CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

SINDY VANESSA MIRANDA MARTÍNEZ

TUTOR:

JOHN FREDDY QUINTERO

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD – RED TEAM & BLUE TEAM
GRUPO 202337164_3

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
SANTA MARTA
2022

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma del presidente jurado

Firma del jurado

Firma del jurado

DEDICATORIA

A Dios todo poderoso por su infinita misericordia y darme la sabiduría y la virtud de ver cumplida su promesa de capacitarme, darme triunfos y victorias.

Por su plan perfecto de que a su tiempo dispondría todo lo necesario para poder ver hecho realidad un anhelo.

A mis padres y familiares por creer en mí y apoyarme con una voz de aliento durante todo el desarrollo de la especialización.

Al la Universidad Nacional abierta y a distancia UNAD junto con su talento humano que han sido guía en este proceso de aprendizaje.

AGRADECIMIENTOS

A Dios por extender su mano sobre mí y darme la fortaleza para salir adelante en medio de la prueba y la dificultad

A mis padres, quienes en el transcurso de la vida me han enseñado que la constancia y la humildad hacen grandes seres humanos.

A todos los tutores y equipo administrativo de la UNAD quienes a través de su dedicación y compromiso aportaron al cumplimiento de un proyecto profesional.

TABLA DE CONTENIDO

GLOSARIO

ACTIVO DE INFORMACION: Es un dato o elemento que tiene valor para la Entidad.

AMENAZA: Es la indicación de un potencial evento no deseado que afecte negativamente la confidencialidad, integridad, disponibilidad o confiabilidad de los activos de información.

CIBERSEGURIDAD: Conjunto de políticas, directrices y métodos para la gestión de riesgos y que son útiles al momento de proteger los activos de una organización.

INCIDENTE: Un Incidente de seguridad de la Información es cualquier evento que vulnere o intente vulnerar la información.

RIESGO: Es la posibilidad que una amenaza explote o penetre una vulnerabilidad de un activo de información, impactando a este activo de información y/o activos asociados, viéndose, afectando del mismo modo los objetivos del negocio

VULNERABILIDAD: Es una debilidad de seguridad asociada a un activo de información que puede hacer que una amenaza se haga efectiva.

NORMA: Conjunto de reglas que regulan el accionar de las personas ante un tema específico en un país.

LEY: Documento que regula una acción o proceder de una sociedad y dictamina tanto la protección de la persona, como la penalización en caso de incurrir en lo ahí consignado.

HARDENIZACION Es una medida de seguridad que se aplica sobre equipos de trabajo con el fin de reducir la superficie de vulnerabilidad, evitando así posibles ataques.

KALI LINUX: Sistema operativo utilizado para realizar las pruebas se seguridad, auditorías y hacking ético de los sistemas.

METASPLOIT: Herramienta utilizada en sistemas operativos como Kali Linux por Blue team y Red team, con la cual se pueden realizar pruebas de intrusión, ejecutar Exploits y documentar tales resultados.

NMAP: Herramienta utilizada en sistemas operativos como Kali Linux, la cual sirve para obtener las direcciones IP de una red, los puertos disponibles de los equipos que encuentra en la red, características de sistemas e información relevante que viaja por la red.

REDTEAM: Es un equipo que actúa como atacante, realizando análisis, descubriendo vulnerabilidades, ataques y realizar de una manera ética sus acciones para de esta forma detectar falencias de seguridad en una organización.

RESUMEN

La información se considera el principal activo de las organizaciones, ésta viaja a través de redes, dispositivos y el talento humano que hace uso de esta; ya que cada vez es mayor el aumento en la interacción de las organizaciones a partir de múltiples medios de comunicación.

La Seguridad informática se caracteriza por brindar la protección a los datos asegurando la Integridad, disponibilidad y Confidencialidad a partir de herramientas y software especializado.

Este trabajo se enfoca en analizar el marco normativo existente en Colombia relacionado con los delitos informáticos y la protección de datos personales, así mismo los procesos de ejecución de pruebas de ciberseguridad.

Min TIC Revela que para el año 2021 el comercio electrónico mostró un aumento en las ventas en línea del 44,3 %, y las transacciones en un 78,7% con relación a la vigencia anterior, según cifras de la Cámara Colombiana de Comercio Electrónico (Ccce).

Teniendo en cuenta lo anterior las organizaciones enfrentan un problema que radica en el aumento de delitos informáticos y por ende en la necesidad de leyes que regulen los temas relacionados a nivel preventivo y correctivo.

Con el desarrollo trabajo, se espera estudiar Leyes, Normas y/Decretos existente en Colombia relacionado con delitos informáticos.

La exposición de las organizaciones a los riegos Informáticos si bien no los exime del riesgo los obliga a mantenerse alerta y ejercer acciones de contención para reducir el impacto de un ataque. La creciente dependencia del internet para que una organización se mantenga en el mercado la convierte en aliada de la tecnología como mecanismo de defensa ante los ciber atacantes. Este trabajo se enfoca en analizar un escenario en el cual expone la situación que enfrenta

WhiteHouse Security y poder ofrecerle una asesoría como equipos BlueTeams para contener un ataque en tiempo real y ofrecer una serie de estrategias que puedan ser implementadas.

PALABRAS CLAVE

SEGURIDAD, DELITOS, LEGISLACION, PROTECCION, CONTENCION

ABSTRACT

Information is considered the main asset of organizations, it travels through networks, devices and the human talent that makes use of it; since the increase in the interaction of organizations from multiple media is increasing.

Computer Security is characterized by providing data protection ensuring Integrity, availability and Confidentiality from specialized tools and software.

This work focuses on analyzing the existing regulatory framework in Colombia related to computer crimes and the protection of personal data, as well as the processes of executing cybersecurity tests.

Min TIC Reveals that by 2021 electronic commerce showed an increase in online sales of 44.3%, and transactions by 78.7% in relation to the previous period, according to figures from the Colombian Chamber of Electronic Commerce (cccc).

Considering the above, organizations face a problem that lies in the increase in computer crimes and therefore in the need for laws that regulate related issues at a preventive and corrective level.

With the development of work, it is expected to study existing Laws, Regulations and/or Decrees in Colombia related to computer crimes.

The exposure of organizations to IT risks, although it does not exempt them from the risk, forces them to remain alert and exercise containment actions to reduce the impact of an attack. The growing dependence on the internet for an organization to stay in the market makes it an ally of technology as a defense mechanism against cyber attackers. This work focuses on analyzing a scenario in which it exposes the situation facing WhiteHouse Security and being able to offer advice such as Blue Teams teams to contain an attack in real time and offer a series of strategies that can be implemented.

KEYWORDS

SECURITY, CRIMES, LEGISLATION, PROTECTION, CONTAINMENT

INTRODUCCIÓN

El considerable uso de internet y las redes de comunicaciones como base de pequeños y grandes negocios ha causado gran impacto en el mundo creando además de la solución a innumerables necesidades de una comunidad la exposición a amenazas y riesgos a distintos niveles.

Teniendo en cuenta que todo tipo de relación económica que se surge y se desarrolla a través de internet involucra un valor económico, comercial y personal surge la necesidad de brindarles protección.

En virtud de lo anterior y a partir de la seguridad informática se busca la protección de los datos y la información y sus pilares fundamentales como son: integridad, disponibilidad y Confidencialidad.

En Colombia se define un delito informático como el acceso de manera ilícita o no autorizada a datos o información que están resguardados en formatos digitales, la Ley 1273 del 2009 en sus artículos detalla cada acto a saber:

✓ Acceso abusivo a un sistema informático.

✓ Obstaculización ilegítima de sistema informático o red de telecomunicación**.**

✓ Interceptación de datos informáticos.

✓ Daño Informático.

✓ Uso de software malicioso.

✓ Violación de datos personales.

✓ Suplantación de sitios web para capturar datos personales.

✓ Hurto por medios informáticos y semejantes.

✓ Transferencia no consentida de activos.

Teniendo en cuenta que los delitos informáticos son mucho más comunes de lo que se imagina, incluso en medio de la emergencia sanitaria (COVID 19) las denuncias se han incrementado un 55%, un ejemplo de ello los Códigos QR *Quick Response*, en español “respuesta rápida”) que aunque positivamente ha sido una alternativa para cuidarse de este virus para los Ciberdelincuentes ha representado la puerta que se ha abierto para incrementar las estafas y amenazas a miles de usuarios que se sirven de su practicidad.

Según EL ESPECATADOR “*Los códigos QR han cobrado protagonismo en nuestro día a día, no obstante, expertos en seguridad informática advierten sobre el uso indebido que se le puede dar a los mismos*” esta noticia del 21 de enero de este medio de comunicación nacional confirma que, aunque el riesgo es inminente siempre se insiste en la perspicacia de los usuarios de la tecnología para no ser presa fácil de los ciberdelincuentes.

