y salidas de la ubicación actual especificando el personal implicado, localización del activo y fecha del movimiento. A continuación, se registra la entrada del activo en la nueva localización.
- En caso de ser una salida, se registra la acción ingresando el personal implicado y la fecha de salida del activo en el respectivo formato. Es de anotar que la salida de un activo de la organización no es definitiva y que un periodo mayor a 1 día deberá estar soportado por una autorización digital o escrita por parte de la gerencia.

Mantenimiento de equipos: Según las políticas de seguridad para los equipos de hardware se debe realizar periódicamente procesos de mantenimiento preventivo y correctivo. A continuación, el proceso que se debe seguir.

- Antes de realizar el mantenimiento respalda la información confidencial y se elimina para evitar afectaciones sobre esta.
- El personal encargado del mantenimiento solicita o trae consigo el equipo adecuado para realizar el mantenimiento.
- Se hace un recuento de hallazgos en el equipo. Toda actividad se registra en su hoja de vida.
- Al finalizar y en caso de ser necesario se restaura la información respaldada.

Inventario de activos: Se mantiene un inventario actualizado de los activos de información de la organización. Este procedimiento aplica cuando se adquiere, asigna o audita un activo.

- Al adquirir un activo en la organización, inmediatamente se debe generar su hoja de vida y registrar sus características, configuración y en caso de tratarse de un equipo de cómputo listar el Software instalado.
- Al asignar un activo a un empleado, se confronta la información en su hoja de vida para verificar sus características, configuración y Software instalado en caso de que esto aplique. Si la información no coincide, ésta es actualizada y se

procede con la entrega de activo al empleado siguiendo el procedimiento estipulado en este documento.

- Al auditar un activo asignado a un empleado, se confronta la información que se encuentra en su hoja de vida con respecto a características, configuración y Software instalado en caso de que sea aplicable. En caso de que la información no coincida, el empleado debe justificar la razón de la inconsistencia. Mientras la inconsistencia se aclara el activo es retirado del empleado para seguir verificando su integridad. Si la situación se aclara se actualiza la hoja de vida del equipo, en caso contrario el empleado deberá acarrear costos por componentes faltantes, reconfigurar el equipo o desinstalar Software no autorizado.

Administración de la configuración de los sistemas: Tomando como base el inventario de activos existe un punto crítico a tener en cuenta y es la configuración de los sistemas de información. Se debe tener en cuenta que situaciones como configuraciones por defecto o malas prácticas pueden exponer a la organización a vulnerabilidades críticas que podrían afectar la seguridad de la infraestructura tecnológica de la organización. Es por esto que es muy importante tener en cuenta los siguientes puntos:

- Cada equipo perteneciente a la organización, una vez adquirido deberá tener en cuenta la restricción de recursos y aplicaciones en su uso para su asignación al personal.
- Los equipos servidores debido a su carácter especial deberán ser más estrictos en su configuración y se deben establecer reglas de tráfico de entrada y salida para sus puertos con el fin de evitar intrusiones inesperadas a nivel interno y externo.
- Las configuraciones de los equipos serán almacenadas y categorizadas en el disco duro externo de la organización de acuerdo al tipo de equipo y su dirección IP asignada. En estos directorios se encontrarán archivos nombrados teniendo en cuenta los siguientes criterios o formato: “Nombre_ Aplicación_Fecha”.
- En caso de cambios en la configuración, esta será revisada por el área de TI y en caso de ser aprobada se actualizará el archivo de configuración de determinada aplicación conservando el archivo antiguo.

Procedimiento de Soporte: Ante la gran necesidad que existe en las organizaciones sobre personal de soporte que pueda colaborar en la solución de problemas tecnológicos, para el reporte y atención de una solicitud se debe optar por el siguiente proceso.

- El empleado realiza la solicitud de soporte a través de correo electrónico empresarial.

- La solicitud es asignada al personal del área de TI encargado de las labores de soporte. Se identifica la gravedad de la solicitud y se asigna un tiempo de atención estimado.
- Se realiza la confirmación de recepción, confirmación y asignación de responsabilidad de la solicitud vía correo electrónico. Asimismo, se solicita autorización para acceder a los recursos de manera física o remota.
- Se atiende la solicitud en los tiempos pactados y se registran los hallazgos, así como las correcciones realizadas en caso de aplicar en la hoja de vida del equipo.
- Si el tiempo pactado no es suficiente para atender la solicitud y no existen más solicitudes se continúa hasta solucionar el inconveniente. En caso de existir solicitudes, se programa una nueva sesión de mutuo acuerdo con el empleado.

Escaneo de virus: Como parte esencial de un proceso preventivo y correctivo, el personal de TI encargado de los servidores debe optar por adquirir un producto antivirus con consola administrable para toda la red, con lo cual se podrá realizar escaneos y actualizaciones masivas. El proceso a seguir será:

- Acceder a la consola de administración de la herramienta antivirus.
- Actualizar la base de datos de virus.
- Forzar la actualización de todos los productos antivirus clientes instalados en la red.
- Forzar el escaneo masivo de los equipos en la red.
- Detectar algún hallazgo en los escaneos.
- Mitigar las amenazas.
- Registrar los hallazgos en la hoja de vida del equipo afectado.

8. INVESTIGADORES Y COLABORADORES

8.1. Proponente Primero

Refiriendose a la persona que se encuentra a cargo del desarrollo del proyecto:

Miguel Angel López Parra, Ingeniero de Sistemas graduado en la Universidad Nacional Abierta y a Distancia – UNAD, estudiante de Especialización en Seguridad Informática con 2 años de experiencia en Desarrollo Web y Mantenimiento de bases de datos en empresas privadas.

8.2. Proponentes Secundarios

Todas aquellas personas que intervienen de manera directa en el desarrollo del presente proyecto:

- **Tutores:**
  - Ing. Juan Jose Cruz.
  - Ing. Salomón González.
  - Ing. Alexander Larrahondo.

- **CJT&T Ingeniería de Software:**
  - Juan Carlos Torres, Gerente General, socio y fundador en CJT&T Ingeniería de Software, Fabrique y @T&T Comunicaciones, Ingeniero de Sistemas ICESI, Especialista en Alta Gerencia, Docente Universitario.
  - Miguel Tovar, Gerente de Fábrica CJT&T Ingeniería de Software. Ingeniero de Sistemas Universidad Mariana, Especialista en Gerencia de Proyectos Universidad del Rosario. Docente Universitario.

9. RECURSOS DISPONIBLES

9.1. ESTUDIO TÉCNICO

9.1.1. Localización del Proyecto: Zona urbana de la Ciudad de Pasto en el Sector Central Comuna 1, con acceso adecuado a transporte, infraestructura con respecto a servicios públicos y mayor seguridad. El punto estratégico para el desarrollo del Proyecto será la UNAD CEAD Pasto, en la cual se cuenta con todos los requerimientos anteriormente descritos, además del apoyo tutorial presencial y virtual ante posibles inquietudes que se puedan presentar para ir abordando las temáticas de una manera más efectiva.

9.1.2. Necesidades de Maquinaria y Equipo

Tabla 21. Necesidades de Maquinaria y Equipo del Proyecto

Equipo	Especificación Técnica	Cantidad
Equipo Portátil	**Procesador** Intel Core > i3 Cuarta Generación **Memoria** > 4 GB DDR3 1800 Mhz **Almacenamiento** > SATA III 500 GB **Conectividad** Tarjeta Ethernet e Inalámbrica	1
Impresora	**HP LaserJet P1102w**	1
Licenciamiento de Software	**Sistemas Operativos** Windows 7 Ultimate	1
	Ofimática Office 2010 Profesional Plus	1
Mobiliario	Silla Ergonómica	1
	Escritorio	1
Fuente: El Autor		

9.1.3. Necesidades de recurso humano: Se requiere de Ingeniero de Sistemas, con capacitación en Seguridad Informática, para la investigación y aplicación de las diferentes pruebas que sean requeridas la correcta aplicación del Pentesting y posterior formulación de una Política de Seguridad Informática.

9.2. ESTUDIO FINANCIERO

9.2.1. Inversiones: Se requiere de la inversión en los siguientes activos tangibles como bienes necesarios para el funcionamiento adecuado del proyecto:

Tabla 22. Inversión en Maquinaria y Equipo de Producción

Detalle	Cantidad	Costo Unitario	Costo Total
Equipos de Cómputo	1	1.200.000	1.200.000
Impresora	1	230.000	230.000
Licencia de Software S.O.	1	70.000	70.000
Licencia de Software Office	1	300.000	300.000
		Total	1.800.000
Fuente: El autor			

Tabla 23. Inversión en muebles, enseres y equipos de administración

Detalle	Cantidad	Costo Unitario	Costo Total
Escritorio	1	350.000	350.000
Silla Ergonómica	1	175.000	175.000
		Total	525.000
Fuente: El autor			

Por tanto, de acuerdo a los datos consignados anteriormente, se determina la inversión fija del proyecto a través de la tabla que se encuentra a continuación:

Tabla 24. Inversión Fija

Conceptos	Costo
Activos Fijos Tangibles	**Costo Total**
Maquinaria y Equipo	1.800.000
Muebles y Equipo de Oficina	525.000
Subtotal	2.325.000
TOTAL INVERSIÓN FIJA	2.325.000
Fuente: El autor	

9.3. COSTOS

9.3.1. Costos de Producción

9.3.1.1. Costo de Mano de Obra: La mano de obra directa e indirecta se debe analizar de acuerdo al personal que está implicado en el desarrollo del Producto de Proyecto definiendo el monto de la remuneración.