Este informe busca principalmente consultar y citar la legislación existente en Colombia referente a Delitos informáticos y Protección de datos, Además estudiar herramientas de Ciberseguridad y de esta forma brindar como Experto en seguridad, la información necesaria para que The WhiteHouse Security sea asertivo en la toma de decisiones sobre la vinculación de empelados a su planta de personal.

Por otro lado, la ejecución de pruebas de intrusión y la contención de ataques informáticos son prácticas de un equipo Blueteams y Redteams para brindar una asesoría a The WhiteHouse Security

PLANTEAMIENTO DEL PROBLEMA

El aumento de transacciones realizadas a través de internet durante los últimos años ha alcanzado niveles altos, son más de 4.388 millones de usuarios de internet para el 2019 cifra que supera la mitad de la población. (El tiempo, 2019)

En cuanto a Colombia los usuarios de internet han aumentado 64% lo que nos ubica en el puesto 34 a nivel mundial.

Colombia figura como uno de los jugadores más importantes para el comercio electrónico en Latinoamérica. Según el e-Commerce Index 2017, el país ocupa el tercer puesto, después de Chile y Brasil, con mayor crecimiento y proyección en este sector de la economía.

El 35% de las empresas en Colombia venden por la red y el 59% de los usuarios de Internet ingresa por dispositivos móviles

A través de las múltiples plataformas se han fortalecido las relaciones empresa-cliente, según el Ministerio de las TIC, esto se debe a que el 61,4% de la población colombiana cuenta con acceso a internet.

A partir del escenario expuesto, se evidencia que, aunque la mayoría de las empresas sabe que se enfrentan riesgos a diario producto de su contacto con la red, no tiene claridad de que procedimiento seguir para atender de manera adecuada los incidentes y prevenir una vulnerabilidad.

¿Cómo puede un equipo de expertos de Blue team y Read team brindar una asesoría a la compañía The WhiteHouse Security teniendo en cuenta las leyes, Decretos o normas sobre delitos informáticos en Colombia para contener ataques y/o atender futuras situaciones que afecten su Ciber Seguridad?

JUSTIFICACIÓN

Este informe tiene como objetivo analizar la legislación existente en Colombia sobre Delitos Informáticos, haciendo énfasis en sus características y alcance que permita tanto a las empresas como la ciudadanía en general conocer cuáles son los adelantos del país en el marco de la protección de los datos y brindar a las víctimas de un ataque un respaldo ante su perdida.

Es importante mencionar la necesidad de que estos actores (empresas y personas naturales) conozca las vulnerabilidades a las que se encuentran expuestos al hacer uso de la tecnología, que existen controles que son necesarios aplicar para minimizar el riego e impacto en caso de su ocurrencia.

En concordancia con lo anterior, la relevancia de la información contenida en el presente trabajo toda vez que con este conocimiento previo se tendrá una mente más abierta a como las leyes pueden convertirse en un aliado en el evento de ser víctima de un delito informático.

Cuando una empresa conoce la regulación se acoge a la prevención y de esta manera pueden mantener una confidencialidad, integridad y disponibilidad de sus datos y servicios, proporcionando a sus clientes seguridad, confianza, transparencia y sobre todo generar un crecimiento exponencial en todos los ámbitos, por la calidad y seguridad con la que realizan sus transacciones.

El ejercicio de documentar la legislación en materia de delitos informáticos permitirá que estudiantes, Organizaciones, centros de formación en otros puedan obtener información veraz y actualizada sobre los avances en esta materia en nuestro país y ser objeto de comparación con otros países.

Por otro lado, permitirá que pequeñas, medianas y grandes empresas puedan mitigar los riesgos de seguridad y al mismo tiempo aportará una trasferencia de

conocimiento que cambiará la cultura organizacional dentro de la administración de los riesgos.

llevado esto a los equipos Blue Team y Red Team, se plantearán escenarios que les permitirán a estos aportar una serie de recomendaciones para robustecer aspectos de seguridad de una organización.

OBJETIVO GENERAL

Brindar un informe guía que describa las acciones propuestas por los expertos de equipos Blue Team y Red Team para resolver aspectos técnicos de seguridad en la empresa WhiteHouse Security

OBJETIVOS ESPECÍFICOS

- ✓ Consultar las leyes, Normas y Decretos sobre Delitos Informáticos en Colombia y Protección de datos personales.
- ✓ Estudiar las características principales de cada Ley.
- ✓ Establecer un banco de trabajo Rejetto
- ✓ Analizar las distintas herramientas de Ciberseguridad.
- ✓ Realizar pruebas de Pentesting y realizar un análisis de estas.
- ✓ Identificar los fallos de seguridad de una maquina Windows
- ✓ Analizar las diferencias entre un equipo Blue Team y un equipo de respuesta de incidentes.

MARCO REFERENCIAL

Para conocer el contexto del presente informe, se ha creado un marco de referencia que incluye el estudio de las leyes, Decretos, resoluciones y demás regulaciones en materia de Delitos informáticos que han sido instauradas en Colombia y su aplicabilidad actualmente para prevenir dichos ataques de cara a una labor de concientización sobre los riesgos y los niveles de impacto.

Debido al aumento en la dependencia del internet, han crecido también los riesgos y las organizaciones han tenido que ver con más responsabilidad la seguridad de sus activos y entender que invertir en ello es tan importante como comprar materia prima para su negocio.

La Ciberseguridad, es un término que data de los años 80, época en la que ya se conocían los ordenadores con CPU Intel y en la que en Estados unidos ya se hablaba de la manipulación de teléfonos suceso que revolucionó la época cuando un hombre de nombre Denny informó sobre la novedad, así mismo Steve Wozniak (Co-fundador de Apple), John Draper (Pirata Informático, Captain Crunch), Kevin Mitnick (Mayor Hacker de la historia) se convirtieron en un equipo dedicado a estudiar el tema.

Desde entonces y producto del trabajo en equipo de estos personajes se habla de Seguridad y de que los usuarios eran vulnerables al usar una computadora entendiendo desde ese momento que las organizaciones dependían de los computadores para su funcionamiento.

Como se ha visto el término de Ciberseguridad, se refiere a la protección de los activos frente a una amenaza y vulnerabilidad.

Un activo para una organización se representa en las personas, los equipos y los sistemas, es por ello por lo que se hablaba en la época de usuario vulnerable cuyo

concepto hasta hoy tiene que ver con la incapacidad de resistencia al presentarse un fenómeno amenazante.

Así las cosas, se tienen tres términos que son los encargados de brindar protección: la Ciberseguridad, la Seguridad informática, Seguridad de la información y un protegido llamado Activo el cual debe ser blindado ante posibles riesgos o vulnerabilidades que de llegarse a materializar se convertirían en una amenaza a partir de lo que se configura como delito informático.

Según ISCA, La ciberseguridad o Seguridad en internet es la “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”. Sobe el tema kaspersky afirma que El gobierno de Estados Unidos invierte USD 13 000 millones al año en ciberseguridad; sin embargo, estos ataques evolucionan con gran rapidez.

De acuerdo con lo señalado por la ISO 27001 “La seguridad informática se describe como la distinción táctica y operacional de la seguridad, mientras que la seguridad de la información es la línea estratégica de la seguridad.” En otras palabras, la seguridad informática incluye las medidas de protección en materia de tecnología e infraestructura y la seguridad de la información involucra los riesgos, amenazas, buenas prácticas y normatividad.

Ahora bien, lo más importante es que las organizaciones sean conscientes de que el riesgo siempre existe y se involucren el proceso constante de mitigación, lo cual les permitirá tomar decisiones desde la alta dirección, alineadas al gobierno de TI y en cumplimiento de las políticas de seguridad y su adecuada implementación.

Dicho lo anterior, se pretende desde el Gobierno nacional crear jurisprudencia vinculando de manera permanente todos los delitos informáticos que van surgiendo en el entendido que estos mutan a diario.

Desde la Corte Constitucional el Habeas data como un derecho es una facultad que brinda respaldo al titular de los datos y otorga ligadas al derecho a la intimidad y a la información.

MARCO TEÓRICO

El concepto de ciberseguridad está orientado a la protección de la información y de los sistemas almacenan o gestionan información con el fin de brindar confidencialidad, la integridad y disponibilidad.

La seguridad informática por su parte es una disciplina basada en herramientas, procedimientos y estrategias cuyo objetivo es garantizar la integridad, disponibilidad y confidencialidad de la información, los cuales se convierten en sus pilares para la adecuada gestión de la información.

Sumado a lo descrito un incidente de seguridad informática es un evento adverso que afecta negativamente a la confidencialidad, integridad y disponibilidad de la información que se procesa, almacena y transmite utilizando una computadora (Campbell, 2003).

Basado en los conceptos citados en los párrafos anteriores vale la pena incorporar un concepto y es la Legislación todas las leyes por la cuales se regula una actividad determinada para el caso en particular los delitos informáticos en Colombia.

Para gestionar la protección de los sistemas, el Red Team a partir de la simulación de ataques dirigidos trabaja en fortalecer la seguridad de las organizaciones.

MARCO CONCEPTUAL

El creciente aumento de ataques cibernéticos por causa de estar conectados, ha generado muchas investigaciones, noticias, entre otras publicaciones que han ocupado la primera plana de revisas e importantes medios de comunicación; sin embargo no ha sido suficiente para que los gerentes y líderes de pequeñas y grandes empresas enciendan alarmas ya que el 80% de las juntas directivas no hacen de la ciberseguridad un tema estratégico para sus compañías, así lo arrojó un reporte de la consultora EY (Guía de Ciberseguridad para el 2019, 2019)

La tendencia en lo que va corrido del año 2021 es mayor inversión por parte de las organizaciones que buscan generar un nivel de confianza hacia sus clientes por lo que le apuestan a la transformación digital a partir de la mejora en la infraestructura de TI e implementación de medidas de seguridad mucho más robustas.

Sectores como el financiero son los más atacados en materia de ciberseguridad, uno de los ataques más significativos ocurridos en Colombia en los últimos años fue en 2011 el 11 de abril cuando fue víctima de un ataque la página web del Ministerio del Interior y de Justicia, las causas son atribuidas a una represaría por un proyecto de ley el cual pretendía penalizar la piratería informática.

Los temas de Ciberseguridad en Colombia son coordinados por el COLCERT y su labor se orienta a la protección de la infraestructura del estado ante cualquier tipo de emergencia.

Se habla de Política Nacional de Seguridad Digital cuya misión es “identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia”

En concordancia con dicha política, se fortalece la labor desde el C4 Centro de Comando, Control, Comunicaciones y Computo de la Policía Nacional, el

Comando Conjunto Cibernético (CCOC), el Centro Cibernético Policial (CCP), el CSIRT de la Policía Nacional.

Los delitos informáticos son crímenes electrónicos que se ejecutan a través de computadores o dispositivos móviles y su finalidad es dañar estos equipos, afectar los canales, hurtar entre otras afectaciones que pueden ser tipificadas y abordadas por un CSIRT.

Los **Ramsomware** son softwares maliciosos que pueden atacar a las maquinas, generando bloqueos o secuestrando la información a cambio de monedas virtuales llamadas bitcoins.

Phishing consiste en el envío de correos electrónicos aparentemente de direcciones confiables pero que lo que buscan es generar fraude.

Los **Malware** son también códigos maliciosos que buscan dañar los sistemas.

Los virus, troyanos o gusanos no menos importantes que los anteriores son parte de la larga lista de eventos (incidentes y vulnerabilidades) que afectan a diario la operación de una empresa.

Con el presente proyecto se realizará un estudio de la legislación existente en Colombia referente a delitos informáticos, su aplicación permitirá que personas naturales y jurídicas conozcan de primera mano los adelantos sobre el tema y además como acudir cuando experimenten incidentes o sean víctimas de algún ataque, así como una gestión adecuada de las vulnerabilidades explotadas mediante la técnica pentesting y lograr que las organizaciones en Colombia sean cada vez más robusta a nivel de infraestructura de seguridad .

Para las organizaciones familiarizarse con conceptos como Analizador de URL, Firewall y controles no es tarea fácil y más aún si su misión no es brindar servicios de tecnología les parecerá extraño; es por esto por lo que al momento de ser víctima de un delito informático la justicia se convierte en el mejor aliado y desde este trabajo se pretende diseñar una amplia y clara lista de leyes y/o decretos

reglamentarios para que la ciudadanía acuda sin temor a que su situación sea atendida.

MARCO LEGAL

El estado colombiano y el Congreso de la república han formulado leyes, Decretos para que todos los ciudadanos puedan actuar en caso de ser víctimas de un delito informático.

En Colombia, desde la década de los 90 se ha sancionado un conjunto de leyes que coadyuvan la gestión del estado en cuanto a delitos cibernéticos, a continuación, se menciona la normatividad existente:

1. Ley No 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

2. Ley No 599 de 2000: Por la cual se expide el código penal. En su artículo No 192, se ratifica la conducta punible de violación ilícita de comunicaciones al establecer el bien jurídico de los derechos de autor y se incluyen algunas conductas relacionadas con el delito informático, tales como el ofrecimiento, venta o compra de equipos para interceptar la comunicación entre personas

3. Ley No 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos' - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Congreso de Colombia, 2009a).

4. Ley No 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC), se crea la Agencia Nacional del Espectro y se dictan otras disposiciones (Congreso de Colombia, 2009b).

5. Decreto No 2364 de 2012: Por medio del cual se reglamenta el artículo No 7 de la Ley No 527 de 1999, sobre la firma electrónica y otras disposiciones (Ministerio

de Comercio, Industria y Turismo, 2002), ítem que corresponde a uno de los lineamientos del Plan de Desarrollo 2010 - 2014.

6. Ley No 1581 de 2012: Por la cual se reglamenta parcialmente el Decreto No 1377 de 2013 y se dictan disposiciones generales para la protección de datos personales (Congreso de Colombia, 2012).

7. Decreto No 1377 de 2013: Por el cual se reglamenta parcialmente la Ley No 1581 de 2012 (Ministerio de Comercio, Industria y Turismo, 2013). Decreto por medio del cual se dictan disposiciones generales para la protección de datos personales. (Congreso de Colombia, 2012).

El CONPES 3854 de 7 de marzo de 2017 se refiere a la Política Nacional de Seguridad Digital la cual pasa a ser responsabilidad de la Dirección de Seguridad de la Presidencia de la república, ya que esta última como máximo órgano ejecutivo puede asegurase que se dará cumplimiento a las políticas y disposiciones.

8. Ley 1928 de 24 de julio de 2018: “Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest”.

Las normas y regulaciones actuales se agrupan en cuatro secciones diferentes de la ley: Circular 029, 042, 052 un anexo a la Circular Básica Jurídica, llamada the Circular de Ciberseguridad SFC CE 007 de junio de 2018.

MARCO TECNOLOGICO

El estado colombiano ha desarrollado esfuerzos para atender los temas de ciberseguridad los cuales son coordinados por el COLCERT y otras entidades como la Policía Nacional coadyuvan la labor.

Para este trabajo se pretende recopilar todos los avances en materia legal que permitan a los ciudadanos contar con un respaldo en caso de ser víctimas de un delito informático y conocer además que técnicas de tipo auditoria les permite comprobar que tan seguros están siendo sus sistemas de información.

Para la documentación se consultarán fuentes oficiales del gobierno Nacional, Actos administrativos, CONPES.

Para las pruebas de Pentesting se utilizará Kali Linux, Aplicación Rejetto

Es importante mencionar que el desarrollo del trabajo alcanzará un nivel de madurez en la medida en que se revisen más fuentes bibliográficas y se utilicen más herramientas para comprobar y monitorear la seguridad de una organización.

MARCO ESPACIAL

De acuerdo con el planteamiento del problema, el presente trabajo será desarrollado en el marco de la necesidad de que empresas y personas naturales de Colombia conozcan los adelantos en jurisprudencia con relación a delitos informáticos y que esto les brinde una ruta al momento de enfrentarse a este tipo de situaciones.

Lo anterior será posible a partir de la consulta, compresión y referencia de las leyes decretos, resoluciones, lo cual se detalla en el Marco Conceptual y deja ver la creciente evolución de los ataques y los sectores más afectados.

La Ciberseguridad y los CSIRT son temas de tendencia y de gran importancia para las organizaciones las cuales se han interesado por el tema de la Seguridad consientes de los grandes riesgos a los que se deben enfrentar como resultado de su posicionamiento en un mercado interconectado, situación que motiva a realizar una investigación rigurosa y basada en realidades que se convierta en un precedente en país.

Luego de desarrollar el presente trabajo se espera poder contar con un insumo documental con “valor” para que empresas y personas naturales puedan disponer de la información necesaria en materia legal sobre delitos informáticos en Colombia.

MARCO METODOLÓGICO

El presente proyecto usaremos varios métodos y técnicas que nos permitan recoger información con el fin de alcanzar los objetivos propuestos.