Tabla 25. Costo de Mano de Obra

Cargo	Valor por Hora	Remuneración diaria (8 horas)	Remuneración semanal	Remuneración mensual	Remuneración Total Proyecto
Ingeniero de Sistemas	15.000	120.000	600.000	2.400.000	9.600.000
				Subtotal	9.600.000
Fuente: El autor					

9.3.1.2. Costos de Materiales: Se tienen en cuenta materiales directos e indirectos que el proyecto requiere para garantizar su ejecución adecuada. Para esto, se ha estipulado que es necesario el uso de materiales de papelería que facilitarían diferentes tareas cotidianas.

Tabla 26. Costos de Materiales

Material	Unidad de Medida	Cantidad	Costo Unitario	Total
Papel	Resma	2	8.900	17.800
Lápiz	Caja	1	2.000	2.000
Lapicero	Caja	1	3.500	3.500
Papel	Resma	1	8.500	8.500
			Total	31.800
Fuente: El autor				

9.3.2. Costo de servicios: Se refiere a aquellos servicios que son necesarios para garantizar la ejecución del proyecto.

Tabla 27. Costos de Servicios

Servicio	Unidad de Medida	Cantidad	Costo Unitario	Total
Internet	Cargo fijo	4	80.000	320.000
			Total	320.000
Fuente: El autor				

Así, de acuerdo a todo el análisis financiero se obtiene la siguiente tabla que clasifica cada costo y gasto de acuerdo a la naturaleza de su aplicación durante el proyecto:

Tabla 28. Distribución de Costos

Costo	Costo Fijo	Costo Variable
Costo de Producción		
Mano de obra directa		9.600.000
Materiales Indirectos		31.800
Servicios		320.000
Subtotal		9.951.800
TOTAL		9.951.800
COSTOS TOTALES		9.951.800
Fuente: El autor		

9.4. RECURSOS INSTITUCIONALES Y HUMANOS

Se requiere de Personal especializado y capacitado que brinde asesoría y apoyo durante la ejecución de todas las actividades que comprenda el proyecto, para esto se acudirá al talento humano correspondiente a Estudiantes y Docentes de la Universidad Nacional Abierta y a Distancia – UNAD en su Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI).

Tutores:

- Ing. Juan Jose Cruz.
- Ing. Salomón González.
- Ing. Alexander Larrahondo.

Estudiante:

- Ing. Miguel López

En lo referente a Recursos Institucionales, asumiendo las diferentes facilidades en materia de implementos y servicios que se ofrecen a través de la Universidad, se pretende utilizar:

- Material de Información a través de la Biblioteca Institucional Física y Virtual.
- Computadores en las Aulas de Informática.
- Servicio de Internet disponible para Estudiantes.

10. RESULTADOS E IMPACTO ESPERADOS

10.1. RESULTADOS

Resultado 1: Resultados de la fase de evaluación

Como se especificó en la fase de evaluación de las pruebas, se hizo uso de dos escaneres: Nessus y OpenVAS, con el objetivo de lograr detectar las vulnerabilidades de los equipos que integran la red de la organización. Así, se obtuvieron los siguientes resultados:

Tabla 29. Resumen severidad en vulnerabilidades encontradas

Severidad	Nessus	OpenVAS	Total	%
Crítica	7	0	7	2.66
Alta	1	13	14	5.32
Media	146	72	218	82.89
Baja	24	0	24	9.13
TOTAL	178	85	263	100
Fuente: El autor				

Lo anterior, permite inferir que, aunque la mayor exposición se hace sobre afectaciones de mediano impacto, existe un alto porcentaje de vulnerabilidades de alto o mayor escala que podría repercutir gravemente sobre los activos de la organización.

Posteriormente, en las tablas 10 y 16 del presente documento se sugieren posibles soluciones de acuerdo a las vulnerabilidades que se detectaron. Así, se puede concluir que las principales causas son las siguientes:

- Defectos de productos de Software
- Carencia sobre control de vulnerabilidades técnicas
- Configuración por defecto en aplicaciones
- Mala configuración de aplicaciones
- Carencia de controles criptográficos

De la anterior categorización, se infieren posibles amenazas que deben ser analizadas y controladas y que se detallan previamente en la tabla 20 del presente documento:

Tabla 30. Resumen relación amenaza y controles

Amenaza	Control
Denegación de servicio	Monitorización de recursos para determinar la capacidad de éstos.
Difusión de Software dañino	Instalación de software anti-malware.
	Generación de planes de recuperación y contingencia ante posibles afectaciones a los sistemas.
Errores de mantenimiento y actualización de programas	Reconocimiento de vulnerabilidades técnicas de los programas instalados.
	Gestión de actualizaciones de Software.
Interceptación de información	Políticas, procedimientos y controles para transferencia de información de manera interna y externa.
	Uso de canales seguros para el uso de mensajería electrónica.
	Uso de herramientas criptográficas para la protección de la información sensible.
Manipulación de programas	Gestión y restricciones sobre el software instalado.
	Acceso restringido a código fuente en la organización.
Fuente: El autor	

Estado actual: Existe un documento de políticas y procedimientos de seguridad de la información que no se está acatando en su totalidad o que no tiene en cuenta los puntos anteriormente expuestos.

Resultado 2: Resumen Ejecutivo

Miguel Angel López como parte de su proyecto aplicado para optar por el título de Especialista en Seguridad Informática de la Universidad Abierta y a Distancia ha efectuado un penetration test con el fin de determinar el grado de exposición de la empresa CJT&T Ingeniería de Software ante un ataque informático. Con autorización previa de los Ingenieros Juan Carlos Torres y Miguel Tovar quienes hacen parte de la gerencia de fábrica de software y la gerencia general de la organización se optó por conducir actividades que simulen el modus operandi de un actor malicioso que pretende desencadenar un ataque dirigido hacia la empresa CJT&T. Lo anterior buscar lograr:

- Identificar si un atacante podría penetrar las defensas de la empresa.
- Determinar el impacto de un fallo de seguridad.
- Determinar los riesgos y amenazas a los que se encuentra expuesta la organización.

Se realizaron esfuerzos para identificar y explotar las debilidades a nivel de seguridad que podrían permitir a un atacante interno o externo obtener acceso no autorizado o denegar los servicios teniendo un impacto en las operaciones de la empresa. Los ataques se condujeron tanto hacia los sitios de Internet que la organización proporcionó como en la red de la empresa basándose sobre la Metodología Penetration Test Standard (PTES).

Siguiendo una metodología progresiva se programaron múltiples fases para poder determinar el nivel de seguridad de la organización. Para esto, en primer lugar, se recabó sobre la información pública de la empresa a través de Internet y la facilidad para obtener los datos de los equipos presentes en la red de la organización.

Lo anterior arrojó los siguientes resultados:

- La información corporativa es fácilmente encontrada a través de los buscadores más populares, permitiendo determinar NIT de la empresa, teléfonos, correos, cuenta bancaria y datos personales de su representante legal.
- Dos de los tres sitios de la empresa no utilizan protocolos seguros para la navegación del usuario.
- Se identifica poca actividad en redes sociales.
- Existe exposición pública sobre diferentes correos empresariales en la red.

Por otra parte, el análisis de subdominios reveló que existen un servidor de correo y ftp propios de la organización. Además, existe un acceso no seguro al servidor de correos utilizando la URL webmail.cjtytsoftware.com.

Posteriormente, se procedió a identificar los equipos que son parte del segmento de red solicitado 192.168.0.0/24. Así, se tuvo que recabar sobre información de cada uno de ellos y posteriormente efectuar pruebas de vulnerabilidades realizados en diferentes periodos de tiempo y usando dos aplicaciones (Nessus y OpenVAS). Con esto se detectaron un total de 263 vulnerabilidades en todos los equipos de la red las cuales se categorizaron de esta manera:

- **Defectos de productos de Software:** Causadas por defectos en las Aplicaciones que se encuentran instaladas en los equipos.

- **Carencia sobre control de vulnerabilidades técnicas:** Revela falta de gestión sobre defectos de Software, es decir, no existe control sobre las vulnerabilidades de las aplicaciones utilizadas, con lo cual, a pesar de que existan soluciones disponibles estas no son aplicadas de manera oportuna.

- **Configuración por defecto en aplicaciones:** Problemas de seguridad por falta de gestión o conocimiento en la instalación de aplicaciones en las cuales permanecen las configuraciones por defecto.

- **Mala configuración de aplicaciones:** Las aplicaciones son configuradas con ajustes inadecuados o inseguros que amplíen la brecha del atacante.

- **Carencia de controles criptográficos:** No existen controles criptográficos o no son adecuados causando que la información que se transporte en la red empresarial no esté encriptada, se utilicen algoritmos de encriptación inadecuados, se usen opciones obsoletas, entre otros.