1. Técnicas.

1.1. Técnica de observación: Esta técnica será usada para visualizar y recopilar información, que permita aclarar el panorama del problema y determinar los acontecimientos importantes y como esto incide en el proyecto.

1.2. Técnica de investigación bibliográfica: Esta técnica será usada para recopilar información de peso y confiabilidad que permitan fundamentar la investigación teórica y será adquirida mediante fuentes de confianza como libros, revistas, artículos científicos, entre otros textos con información de alta relevancia.

2. Aplicación sobre los objetivos específicos:

2.1. Objetivo número 1: Consultar las leyes, Normas y Decretos sobre Delitos Informáticos en Colombia y Protección de datos personales. Para lograr este objetivo es necesario consultar diferentes fuentes bibliográficas, principalmente del Gobierno Nacional que den cuenta de los avances en el tema objeto del presente trabajo.

2.2. Objetivo número 2: Estudiar las características principales de cada Ley.

Para desarrollar este objetivo se hace necesario estudiar cada una de las leyes y decretos e identificar circunstancia de tiempo, modo y lugar en el que se materializa cada delito para que pueda encajar sobre cada ley o Articulo de la misma.

2.3. Objetivo número 3: Analizar las distintas herramientas de Ciberseguridad.

Para desarrollar este objetivo se hace necesario consultar el listado TOP de herramientas de Ciberseguridad existentes y la aplicación de cada una de ellas.

Metasploit, Nmap, OpenVas; A nivel de red Firewall, Antivirus, Herramientas de identidad digital.

1.4 Realizar pruebas de Pentesting y realizar un análisis de estas.

Para desarrollar este objetivo se realizan paso a paso pruebas de pentesting

1.5 Identificar los fallos de seguridad de una maquina Windows

Para desarrollar este objetivo se utiliza una aplicación Rejetto en una maquina con sistema operativo Windows 7 que tiene un exploit instalado.

1.6 Analizar las diferencias entre un equipo Blue Team y un equipo de respuesta de incidentes.

Para desarrollar este objetivo, se requiere consultar bibliografía para aprender no solo un concepto de Red Team y Blue Team, sino conocer su forma de accionar y contribuir a fortalecer de seguridad de una organización desde distintas estrategias de intervención.

DESARROLLO DEL INFORME

legislación "leyes, decretos" existen actualmente y las características principales de cada ley.

La exposición a la tecnología como parte de la optimización de los procesos en las empresas y/o establecimientos de comercio ha incidido en el aumento de los delitos informáticos en Colombia y el mundo.

Para hablar de Protección de datos personales es importante entender que los delitos ocasionados por el tratamiento de estos llevan consigo una serie de responsabilidades de Tipo Penal, Administrativa, Contractual, Económica y Bancaria.

Al respecto, en Colombia existen la Ley 1273 de 2009, en la cual se respaldan las empresas y personas naturales para denunciar los ataques contra la información, la violación de datos personales, el acceso abusivo a sistema informático, la interceptación de datos informáticos, el uso de software malicioso, entre otros. La presente Ley va ligada a la **responsabilidad penal** en la cual intervienen fiscalía y policía quienes tienen la facultad para llevar a la cárcel o imponen sanciones de tipo económico.

La protección sobre el mal manejo de los datos personales está a cargo de la SIC en el marco de la Ley 1581 de 2012 y trata **responsabilidades de tipo administrativo** por parte de la Delegatura de protección de datos de la Superintendencia de Industria y Comercio, que tiene facultades legales para sancionar hasta con 2000 salarios mínimos legales vigentes.

De aquí la obligatoriedad de las entidades públicas y privadas de hacer registro nacional de sus bases de datos RNBD y de esta forma poder reportar los **incidentes informáticos** que afecten la información personal dentro de las 24 horas siguientes del momento que se conozca el incidente.

Hablemos de “Habeas Data”, En Colombia la Corte Constitucional definió la Ley 1581 de 2012 y el Decreto 1377 de 2013, como el derecho constitucional que tienen todas las personas a conocer, suprimir, actualizar y rectificar todo tipo de datos personales recolectados, almacenados o que hayan sido objeto de tratamiento en bases de datos en las entidades del públicas y privadas, en ese sentido se limita la posibilidad de su divulgación, publicación o cesión.

Etapas del pentesting, ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Como ya se ha mencionado en el desarrollo del documento todo computador o dispositivo móvil conectado a internet es susceptible a recibir un ataque por lo que la verdadera preocupación de las pequeñas y grandes empresas debe ser invertir en ciberseguridad y de esa forma poder mitigar su impacto.

De ahí surge pentesting o test de penetración como una práctica que permite determinar los alcances o el nivel de seguridad de la información que tiene una compañía, te preguntaras quien realiza este tipo de actividad pues se le llama Pentester o auditor de Ciberseguridad un término interesante y de hecho un rol con alta demanda en el mercado debido al incremento de casos.

Existen varios tipos de Pentesting para abordar la seguridad de una organización; estas pruebas pueden ser realizadas sobre varios aspectos como la seguridad de la red sin importar su estructura, en alguna aplicación de software que utilice la organización, en la seguridad física de la organización y por último en el personal a partir de la ingeniería Social.

Es importante mencionar que la ejecución de estas pruebas puede llevarse a cabo con o sin anuncio previo, con solo el nombre de la empresa o por el contrario recibiendo toda la información de la empresa objeto de la prueba, incluso puede hacerse combinando las dos estrategias lo cual se conoce con el termino Grey-box o caja gris. Dicho de otra forma, el pentesting puede ser de 3 tipos: *Caja blanca* que es donde el auditor tiene el conocimiento de cómo está estructurada la empresa conoce contraseñas, IP y toda la información necesaria para ejecutar la prueba, *Caja Negra* donde se simula un escenario real porque el pentester lo único que conoce es el nombre de la empresa y esto lo sitúa en un rol de "delincuente informático real", *Caja Gris* es una combinación de los dos primeros es decir que el pentester conoce solo cierta información de la compañía.

Un Pentesting se lleva a cabo a partir de 3 fases que son Pre-Ataque, Ataque y Post-Ataque; en la primera el propósito es planear el ataque a realizar luego de ello se define un objetivo a partir de una vulnerabilidad y el post- Ataque que consiste en el reporte o resultado de la actividad realizada.

Para la ejecución de las pruebas pentesting se utilizan algunas herramientas algunas de ellas en su orden de popularidad son Nmap, Nessus, Wireshark, Burp Suite, John the Ripper.

Herramientas de ciberseguridad

Metasploit Es una herramienta enfocada a auditores de seguridad y equipos red Teams y Blue Teams contiene miles de Sploit que son vulnerabilidades conocidas y códigos para explotarlas. Es posible con ella trabajar con Nmap su principal característica es que es gratis y multiplataforma.

Nmap Es una herramienta utilizada para explorar una red.

OpenVas Es un escanner de vulnerabilidades desarrollado en el año 2009 por la empresa Greenbone Networks en código abierto su uso radica en pruebas autenticadas, no autenticadas ajustable según la escala de la exploración a realizar**.**

ExploitDB Es un directorio web donde se pueden encontrar miles de vulnerabilidades de las aplicaciones, dicha información es actualizada frecuentemente y los encargados de este repositorio de información son los hackers.

CVE en inglés Common Vulnerabilities and exposures es una lista de vulnerabilidades identificadas por un número por ser publica su propósito es que los expertos en TI puedan adelantar investigaciones que lleven a solucionar puntos vulnerables y brindar mayor seguridad a los sistemas informáticos.

Los CVE son supervisados por la MITRE Corporation y as Autoridades de numeración o CNA son las encargadas de asignar un número a cada vulnerabilidad.

Cualquier persona puede notificar que encontró una vulnerabilidad incluso proveedores ofrecen dinero a cambio de que les ayuden identificando fallas a sus desarrollos.

la antítesis entre lo jurídico y lo ético

A lo largo de la historia de la humanidad, un problema filosófico que ha estado siempre como uno de los grandes dilemas, surgiendo la pregunta si el derecho se encuadra del obrar justo en general, lo que implica necesariamente remitirse a la ética como fundamento de su carácter jurídico.

Grandes exponentes del pensamiento como Enmanuel Kant sostuvo que el derecho surge precisamente de un postulado ético, con una concepción aún más fuerte, sosteniendo que estas dos esferas no debían mirarse de manera independientes, sino como una esfera de “orden moral”.

Análisis Legal

De acuerdo con lo plasmado en el Anexo 3 “ACUERDO”, se evidencia varios procesos ilegales consignados en este, tales como:

Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados. (subrayado y negrilla fuera de texto).

Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de

utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”. (subrayado y negrilla fuera de texto).

De conformidad con la ley 1273 de 2009, De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, estaría vulnerando el artículo 269ª y 269C que establece:

A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial. (subrayado y negrilla fuera de texto).

Cuarta. Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a: De ser necesario o conveniente

según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la información confidencial segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de esta o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la información confidencial, sea verbal, escrita, visual, tangible e intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Whitehouse Security, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla. (subrayado y negrilla fuera de texto).

3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros. (subrayado y negrilla fuera de texto).

En virtud de la ley 1273 de 2009, se está violando el l Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas. (subrayado y negrilla fuera de texto).

Atendiendo lo establecido en el Código de ética COPNIA- está contraviniendo el CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES, en lo referente al numeral:

f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;

6. Mantener la información confidencial en reserva hasta tanto adquiera el carácter de pública. (subrayado y negrilla fuera de texto).

7. Responder por el mal uso que le den sus representantes a la información confidencial. (subrayado y negrilla fuera de texto).

Considero que el receptor no tiene responsabilidad respecto del uso que la organización de a la información una vez esta sale de su esfera o custodia pues se pierde control de este activo.

8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento. (subrayado y negrilla fuera de texto).

La gerencia desde el mismo momento que suscribe los contratos el proceso está viciado debido a irregularidades que identifica el abogado y la organización omite desde lo ético y se ciñe solo verbalmente a señalar “tenga cuidado al firmar”, lo que deja claro que no existe coherencia entre el acuerdo de confidencialidad con respecto a las funciones del personal reclutado para la conformación de los equipos Red Teams y Blue Teams.

Se habla de disfrazar en ejercicio de la profesión el verdadero sentido de la confidencialidad y manipular la información con justificante de una política estatal o institucional de actuar “Legitimo”

9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security. (subrayado y negrilla fuera de texto).

Obligaciones de la ´parte reveladora

Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.

Argumento que rechaza la propuesta del salario de $15.000.000 de pesos colombianos mensuales de conformidad con lo dispuesto en COPNIA en su código de ética para ingenieros.

Atendiendo los lineamientos planteados en el Código de Ética COPNIA- CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES, no aceptaría una oferta laboral bajo estas condiciones toda vez que contraviene no solo principios éticos que rigen la profesión de Ingeniero sino también transgreden las normativas del ordenamiento penal contemplado en la ley 1273 de 2009 por cuanto me encontraría en curso de las siguientes violaciones:

ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. Son prohibiciones especiales a los profesionales respecto de la sociedad: a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación

ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES. Son deberes de los profesionales de quienes trata este Código para con la dignidad de sus profesiones:

b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones;

3. Deberá buscar la noticia del caso “OPERACIÓN ANDROMEDA BUGGLY” en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.

El caso “OPERACIÓN ANDROMEDA BUGGLY”, cuyo lema era “Queremos enseñar y aprender”, creada en el año 2014 de forma Legal con el único propósito “adquirir conocimientos de informática del hacking ético”; sin embargo, las implicaciones Legales y éticas de este suceso que puso al país y fuerzas militares en las pantallas por un tiempo y se evidencian cuando el jefe de inteligencia del Ejército, general Ricardo Zúñiga, negó la existencia de esa central; sin embargo de manera casi simultánea fue retirado de su cargo al igual que otros integrantes y empiezan a destaparte las ollas.

Es importante mencionar que producto de las investigaciones, testimonios y pruebas halladas se encuentra que:

1. No se realizan estudios de seguridad para la selección de los agentes que integrarían la operación

2. Ausencia de supervisión en las actividades desarrolladas por los integrantes de la operación, teniendo en cuenta que estos estaban dotados con amplios conocimientos en Seguridad de la información.

3. Teniendo en cuenta que la información que se manejaba dentro de la operación era sensible, el equipo carecía de control y disciplina para recibir visitantes o nuevos integrantes lo que se convirtió en una gran falla a nivel de seguridad de la información y su principio de confidencialidad.

En virtud de lo anterior se puede hablar de una violación a los siguientes artículos de la ley 1273 de 2009:

- ✓ Artículo 269A: Acceso abusivo a un sistema informático.
- ✓ Artículo 269C: Interceptación de datos informáticos.
- ✓ Artículo 269E: Uso de software malicioso
- ✓ Artículo 269F: Violación de datos personales.

Informe de herramientas y procedimientos utilizados para dar solución al escenario de Red Team de acuerdo con los pasos del pentesting.

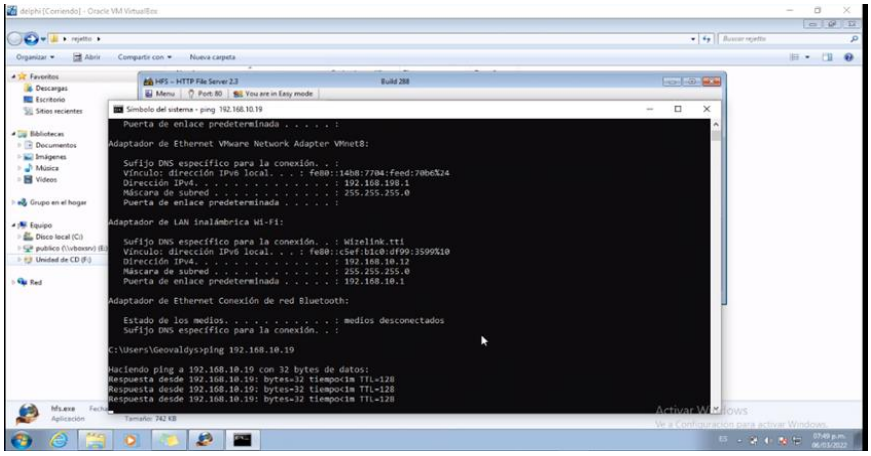
Contacto: El equipo Red Team de la compañía hará uso de la aplicación llamada Rejetto v. 2.3 bajo un windows 7 con arquitectura X64, una MV Kali Linux para efectos de investigar una presunta fuga de información por lo que se hace necesario explotar las vulnerabilidades.

Recolección de información:

Partiendo de la instalación del banco de trabajo de rejetto 2.3 (HTF – HTTP File Server) el cual fue instalado sobre una máquina virtual (ver imágenes), se instalarán los siguientes sistemas operativos: Windows 7 de 32 bit, Kali Linux

En la figura 1. Se puede observar como verificar el direccionamiento IP haciendo uso del comando **ipconfig**

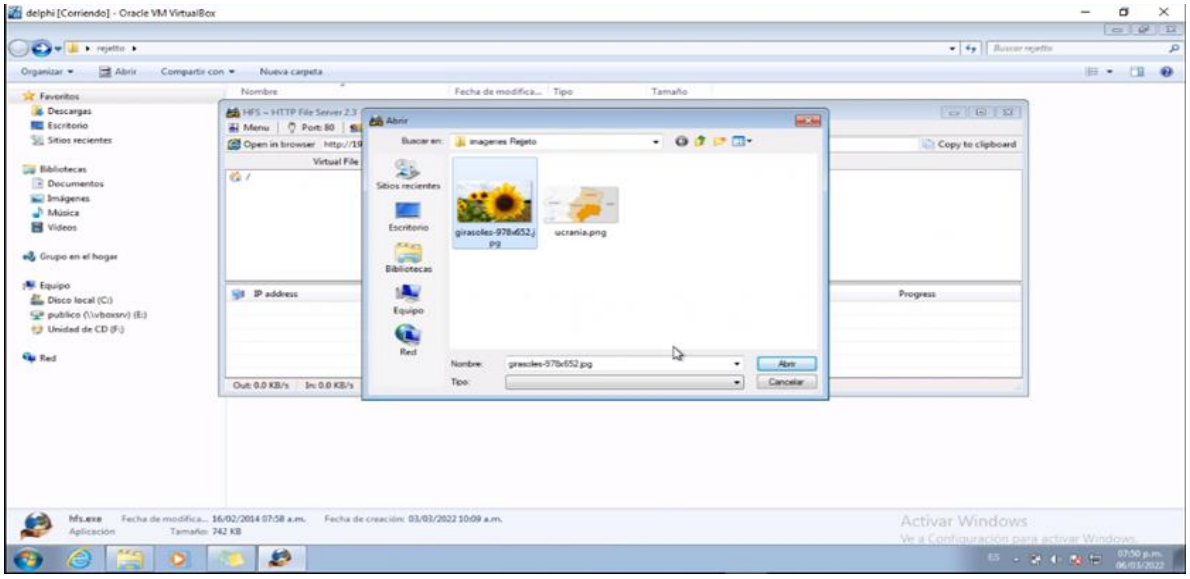
Figura. 1. Comando Ipconfig



Fuente El autor

En el Rejetto se encuentran fichero o imágenes como se pueden obervar en la Figura 2 a continuacion.