El hecho de que existan vulnerabilidades en la infraestructura tecnológica de la organización sin el tratamiento adecuado trae consigo diferentes amenazas que atentan en contra de la disponibilidad, integridad y confidencialidad de la información presente en los sistemas provocando daños y pérdidas sobre los activos de la organización. Así, de acuerdo a los resultados de las pruebas, éstas se pueden resumir de la siguiente manera:

- **Denegación de servicio:** Uno o varios sistemas son comprometidos, denegando la disponibilidad o acceso a éstos para quien necesite de sus recursos.

- **Difusión de software dañino:** Representado por cualquier tipo de malware, ya sea un virus, troyano, keylogger, adware, entre otros. De igual manera, en esta categoría se presentan todos los scripts ejecutados de manera maliciosa aprovechando la falta de validaciones sobra parámetros de entrada/salida de aplicaciones web o móviles. El software dañino puede comprometer el sistema sin el consentimiento del usuario con el fin de obtener información privilegiada, secuestrar el equipo o los datos, denegar uno o varios servicios o simplemente indisponer al usuario.

- **Errores de mantenimiento y actualización de programas:** El hecho de tener aplicaciones desactualizadas trae consigo no solo vulnerabilidades, sino también defectos que representan riesgos en la seguridad y usabilidad. Por lo tanto, es importante, mantener una gestión sobre este tipo de problemas.

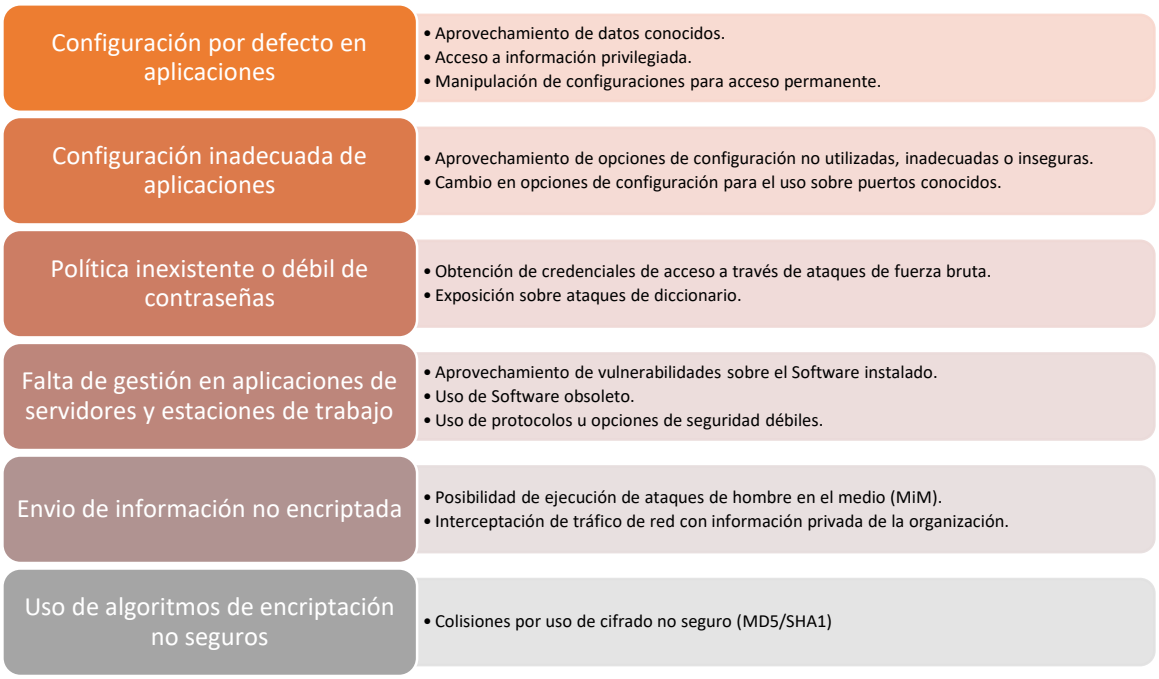
- **Interceptación de información:** Las vulnerabilidades detectadas pueden causar que un atacante sea capaz de interceptar información a través de

software externo que le permita obtener información sensible mediante el análisis del tráfico de red. Asimismo, existe un alto riesgo de inyección de DNS o ARP con el objetivo de hacerse en el medio y obtenerla por su cuenta. Dependiendo del tipo de información las consecuencias podrían partir desde un desprestigio hacia la empresa y podrían llegar hacia el uso de credenciales de acceso privilegiado para la autenticación exitosa en servicios de correo, mensajería, redes sociales, hosting, entre otros. Lo anterior, también podría hacer posible el escalamiento en los sistemas internos de la empresa para obtener control total sobre uno o varios equipos que pertenezcan a la red informática.

- **Vulnerabilidades de programas:** Ante la gran cantidad de programas instalados en los equipos de la red organizacional, existe una gran posibilidad de que muchos de ellos no fueran previamente autorizados por la gerencia. En este sentido, no se tiene certeza sobre el nivel de seguridad, estabilidad y confiabilidad del Software instalado en los sistemas.

Así, partiendo del hecho de que existen amenazas que pueden poner en riesgo las operaciones normales de la organización, éstas se pueden materializar teniendo en cuenta los aspectos recopilados a continuación:

Figura 75. Riesgos de ataque informático



Fuente: El autor

Ahora, es de señalar que se lograron verificar las siguientes situaciones:

- Existen aplicaciones con configuraciones por defecto como IIS que despliegan la pantalla de bienvenida indicando el número de versión que se encuentra ejecutando el servidor.

- Se detectaron aplicaciones con archivos de instalación almacenados en el sistema. Tal es el caso de Apache Tomcat.

- Existen aplicaciones web desplegadas en el servidor IIS del equipo central en el cual no se han establecido las configuraciones necesarias para bloquear la afectación sobre vulnerabilidades que permiten la ejecución de código remoto. Esto implica facilidades para realizar una denegación de servicio.

- Se corrobora la falta de validación sobre entrada de datos en aplicaciones instaladas como Agora CGI o 12Planet Chat Server que podrían ser riesgosas para efectuar ataques de cross site scripting(XSS). Estos ataques podrían exponer información privada de la sesión del usuario sin su consentimiento.

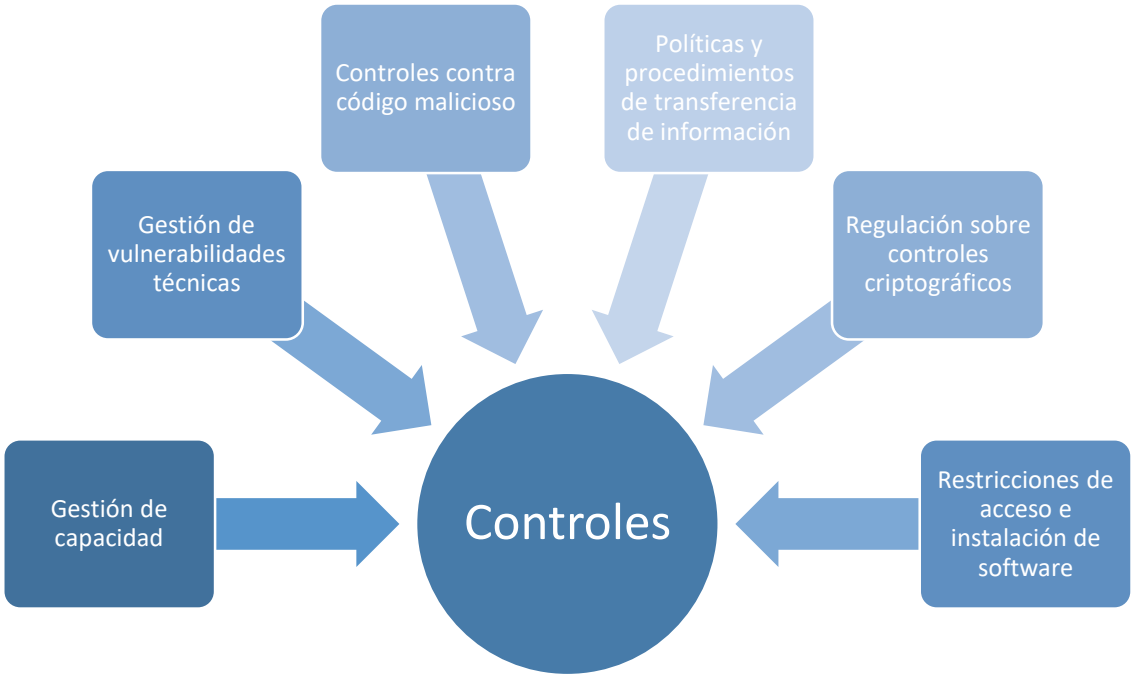
- Se obtuvo acceso sobre los recursos de red de varios equipos debido a que no contaban con un proceso de autenticación. Este puede ser el medio de entrada para un atacante, debido a que se expone información que posiblemente pueda ser relevante hacia el público que sin los debidos cuidados podría ser modificada o eliminada.

- Existe un alto riesgo sobre un ataque de fuerza bruta o de diccionaro para obtener acceso a las bases de datos empresariales debido a que no se cuenta con las últimas versiones de Software instaladas, con lo cual a través del uso de Scripts externos se puede forzar mensajes de error durante la autenticación de un usuario.

- Existe un alto riesgo de ataques de hombre en el medio, con los cuales un atacante se podría ubicar en medio del router y otro equipo que sea el blanco de ataque, para interceptar el tráfico de red y obtener información confidencial.

Así, tomando un control como aquella implementación sobre medidas de seguridad en razón de la mitigación de los riesgos que implican las amenazas a los activos de información, se proponen las siguientes soluciones:

Figura 76. Controles de seguridad



Fuente: El autor

- **Gestión de capacidad:** Es necesario evaluar si la actual capacidad de los equipos garantiza un rendimiento óptimo en razón a la ejecución de una carga habitual de procesos ejecutados de manera simultanea. Asimismo, se deberán estimar proyecciones de tiempo de vida o en lo que concierne a mejoras a nivel de Software/Hardware para un mejor aprovechamiento de los recursos.

- **Gestión de las vulnerabilidades técnicas:** Se debe dar seguimiento sobre las vulnerabilidades de las aplicaciones instaladas en el sistema con el fin de dar tratamiento adecuado a las mismas.

- **Controles contra códigos maliciosos:** Se debe garantizar la instalación de las herramientas necesarias de Software/Hardware para la protección de los equipos de cómputo ante la amenaza de ejecución de código malicioso. En este apartado, también se debe tener en cuenta que la concientización de los usuarios sobre las amenazas externas y las restricciones que se realicen en cuanto a sitios autorizados para la navegación.

- **Políticas y procedimientos de transferencia de información:** Se deben formular políticas y procedimientos para el control de las amenazas presentes en la tranferencia de información física y lógica en un entorno donde puede existir interacción entre usuarios internos y externos debido al continuo uso de mensajería electrónica y transferencia de recursos a través de la red interna.

- **Regulación sobre controles criptográficos:** Para proteger el tráfico de red independiente del protocolo que aplique, se hace necesario implementar políticas sobre el uso de controles criptográficos para garantizar la integridad y confidencialidad de la información.

- **Restricciones de acceso e instalación de Software:** De acuerdo a las políticas y procedimientos que se definan para la organización, se hace necesario restringir los permisos de los usuarios de acuerdo al uso que se le de a los equipos de cómputo limitando a su vez la instalación de software para garantizar que solamente estén instalados aquellos que son de confianza o están autorizados.

Asimismo, se proponen las siguientes acciones relacionadas:

- Seguimiento y verificación sobre capacidad con respecto a características de hardware instalado en los servidores de la organización.

- Instalación de soluciones de seguridad integrales a través de centralización de Software antimalware que cuente con características que faciliten la interacción con todos los equipos de la red corporativa, programando escaneos periódicos sin la necesidad de la interacción del usuario.

- Protección integral sobre servidores de la organización, los cuales al menos deben contar con un antivirus y un firewall instalado. Asimismo, se deberá evaluar la pertinencia de las reglas de entrada y salida del firewall a fin de evitar la intrusión de agentes externos no autorizados.

- Restricción sobre la navegación de sitios no autorizados a través de los distintos equipos de cómputo.

- Formulación sobre políticas y procedimientos para la transferencia de información entre usuarios internos y externos a la red corporativa.

- Revocación sobre altos privilegios en las cuentas de usuario de los equipos de la organización. Únicamente el personal autorizado debe efectuar acciones de instalación de Software o modificaciones en las configuraciones administrativas.

- Restricción sobre los de equipos de cómputo para garantizar que su uso es netamente para actividades laborales.

- Implementación de un inventario de Software para cada uno de los equipos de la red corporativa.

- Comprobación periódica sobre vulnerabilidades técnicas y actualizaciones presentes en el Software instalado para los equipos de la organización.

- Formulación de políticas y procedimientos de respaldo que cubran el almacenamiento sobre la información sensible de manera periódica en el servidor de respaldo.

Resultado 3: Políticas y procedimientos de seguridad acordes a los hallazgos.

Como producto de los resultados encontrados a partir de las pruebas de Pentesting se ha efectuado la formulación de políticas de seguridad informática para la organización CJT&T Ingeniería de Software. Entonces, estas representan el insumo de consulta, socialización e implementación de procedimientos de prevención y solución para situaciones generales y detectadas que expongan los sistemas informáticos. Este contenido se puede encontrar en el punto 7.5 del presente documento.

Asimismo, se realiza la formulación de procedimientos de seguridad que detallan de qué manera se dará cumplimiento a lo establecido en las políticas de seguridad mencionadas anteriormente. Esta temática se trata este punto en el apartado 7.6 del presente documento.

10.2. IMPACTO ESPERADO

El presente proyecto se plantea como el desarrollo de pruebas de Pentesting que permitan el diseño de políticas y procedimientos para la seguridad de la información en la organización. Así, una vez finalizado el desarrollo se proyecta alcanzar el siguiente impacto sobre la empresa:

- Concientizar a la gerencia de la empresa sobre la necesidad de establecer medidas de protección para estar preparados ante un eventual ataque informático.

- Concientizar al personal de la empresa sobre la necesidad de tener conocimientos básicos en materia de seguridad para evitar ser víctimas de las técnicas de los atacantes y además hagan buen uso de los recursos institucionales.

- Posibilitar la creación de un canal de comunicación entre la gerencia y los empleados para trabajar conjuntamente hacia la ejecución de los contenidos presentes en los procedimientos de seguridad de la información a fin de que

éstos se conviertan en la guía diaria para que la ejecución de las tareas cotidianas sea efectuada de manera segura procurando la protección de los activos más importantes para la empresa.

- Minimizar el impacto de un atacante que intenta realizar un ataque informático a la infraestructura tecnológica de la empresa, teniendo como insumo las políticas y procedimiento de seguridad de la información que no solo permiten establecer acciones de prevención, sino también de corrección, mantenimiento, mejora y recuperación.

- Evitar la alteración, pérdida o indisponibilidad de la información debido a la falta de mantenimiento o monitorización en los activos de información.

11. DIVULGACIÓN

Como autor del presente proyecto de grado autorizo a la Universidad Nacional Abierta y a Distancia – UNAD con el fin de que pueda disponer del presente documento para su divulgación en los diferentes formatos: electrónico, digital, en red, Internet y en general por cualquier formato conocido o por conocer.

12. CRONOGRAMA

Actividad	Febrero				Marzo				Abril				Mayo			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. Revisión de Información																
Identificación de fuentes																
Localización física de fuentes																
Consulta de fuentes localizadas																
Recopilación de Información																
Ordenamiento de Información																
2. Propuesta																
Propuesta de presentación																
Trabajo Legal																
3. Recolección de Información																
Empresarial																
Individual																
4. Análisis de vulnerabilidades																
5. Explotación Vulnerabilidades																
6. Post-explotación Vulnerabilidades																
7. Creación de reporte																
8. Desarrollo de Política SI																
Creación																
Revisión																
Aprobación																
9. Formulación Procedimientos SI																

CONCLUSIONES

1. Dado el actual contexto en el cual la Seguridad Informática ha logrado tener un gran protagonismo, el uso de herramientas automatizadas facilita la labor correspondiente a las diferentes fases del Pentesting, sin embargo, éstas no deben sesgar el criterio del experto y este debe acudir hacia la creatividad para plantear diferentes vectores de ataque que permitan revelar los escenarios en los cuáles un atacante podría aprovecharse sobre los diferentes fallos de seguridad que tendría una organización.

2. La identificación de vulnerabilidades permite constatar las debilidades de seguridad a nivel organizacional las cuales se deberán priorizar para dar tratamiento a los riesgos con el fin de fortalecer los mecanismos de protección contra intrusos.

3. El análisis de vulnerabilidades permitió establecer los puntos comunes sobre las posibles causas de estos resultados para evaluar las amenazas con el fin de poder formular los controles adecuados en respuesta a las necesidades de la organización.

4. La fase de explotación es clave y representa la diferencia entre un simple análisis de vulnerabilidades y un Pentesting permitiendo comprobar y establecer el alcance de los hallazgos realizados en fases anteriores.

5. Los procedimientos de seguridad informática permiten que el personal de la organización tenga a su disposición la información necesaria que sea la herramienta para poder proteger de manera efectiva los activos que estén a su alcance y que sean su responsabilidad.

6. Los procedimientos de seguridad informática permiten definir las pautas detalladas sobre la implementación de las políticas siendo claves sobre el modo de actuación del personal detallando que se debería hacer con respecto a procesos específicos claves en la seguridad de la organización.

RECOMENDACIONES

- A fin de establecer un mayor control sobre la interacción de los usuarios con los sistemas operativos y de información, es necesario establecer una gestión de los mismos partiendo desde el principio de mínimo privilegio a fin de facilitar posteriores tareas de administración y auditoria.