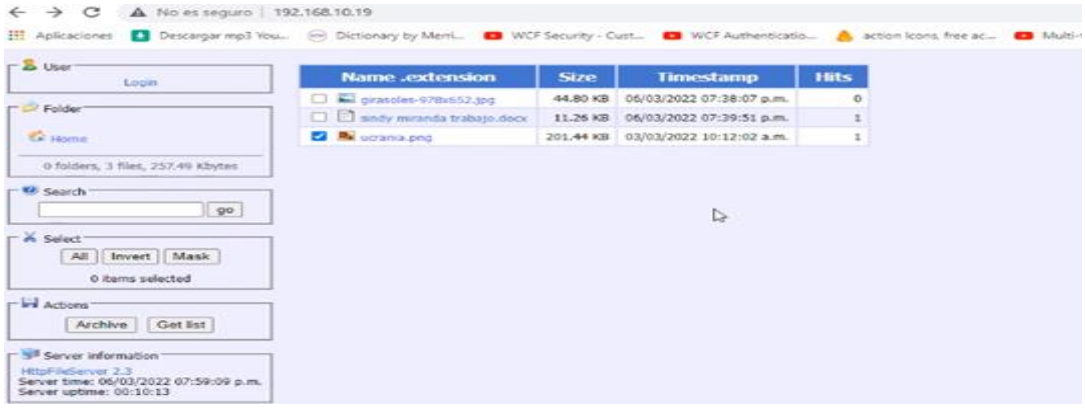
Figura. 2. Imágenes cargadas en Rejetto



Fuente El autor

Acceder a las imágenes de Rejetto es muy sencillo y esto se puede evidenciar observando la Figura 3 , donde se listan los archivos cargados en el mismo.

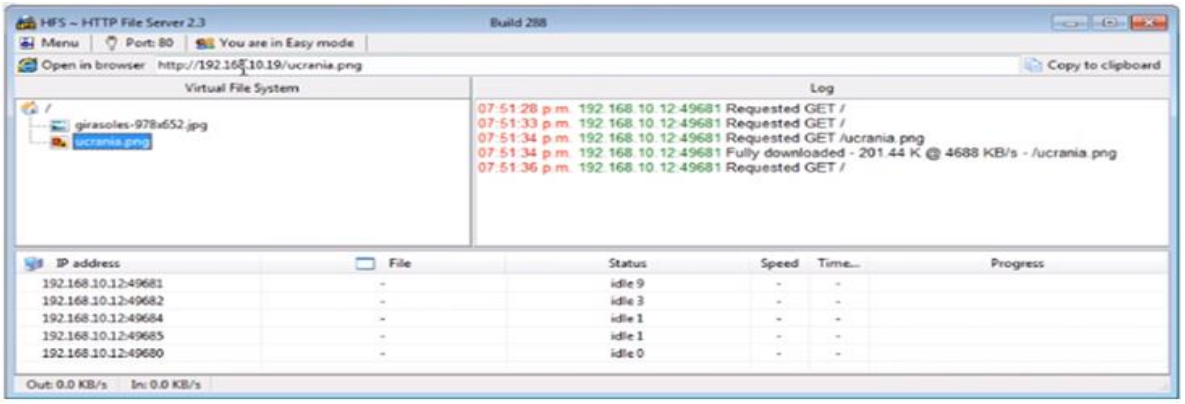
Figura. 3. Acceso a las imágenes de Rejjeto



Fuente El autor

No solamente se pueden obervar los archivo , sino que la Figura 4 accediendo a cada imagen brinda un detalle de su cargue.

Figura 4. Acceso a imagenes



Fuente El autor

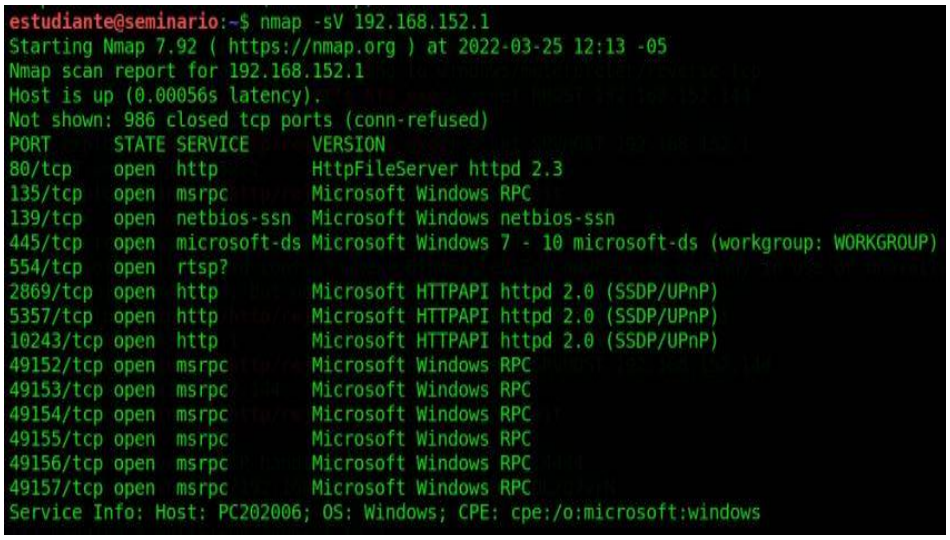
Modelado de la Amenaza

Para realizar el Escaneo se utilizará la herramienta NMAP sobre la máquina de Kali Linux, cuya dirección IP se obtiene con **inet addr y con** NMAP a partir del comando **sudo nmap –sP** se da inicio al escaneo.

Uso de la máquina virtual Kali Linux.
Primero verificamos cual es la ip asignada a la máquina virtual UBUNTU, para después colocarla en la dirección del Kali y verificar el alcance del servicio XAMPP para ello es necesario utilizar el comando ifconfig como se ve en la Figura 5.

Estando en la máquina virtual Kali, buscamos las herramientas de exploración y allí seleccionamos NMAP, Iniciando el escaneo, su ejecución se puede observar la Figura 5.

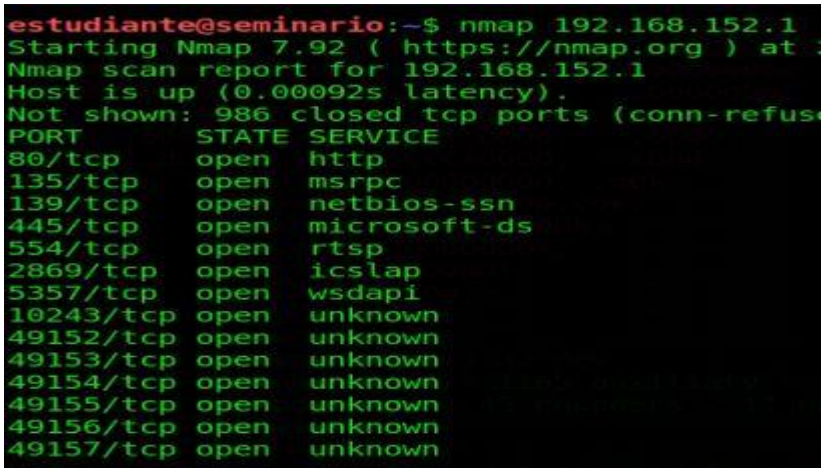
Figura .5. NMAP



Fuente El autor

Gracias a este completo escaneo es posible identificar que puertos se encuentran abiertos, es necesario observar la figura 6 donde se observa nombre del puerto y estado

Figura 6. Puerto abierto



Fuente El autor

Teniendo en cuenta que la función de NMAP es escanear puertos, puede realizar incluso un inventario de la red para comprobar que servicio se encuentra elevado; se afirma en este momento que el puerto 80 se encuentra abierto.