- Es necesario seguir una política de contraseñas seguras para los usuarios sobre todos los servicios que se relacionen con su actividad laboral. Esto cubriría principalmente cuentas de correo empresariales, credenciales de acceso en sistemas operativos, TFS, Sharepoint, entre otros. Desde las políticas de seguridad se debe seguir con los criterios establecidos para definir la complejidad adecuada de una contraseña, almacenamiento y los cambios periódicos sobre éstas.

- Se debe establecer un inventario sobre las aplicaciones instaladas en cada uno de los equipos de la organización. Asimismo, se debe establecer cuales son las aplicaciones autorizadas o de confianza. Con lo anterior, se afirma que se debe bloquear cualquier otra aplicación que no esté autorizada y restringir que los usuarios pueden efectuar tareas administrativas.

- Se debe evitar el uso de software obsoleto ya que representa un alto riesgo de seguridad debido a su falta de soporte y a un entorno dinámico que tiene disponible gran cantidad de información para aprovechar cualquier tipo de vulnerabilidad presenta en aplicaciones antiguas.

- Es necesaria la gestión de vulnerabilidades de acuerdo a las aplicaciones instaladas en los equipos. Esta acción se debe realizar de manera periódica evaluando su grado de impacto para facilitar el planteamiento de soluciones oportunas.

- Es conveniente gestionar las actualizaciones de sistemas operativos y aplicaciones. El contar con las versiones más recientes minimiza el riesgo de aprovechamiento sobre fallos de seguridad por parte de un atacante.

- Las aplicaciones de seguridad son un componente que no debe ignorarse en ninguno de los equipos de la organización para contar con la máxima protección sobre los riesgos externos. Así, la instalación y actualización de Software antivirus y el hecho de contar con un firewall a nivel de software o hardware son el punto de partida.

- Es necesario programar capacitaciones al personal en materia de seguridad, exponiendo tanto los principales riesgos a los cuales se está expuesto, los

ataques más comunes y las principales técnicas que los atacantes utilizan para hacerse con información privilegiada. Ahora, también es esencial exponer desde la gerencia las políticas y procedimientos de seguridad para que sean tenidos en cuenta sobre cada acción que los involucra en su quehacer diario.

- Al momento de instalar una aplicación se debe verificar que las configuraciones establecidas no sean de carácter inseguro con el fin de no abrir una brecha de seguridad hacia los atacantes internos o externos. Asimismo, desde esta perspectiva es muy importante revisar las configuraciones finales con el fin de evitar el uso de parámetros que sean inseguros.

- Toda la información sensible que pasa por una red externa debe enviarse encriptada o en su defecto generar hashes desde algoritmos seguros con el fin de evitar que ésta sea alterada y que el receptor tenga en su poder información equivocada.

- Todo recurso en red debe requerir de autenticación para la obtención de acceso.

- Se debe tener especial cuidado con la información corporativa que se encuentra disponible para el público. El hecho de tener expuesta información financiera sensible podría implicar un alto riesgo no solo para la reputación de la empresa sino como un medio de extorsión o amenaza.

BIBLIOGRAFÍA

CÓDIGO VERDE. *Prueba de Penetración (PenTest) [en línea]*. [Consultado el 14 de Marzo de 2015]. Disponible en Internet: <http://codigoverde.com/consultoria-especializada/prueba-de-penetracion-pentest/>

DRAGÓN. *¿Cómo se realiza un Pentest? [en línea]*. [Consultado el 14 de Marzo de 2015]. Disponible en Internet: <http://www.dragonjar.org/como-realizar-un-pentest.xhtml>

NYXBONE. *Pentest [en línea].* [Consultado el 14 de Marzo de 2015]. Disponible en Internet: <http://www.nyxbone.com/pentest.html>

CATOIRA, Fernando. *Penetration Test, ¿en qué consiste? [en línea].* [Consultado el 15 de Marzo de 2015]. Disponible en Internet: <https://hackersenlared.wordpress.com/category/capacitacion/que-es-un-pentest/>

PENETRATION TESTING TOOLS. *Penetration Testing Framework [en línea]*. [Consultado el 17 de Marzo de 2015]. Disponible en Internet: <http://www.pen-tests.com/penetration-testing-framework.html>

HERZOG, Pete. *Open Source Security Testing Methodology Manual (OSSTMM) [en línea]*. [Consultado el 17 de Marzo de 2015]. Disponible en Internet: <http://www.isecom.org/research/osstmm.html>

CEPEDA, Fausto. *Yo esperaba un buen reporte de pentest [en línea]*. [Consultado el 10 de Abril de 2015]. Disponible en Internet: <http://searchdatacenter.techtarget.com/es/opinion/Yo-esperaba-un-buen-reporte-de-pentest>

GROSS, Manuel. Conozca 3 tipos de investigación: *Descriptiva, Exploratoria y Explicativa [en línea]*. [Consultado el 12 de Abril de 2015]. Disponible en Internet: <http://manuelgross.bligoo.com/conozca-3-tipos-de-investigacion-descriptiva-exploratoria-y-explicativa>

CANTILLO, Eleazar y Otros. *Diseño e Implementación de un Sistema de Información para la asignación de citas de consulta externa en las áreas de medicina general, odontología y psicología [en línea]*. [Consultado el 14 de Abril de 2015]. Disponible en Internet: <http://www.konradlorenz.edu.co/images/stories/suma_digital_sistemas/2009_01/eleazar.pdf>

ACOSTA, Ricardo. *Guía para la elaboración de un anteproyecto [en línea].* [Consultado el 16 de Abril de 2015]. Disponible en Internet: <http://blog.utp.edu.co/ricosta/files/2011/08/GUIA-UNIFICADA-ELABORACION-ANTEPROYECTO-DE-INVESTIGACION-V2012.pdf>

BOGOTÁ. UNIVERSIDAD NACIONAL DE COLOMBIA. *Guía para elaboración de políticas de seguridad [en línea]*. [Consultado el 17 de Abril de 2015]. Disponible en Internet: <http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf>

CORDERO, Hernan. *Elaboración de Proyecto de Investigación Cuantitativa [en línea]*. [Consultado el 19 de Abril de 2015]. Disponible en Internet: <http://www.une.edu.pe/dev/investigacion.pdf>

GAMINO, Jonathan. *Proceso de Penetration Testing [en línea].* [Consultado el 22 de Abril de 2015]. Disponible en Internet: <https://www.academia.edu/7168943/1.-_Penetration_testing>

MIERES, Jorge. *Certified Ethical Hacker Review Guide [en línea].* [Consultado el 10 de Mayo de 2015]. Disponible en Internet: <http://www.it-docs.net/ddata/863.pdf>

ESQUIVEL, Mario. *Marco Histórico [en línea].* [Consultado el 12 de Mayo de 2015]. Disponible en Internet: <https://sites.google.com/site/scesquivelsuazomarialuisa/7-conclusiones/5-2-marco-historico>

RUSSO, Hector. *La historia del hacking: hechos y hackers más notorios [en línea].* [Consultado el 14 de Mayo de 2015]. Disponible en Internet: <http://geeksroom.com/2014/05/la-historia-del-hacking-hechos-y-hackers-mas-notorios/85638/>

HERNANDEZ, Jeisson. *Marco teórico [en línea].* [Consultado el 15 de Mayo de 2015]. Disponible en Internet: <http://proyectoseguridadcemv.wikispaces.com/file/view/marco_teorico.pdf>

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE. *Coordinación trabajo de grado Protocolo Pasantía Comunitaria como Opción de Grado [en línea].* [Consultado el 16 de Mayo de 2015]. Disponible en Internet: <http://www.uao.edu.co/sites/default/files/PASANTIACOMUNITARIA.DOC>

FERRERIRA DA SILVA, Rejane. *Introducción a las técnicas cualitativas de investigación aplicadas en salud [en línea].* [Consultado el 20 de Mayo de 2015]. Disponible en Internet:

<https://books.google.com.co/books?id=o2n57QYwMDIC&pg=PA74&lpg=PA74&dq=analisis+de+documentos+tecnica+de+investigacion&source=bl&ots=mChvJlCz3_&sig=MzbBrQiQf6VHTF6whwBKqUaQmYA&hl=es-419&sa=X&ei=bvhfVZS9MNCJNrvFgKgI&ved=0CEEQ6AEwCDgK#v=onepage&q=analisis%20de%20documentos%20tecnica%20de%20investigacion&f=false>

CONGRESO DE COLOMBIA. *Ley 1273 de 2009 [en línea].* [Consultado el 14 de Marzo de 2016]. Disponible en Internet: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>

CONGRESO DE COLOMBIA. Decreto 1377 de 2013 [en línea]. [Consultado el 14 de Marzo de 2016]. Disponible en Internet: < http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646#0>

DEFINICIONABC. Definición de Hacker [en línea]. [Consultado el 15 de Marzo de 2016]. Disponible en Internet:< http://www.definicionabc.com/tecnologia/hacker-2.php>

SEGURIDADPC.NET. Concepto de Hackers [en línea]. [Consultado el 15 de Marzo de 2016]. Disponible en Internet: <http://www.seguridadpc.net/hackers.htm>

EMMANUEL. Hacker, Cracker, Lammer, Newbie [en línea]. [Consultado el 15 de Marzo de 2016]. Disponible en Internet: < http://planethacked.blogspot.com.co/2009/11/hacker-cracker-lammer-newbie.html>

TECNOPRIMERO. Hacker, Cracker, Lamer, Defacer, ScriptKiddie, Newbie, Phreaker [en línea]. [Consultado el 15 de Marzo de 2016]. Disponible en Internet: < http://tecnoprimero1234.blogspot.com.co/p/hacker-cracker-lamer-defacer.html>

PENTEST-STANDARD. PTES Technical Guidelines [en línea]. [Consultado el 18 de Marzo de 2016]. Disponible en Internet: < http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines#Blind_Files>

RAYME, Ruben. Gestión de seguridad de la información y los servicios críticos de las universidades: un estudio de tres casos en Lima Metropolitana [en línea]. [Consultado el 19 de Marzo de 2016]. Disponible en Internet: <http://cybertesis.unmsm.edu.pe/xmlui/bitstream/handle/cybertesis/428/Rayme_sr.pdf?sequence=1>

AIRCRACK-NG. Introduction [en línea]. [Consultado el 19 de Marzo de 2016]. Disponible en Internet: <http://www.aircrack-ng.org/doku.php?id=Main&DokuWiki=1dorfvfs70np50eq5ejhfc5j46>

KALI. THC-IPV6 [en línea]. [Consultado el 19 de Marzo de 2016]. Disponible en: <http://tools.kali.org/information-gathering/thc-ipv6>

TUTORIALES BLOGGER. Brutus Password Cracker AET2 [en línea]. [Consultado el 19 de Marzo de 2016]. Disponible en Internet: <http://tutorbgg.blogspot.com.co/2013/12/brutus-password-cracker-aet2.html>

BEYONDTRUST. Retina Community [en línea]. [Consultado el 19 de Marzo de 2016]. Disponible en Internet: <https://info.beyondtrust.com/community.html>

HARVEY, Phil. ExifTool [en línea]. [Consultado el 20 de Marzo de 2016]. Disponible en Internet: <http://www.sno.phy.queensu.ca/~phil/exiftool/>

SECTOOLS. fgdump [en línea]. [Consultado el 20 de Marzo de 2016]. Disponible en Internet: < http://sectools.org/tool/fgdump/>

DragoN. FOCA – Herramienta para análisis de Meta Datos [en línea]. [Consultado el 20 de Marzo de 2016]. Disponible en Internet: <http://www.dragonjar.org/foca-herramienta-para-analisis-meta-datos.xhtml>

MCAFEE. SiteDigger v3.0 Released 12/01/2009 [en línea]. [Consultado el 20 de Marzo de 2016]. Disponible en Internet: <http://www.mcafee.com/us/downloads/free-tools/sitedigger.aspx>

ANTRAX. SQLi Automatizado con Havij [en línea]. [Consultado el 20 de Marzo de 2016]. Disponible en Internet: <http://www.antrax-labs.org/2012/02/sqli-automatizado-con-havij.html>

PCADVISOR. inSSIDer 4.0 [en línea]. [Consultado el 20 de Marzo de 2016]. Disponible en Internet: <http://www.pcadvisor.co.uk/download/networking-tools/inssider-40-715/>

PATERVA. Maltego [en línea]. [Consultado el 20 de Marzo de 2016]. Disponible en Internet: <https://www.paterva.com/web6/products/maltego.php>

NMAP. Guía de referencia de nmap [en línea]. [Consultado el 21 de Marzo de 2016]. Disponible en: <https://nmap.org/man/es/>

DragoN. p0f – Identificación pasiva del Sistema Operativo [en línea]. [Consultado el 21 de Marzo de 2016]. Disponible en: <http://www.dragonjar.org/p0f-identificacion-pasiva-del-sistema-operativo.xhtml>

PANGOLIN. Pangolin Free 3.2.3 [en línea]. [Consultado el 21 de Marzo de 2016]. Disponible en: <http://pangolin-free.soft32.com/>

KALI. snmpcheck [en línea]. [Consultado el 21 de Marzo de 2016]. Disponible en: <http://tools.kali.org/information-gathering/snmpcheck>

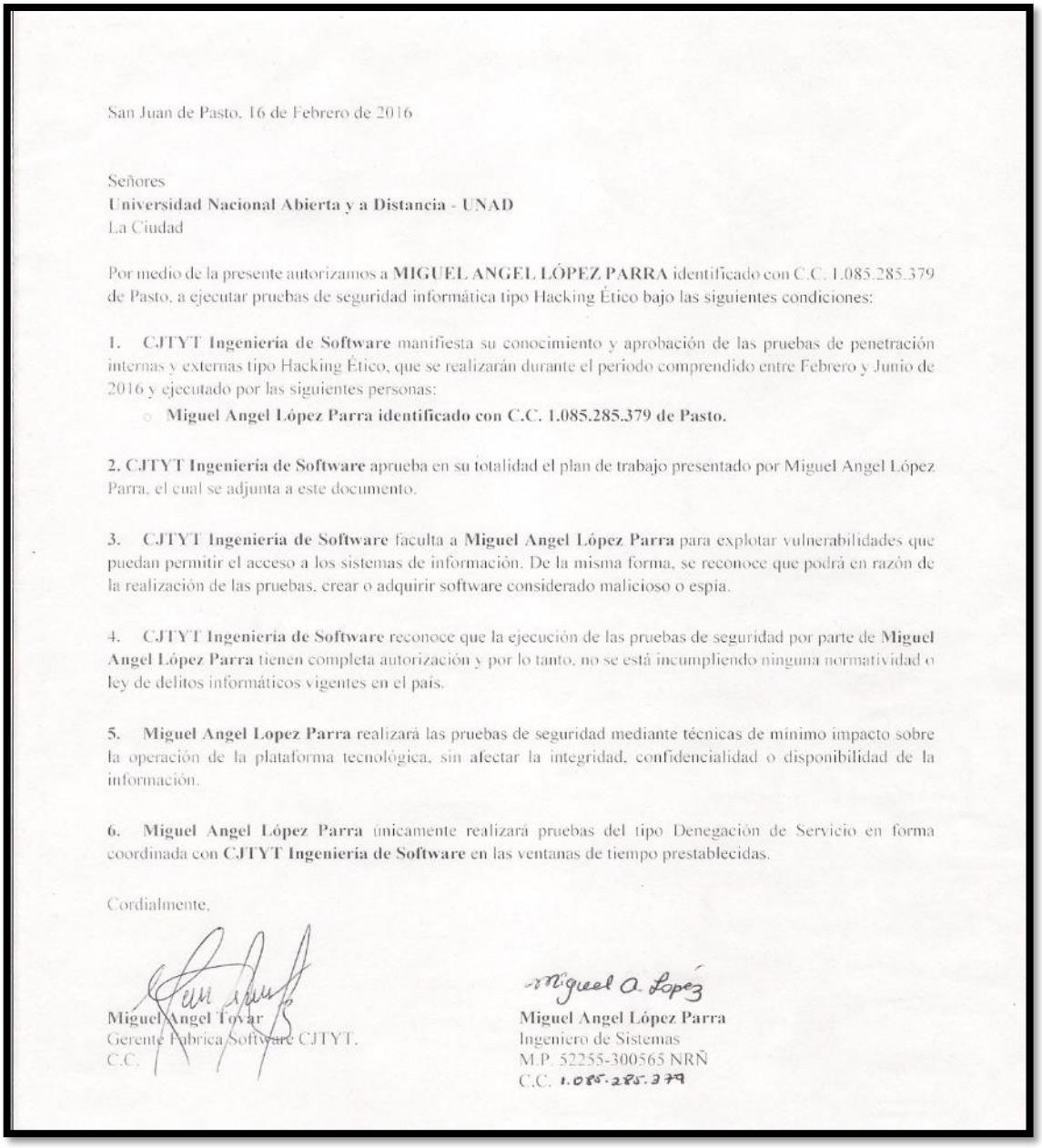
ReYDeS. Ataque Remoto De Contraseñas Utilizando THC-Hydra [en línea]. [Consultado el 21 de Marzo de 2016]. Disponible en: < http://www.reydes.com/d/?q=Ataque_Remoto_de_Contrasenas_utilizando_THC_Hydra>

BENITEZ, Moisés. Gestión Integral. [En línea] [Consultado el 10 de Mayo de 2016]. Disponible en: <http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf>

UNAM. Esquemas de Seguridad Informática [En línea]. [Consultado el 11 de Mayo de 2016]. Disponible en: < http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Procedimientos.php>

ANEXOS

ANEXO A. AUTORIZACIÓN EJECUCIÓN DE PENTESTING



San Juan de Pasto, 16 de Febrero de 2016

Señores
Universidad Nacional Abierta y a Distancia - UNAD
La Ciudad

Por medio de la presente autorizamos a **MIGUEL ANGEL LÓPEZ PARRA** identificado con C.C. 1.085.285.379 de Pasto, a ejecutar pruebas de seguridad informática tipo Hacking Ético bajo las siguientes condiciones:

1. **CJTYT Ingeniería de Software** manifiesta su conocimiento y aprobación de las pruebas de penetración internas y externas tipo Hacking Ético, que se realizarán durante el periodo comprendido entre Febrero y Junio de 2016 y ejecutado por las siguientes personas:
   - **Miguel Angel López Parra identificado con C.C. 1.085.285.379 de Pasto.**

2. **CJTYT Ingeniería de Software** aprueba en su totalidad el plan de trabajo presentado por Miguel Angel López Parra, el cual se adjunta a este documento.