Análisis de Vulnerabilidad

Tener puertos abiertos en una red amenaza la confidencialidad, integridad y disponibilidad de la misma ya que es tener la puerta abierta a un intruso que puede ejecutar cualquier tipo de acciones para acceder a información,

Acceder a el equipo de Windows 7 objeto del presente trabajo permitió escuchar un puerto, si bien no todos los puertos son un riego pueden explotar vulnerabilidades como Accesos no autorizados, Vulnerabilidades de red expuesta, Ataques de denegación de servicio

Explotación

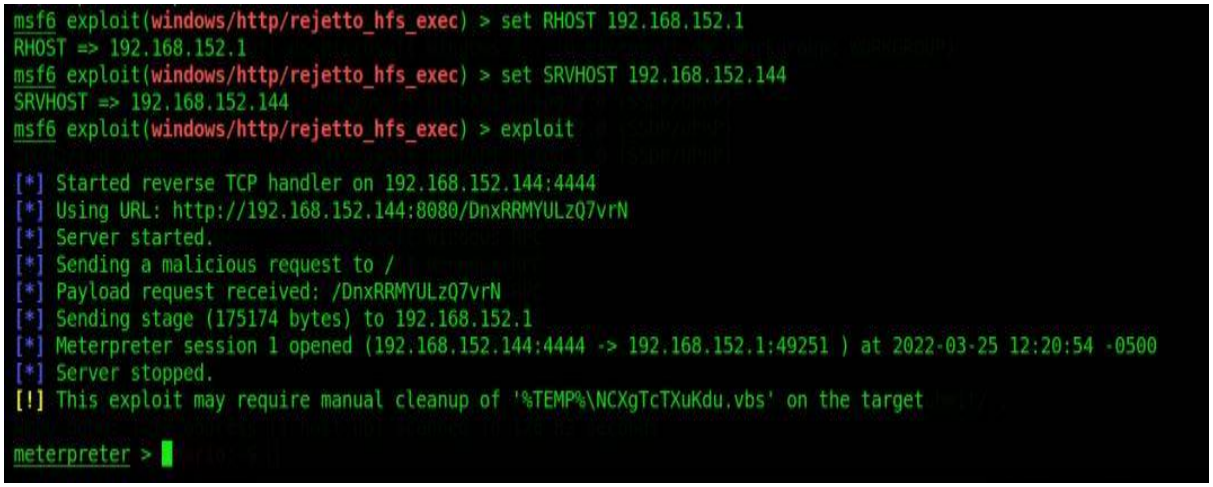
Ejecución del Metasploit Framework en Kali Linux a partir del comando:

exploit/Windows/http/rejetto_hfs_exec

Para realizar el exploit se ejecuta el comando: **Exploit**

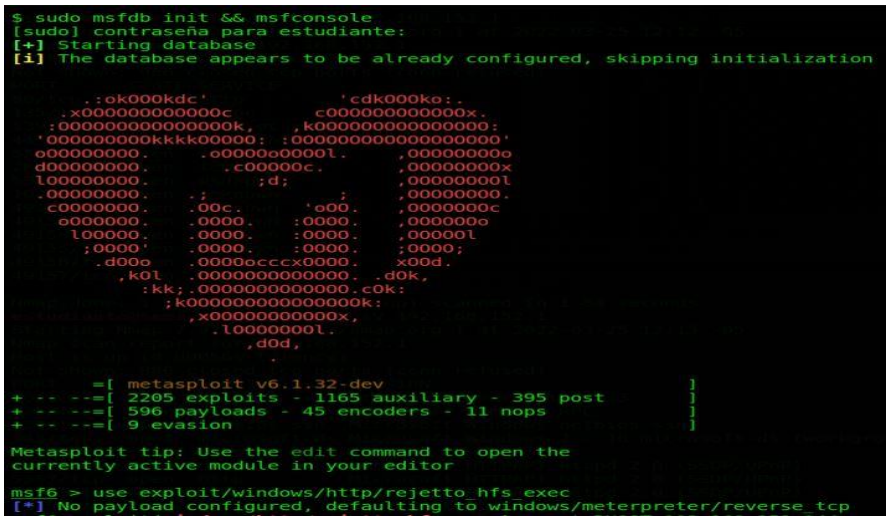
Su propósito conectarse con la maquina víctima y abre una sesión de meterpreter, es necesario para esto visualizar la Figura 7 y 8.

Figura 7 Ejecución



El equipo víctima de nombre SRVHOST

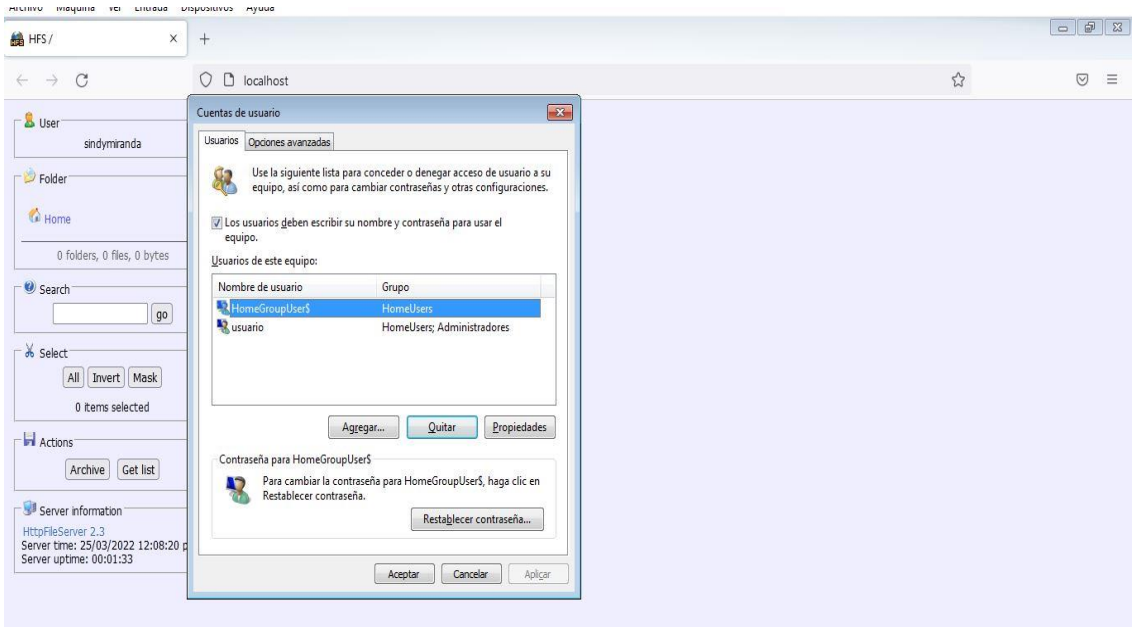
Figura 8. Ejecución Exploit



Fuente El autor

Acto seguido crear un usuario, el cual tendrá como nombre sindymiranda ejecutando el comando: **net user sindymiranda /add;** sin embargo es necesario validar que no existe dicho usuario en la figura 9.

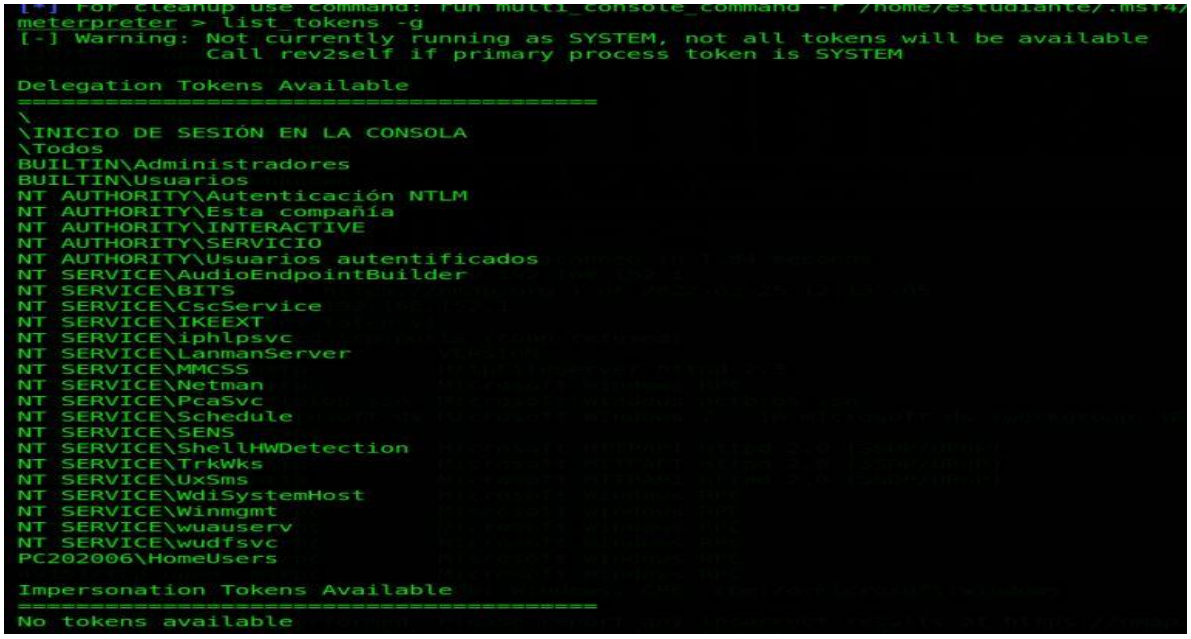
Figura 9. Pre creación de usuario



Fuente el autor

El equipo tiene la labor de asignar el usuario a crear al grupo de administradores, por lo que se muestran los grupos de usuario en la Figura 10.