3. **CJTYT Ingeniería de Software** faculta a **Miguel Angel López Parra** para explotar vulnerabilidades que puedan permitir el acceso a los sistemas de información. De la misma forma, se reconoce que podrá en razón de la realización de las pruebas, crear o adquirir software considerado malicioso o espía.

4. **CJTYT Ingeniería de Software** reconoce que la ejecución de las pruebas de seguridad por parte de **Miguel Angel López Parra** tienen completa autorización y por lo tanto, no se está incumpliendo ninguna normatividad o ley de delitos informáticos vigentes en el país.

5. **Miguel Angel Lopez Parra** realizará las pruebas de seguridad mediante técnicas de mínimo impacto sobre la operación de la plataforma tecnológica, sin afectar la integridad, confidencialidad o disponibilidad de la información.

6. **Miguel Angel López Parra** únicamente realizará pruebas del tipo Denegación de Servicio en forma coordinada con **CJTYT Ingeniería de Software** en las ventanas de tiempo prestablecidas.

Cordialmente,

Miguel Angel Tovar
Gerente Fabrica Software CJTYT.
C.C.

Miguel A. López

Miguel Angel López Parra
Ingeniero de Sistemas
M.P. 52255-300565 NRÑ
C.C. 1.085.285.379

Para efectos de verificación de la autorización aquí suscrita se puede comunicar a través de los siguientes medios de contacto:

- Teléfono: 3216437263
- Correo Electrónico: mtovar@cjtytsoftware.com

ANEXO B. RED DE DATOS CJT&T INGENIERÍA DE SOFTWARE (Ver anexo. Archivo PDF Red_datos_CJT&T.pdf)

Red_datos_CJT&T.pdf

ANEXO C. RED DE DATOS CJT&T INGENIERÍA DE SOFTWARE POR PISO
(Ver anexo. Archivo PDF Red_pisos_CJT&T.pdf)

Red_pisos_CJT&T.pdf

ANEXO D. ESCANEO SERVIDOR WEB CJTYTSOFTWARE.COM

```
# Nmap 7.01 scan initiated Tue Apr 12 01:06:27 2016 as: nmap -T5 -v -p 1-65535 -
oA Nmap_FULL_client cjtytsoftware.com
Warning: 67.23.254.6 giving up on port because retransmission cap hit (2).
Nmap scan report for cjtytsoftware.com (67.23.254.6)
Host is up (0.15s latency).
rDNS record for 67.23.254.6: dime180.dizinc.com
Not shown: 63585 filtered ports, 1928 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
26/tcp   open  rsftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
1291/tcp open  seagulllms
2077/tcp open  unknown
2078/tcp open  unknown
2082/tcp open  infowave
2083/tcp open  radsec
2086/tcp open  gnunet
2087/tcp open  eli
2095/tcp open  nbx-ser
2096/tcp open  nbx-dir
3306/tcp open  mysql

Read data files from: /usr/bin/../share/nmap
# Nmap done at Tue Apr 12 01:18:14 2016 -- 1 IP address (1 host up) scanned in
706.74 seconds
```

ANEXO E. BARRIDO DE PING REALIZADO A LA RED 192.168.0.0 EL 12 DE ABRIL

Starting Nmap 7.12 (https://nmap.org) at 2016-04-12 12:40 COT
Nmap scan report for 192.168.0.1
Host is up (0.0034s latency).
MAC Address: 00:1B:11:CF:1E:C2 (D-Link)
Nmap scan report for 192.168.0.86
Host is up (0.00017s latency).
MAC Address: 00:26:90:62:68:AC (I DO IT)
Nmap scan report for 192.168.0.100
Host is up (0.00060s latency).
MAC Address: 5C:F3:FC:2B:05:90 (IBM)
Nmap scan report for 192.168.0.109
Host is up (0.028s latency).
MAC Address: C8:F7:33:78:28:69 (Intel Corporate)
Nmap scan report for 192.168.0.115
Host is up (0.00040s latency).
MAC Address: 00:23:24:3D:07:E0 (G-pro Computer)
Nmap scan report for 192.168.0.116
Host is up (0.021s latency).
MAC Address: CC:AF:78:B3:8B:AB (Hon Hai Precision Ind.)
Nmap scan report for 192.168.0.118
Host is up (0.00043s latency).
MAC Address: 00:23:24:55:76:52 (G-pro Computer)
Nmap scan report for 192.168.0.121
Host is up (0.00035s latency).
MAC Address: 84:34:97:22:92:2A (Hewlett Packard)
Nmap scan report for 192.168.0.124
Host is up (0.028s latency).
MAC Address: 48:D2:24:35:B8:D9 (Liteon Technology)
Nmap scan report for 192.168.0.125
Host is up (0.00042s latency).
MAC Address: F0:92:1C:57:08:B7 (Hewlett Packard)
Nmap scan report for 192.168.0.130
Host is up (0.00060s latency).
MAC Address: 00:23:24:55:79:4F (G-pro Computer)
Nmap scan report for 192.168.0.134
Host is up (0.00032s latency).
MAC Address: 5C:F3:FC:2B:05:8C (IBM)
Nmap scan report for 192.168.0.157
Host is up (0.00017s latency).
MAC Address: 00:23:24:56:84:71 (G-pro Computer)
Nmap scan report for 192.168.0.185

Host is up (0.00021s latency).
MAC Address: 00:23:24:56:83:60 (G-pro Computer)
Nmap scan report for 192.168.0.188
Host is up (0.00029s latency).
MAC Address: 12:8B:18:B2:60:2B (Unknown)
Nmap scan report for 192.168.0.200
Host is up (0.00014s latency).
MAC Address: 34:40:B5:D5:1B:E0 (IBM)
Nmap scan report for 192.168.0.209
Host is up (0.00020s latency).
MAC Address: D8:D3:85:90:4E:C0 (Hewlett Packard)
Nmap scan report for 192.168.0.222
Host is up (0.00048s latency).
MAC Address: 00:23:24:3D:10:30 (G-pro Computer)
Nmap scan report for 192.168.0.245
Host is up (0.0011s latency).
MAC Address: 50:B7:C3:07:17:81 (Samsung Electronics)
Nmap scan report for 192.168.0.246
Host is up (0.0018s latency).
MAC Address: 00:23:24:55:78:9B (G-pro Computer)
Nmap scan report for 192.168.0.249
Host is up (0.00044s latency).
MAC Address: 00:23:24:55:4C:C1 (G-pro Computer)
Nmap scan report for 192.168.0.254
Host is up (0.0037s latency).
MAC Address: 00:E0:4D:44:64:74 (Internet Initiative Japan)
Nmap scan report for 192.168.0.132
Host is up.
Nmap done: 256 IP addresses (23 hosts up) scanned in 53.50 seconds

ANEXO F. ESCANEO DE PUERTOS REALIZADO A LA RED 192.168.0.0 EL 12 DE ABRIL (Ver anexo. Archivo de Texto Escaneo de Puertos en 192.168.0.0_12_Abril.txt)

Escaneo de Puertos
en 192.168.0.0_12_A

ANEXO G. ESCANEO DE VULNERABILIDADES POR IP MEDIANTE NESSUS EL 28 DE ABRIL (Ver anexo. Archivo PDF Escaneo_Vulnerabilidades_28_Abril_IP.pdf)

Escaneo_Vulnerabil
idades_28_Abril_IP.p

ANEXO H. ESCANEO DE VULNERABILIDADES POR VULNERABILIDAD MEDIANTE NESSUS EL 28 DE ABRIL (Ver anexo. Archivo PDF Escaneo_Vulnerabilidades_28_Abril_Descripcion.pdf)

Escaneo_Vulnerabil
idades_28_Abril_Des

ANEXO I. BARRIDO DE PING REALIZADO A LA RED 192.168.0.0 EL 12 DE MAYO (Ver anexo. Archivo de texto Barrido de Ping en 192.168.0.0_12_Mayo.txt)

Barrido de Ping en
192.168.0.0_12_May

ANEXO J. ESCANEO DE PUERTOS REALIZADO A LA RED 192.168.0.0 EL 12 DE MAYO (Ver anexo. Archivo de texto Escaneo de Puertos en 192.168.0.0_12_Mayo.txt)

Escaneo de Puertos
en 192.168.0.0_12_M

ANEXO K. ESCANEO DE VULNERABILIDADES MEDIANTE OPENVAS EL 12 DE MAYO (Ver anexo. Archivo PDF Escaneo_Vulnerabilidades_12_Mayo.pdf)

Escaneo_Vulnerabil
idades_12_Mayo.pdf

ANEXO L. ANÁLISIS DE TRÁFICO CON WIRESHARK REALIZADO A LA RED DURANTE UN ATAQUE INFORMÁTICO (Ver anexo. Archivo pcapng SniffWireshark.pcapng)

SniffWireshark.pcapng

ANEXO M. RESUMEN ANÁLITICO DE EDUCACIÓN (RAE)

Universidad Nacional Abierta y a Distancia	**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE

1. Información General	
Tipo de documento	Trabajo de grado de Especialización
Acceso al documento	Universidad Nacional Abierta y a Distancia – UNAD
Título del documento	Implementación de Procedimientos de Seguridad Eficientes producto de hallazgos posteriores a la ejecución de un Penetration Test aplicado a la empresa CJT&T Ingeniería de Software.
Autor	López Parra, Miguel Angel.
Asesor	Larrahondo Nuñez, Alexander.
Publicación	Bogotá. Universidad Nacional Abierta y a Distancia, 2016.
Unidad Patrocinante	CJT&T Ingeniería de Software.
Palabras Claves	Procedimientos de Seguridad, Políticas de Seguridad, Pentesting, Hacking Ético, Delitos Informáticos, Herramientas Informáticas.

2. Descripción
La necesidad de efectuar un Hacking Ético toma sentido al analizar el crecimiento de los delitos informáticos en el país. Así, ésta magnífica herramienta permite simular las diferentes fases de un ataque informático para formular posibles escenarios de exposición que serían información clave para identificar las falencias actuales de los sistemas de la organización en materia de seguridad determinando amenazas y activos sensibles. Es decir, el hecho de poder determinar la facilidad del atacante para acceder y emprender contra los elementos sensibles de la empresa sería determinante para trazar un panorama sobre la situación real de los sistemas y la posterior implementación de mejoras verificando los mecanismos de seguridad. De esta manera, se podrán para evitar interferencias en la operación de la empresa que serían las causantes de pérdidas de todo tipo.

Por lo tanto, las pruebas que se desprenden del Hacking Ético son las responsables de evaluar el nivel de seguridad de la organización en el ámbito informático que será fundamental para la toma de decisiones.

Los resultados son insumo para el planteamiento de recomendaciones aplicadas al contexto generando políticas y procedimientos consecuentes para mantener la organización a salvo o con un mínimo impacto en sus activos de información.

3. Fuentes

El trabajo de grado constituyó un trabajo de campo extenso que está soportado teniendo en cuenta las siguientes como las más relevantes referencias:

CÓDIGO VERDE. *Prueba de Penetración (PenTest) [en línea]*. [Consultado el 14 de Marzo de 2015]. Disponible en Internet: <http://codigoverde.com/consultoria-especializada/prueba-de-penetracion-pentest/>

DRAGÓN. *¿Cómo se realiza un Pentest? [en línea]*. [Consultado el 14 de Marzo de 2015]. Disponible en Internet: <http://www.dragonjar.org/como-realizar-un-pentest.xhtml>

NYXBONE. *Pentest [en línea].* [Consultado el 14 de Marzo de 2015]. Disponible en Internet: <http://www.nyxbone.com/pentest.html>

CATOIRA, Fernando. *Penetration Test, ¿en qué consiste? [en línea].* [Consultado el 15 de Marzo de 2015]. Disponible en Internet: <https://hackersenlared.wordpress.com/category/capacitacion/que-es-un-pentest/>

PENETRATION TESTING TOOLS. *Penetration Testing Framework [en línea]*. [Consultado el 17 de Marzo de 2015]. Disponible en Internet: <http://www.pen-tests.com/penetration-testing-framework.html>

HERZOG, Pete. *Open Source Security Testing Methodology Manual (OSSTMM) [en línea]*. [Consultado el 17 de Marzo de 2015]. Disponible en Internet: <http://www.isecom.org/research/osstmm.html>

4. Contenidos

En el presente trabajo de grado se optó por el área de conocimiento correspondiente a la Seguridad en redes centrándose en el proceso que implica realizar un Pentesting para formular prácticas de seguridad adecuadas en la empresa CJT&T Ingeniería de Software.

El estudio surge en respuesta a la preocupación del autor sobre la situación de seguridad actual de la organización patrocinante. Así, motivado sobre el inminente riesgo de intrusiones abusivas basados en la gran gama de modalidades de ataques informáticos, así como herramientas disponibles de manera pública en la actualidad se hace necesario establecer mecanismos de protección que sean capaces de mejorar las condiciones de disponibilidad, integridad, autenticidad y no repudio con respecto a los activos de información críticos.

En este sentido, en primera instancia se ha centrado el estudio sobre el principal objetivo de lograr la implementación de procedimientos de seguridad basados en políticas formuladas en respuesta a una serie de fases producto del proceso de Pentesting.

Así, el Pentesting o Hacking Ético se ejecutará en referencia al estándar PTES (Penetration Test Execution Standard) debido a que su contenido es el resultado de las características comunes correspondientes a casos de éxito en la aplicación de este tipo de pruebas.

Entonces, siguiendo el cronograma de actividades puesto en conocimiento a la organización se procedió con el inicio de la fase de recolección de información en la cual se pretendió obtener la mayor cantidad de datos útiles desde fuentes públicas y privadas para reconocer e indagar sobre aquellos datos que podrían ser de utilidad e interés para el atacante que busca conocer y adentrarse sobre la infraestructura y el negocio de su objetivo. En este punto, se efectúan procesos como la inteligencia de fuentes abiertas y el footprint de internet, interno y externo.

Cuando se cuenta con el suficiente conocimiento sobre el objetivo, llega el momento de efectuar un análisis sobre las vulnerabilidades en los sistemas. Los escáneres Nessus y OpenVAS en conjunto con los procesos de observación realizados en la empresa permitieron detectar aquellas falencias en los diferentes dispositivos de la organización. La severidad de estas fallas permite priorizar su solución desde las alternativas propuestas por estos programas o medidas a nivel de hardware y software asociadas con la protección de los activos. El escanear las vulnerabilidades permitió generar los vectores de ataque para establecer de qué manera sería expuesta la organización con respecto a determinadas amenazas.

Posterior a esto, el proceso de explotación materializó los vectores de ataque para simular escenarios en la organización y dejar constatado y evidenciada la gravedad o consecuencias que podrían implicar este tipo de situaciones. En cuestión, se podría denegar los servicios, robar información, usurpar identidades, controlar recursos, entre otros.

Finalmente, con esta información se formulan unas políticas y procedimientos en respuesta a las vulnerabilidades encontradas, para garantizar que tanto personal como dirección basen sus actuaciones sobre buenas prácticas y mecanismos de prevención teniendo claridad sobre los conceptos de seguridad.

5. Metodología

Método de investigación: Enfoque inductivo-deductivo con el fin de organizar los procedimientos lógicos y llegar mediante diferentes técnicas e instrumentos hacia una descripción más detallada de la realidad relacionada con la Seguridad Informática y Hacking Ético.

Población del estudio: Talento humano de la empresa CJT&T Ingeniería de Software

Unidad de análisis: Área de tecnología de la empresa.

Hipótesis General: La realización de un Penetration Test permite conocer el nivel de seguridad informática que existe en la empresa CJT&T, contribuyendo hacia la prevención de posibles ataques a la infraestructura tecnológica de la organización.

Procedimiento a seguir:

- Identificación y localización de fuentes de información.
- Consulta de fuentes localizadas.
- Recolección y Ordenamiento de Información
- Interpretación y análisis de Información
- Presentación de análisis final a manera de conclusiones y presentación formal del proyecto.

Forma de Investigación: Investigación Aplicada.

Tipo de Investigación: Investigación Descriptiva.

5. Conclusiones

Dado el actual contexto en el cual la Seguridad Informática ha logrado tener un gran protagonismo, el uso de herramientas automatizadas facilita la labor correspondiente a las diferentes fases del Pentesting, sin embargo, éstas no deben sesgar el criterio del experto y este debe acudir hacia la creatividad para plantear diferentes vectores de ataque que permitan revelar los escenarios en los cuáles un atacante podría aprovecharse sobre los diferentes fallos de seguridad que tendría una organización.

La identificación de vulnerabilidades permite constatar las debilidades de seguridad a nivel organizacional las cuales se deberán priorizar para dar tratamiento a los riesgos con el fin de fortalecer los mecanismos de protección contra intrusos.

El análisis de vulnerabilidades permitió establecer los puntos comunes sobre las posibles causas de estos resultados para evaluar las amenazas con el fin de poder formular los controles adecuados en respuesta a las necesidades de la organización.

La fase de explotación es clave y representa la diferencia entre un simple análisis de vulnerabilidades y un Pentesting permitiendo comprobar y establecer el alcance de los hallazgos realizados en fases anteriores.

Los procedimientos de seguridad informática permiten que el personal de la organización tenga a su disposición la información necesaria que sea la herramienta para poder proteger de manera efectiva los activos que estén a su alcance y que sean su responsabilidad.

Los procedimientos de seguridad informática permiten definir las pautas detalladas sobre la implementación de las políticas siendo claves sobre el modo de actuación del personal detallando que se debería hacer con respecto a procesos específicos claves en la seguridad de la organización.