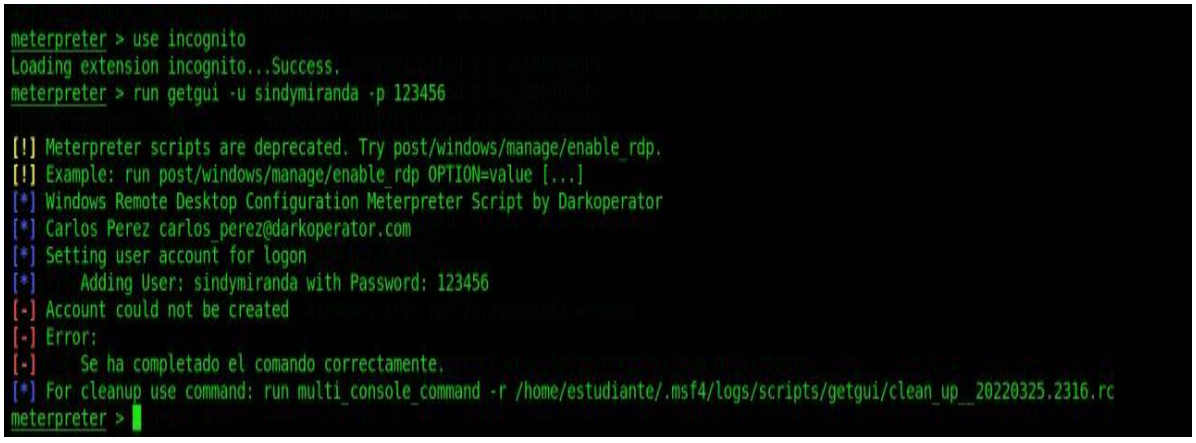
Figura 10. Grupos de usuario



Fuente el usuario

A continuación, el procedimiento para la creación de usuario sindymiranda

Figura 11. Usuario sindymiranda



Fuente el usuario

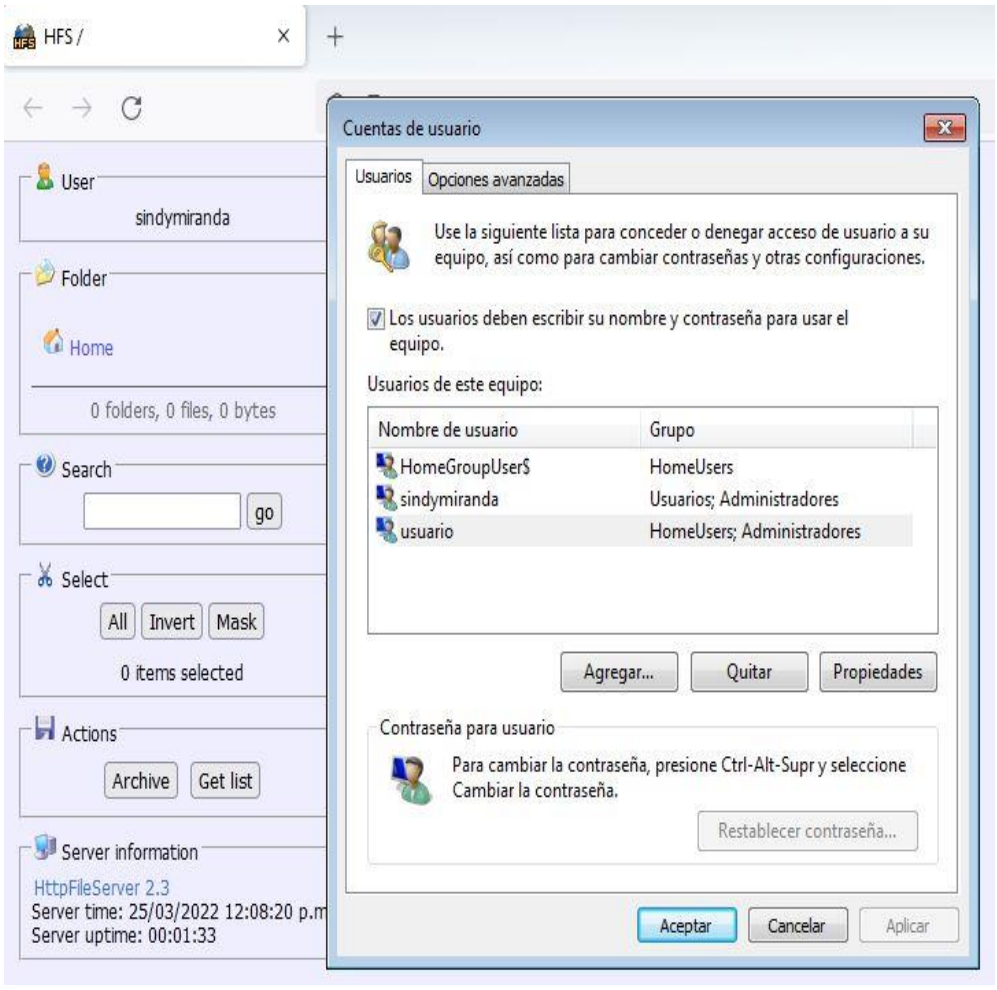
Agregar privilegio de administrador es posible a partir del comando add_localgroup_user.

Figura 12. Asignar permiso

Fuente el usuario

Evidencia de que el usuario **sindymiranda** ha sido creado, a partir de la Figura 13

Figura 13 **Pos creación de usuario**



Fuente el usuario

Desde el Windows 7 podemos ir a **Panel de control - Cuentas de usuario - Administrar otra cuenta**

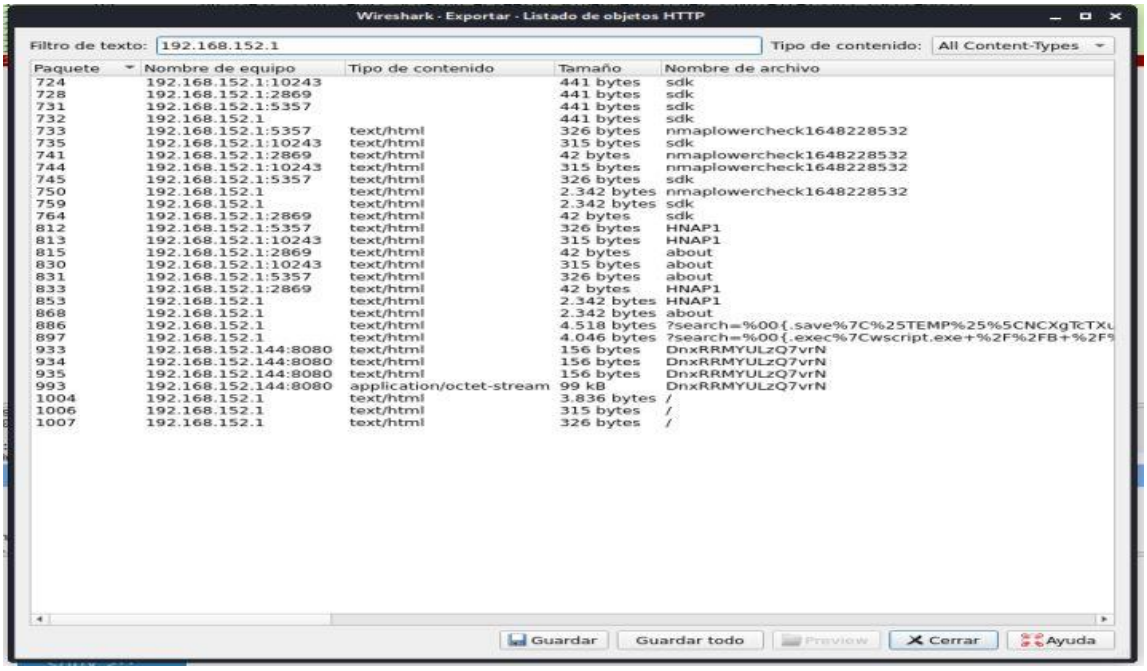
Post- explotación

Con la realización de los pasos descritos anteriormente se puede comprobar que el exploit cumplió el cometido y que la vulnerabilidad permitió acceder al equipo Windows 7 y crear un usuario administrador.

Wireshark fue la herramienta utilizada para análisis de tráfico, maquinas con mas interación en este caso la víctima y el servidor atacante; Por último el Frame que fue capturado.

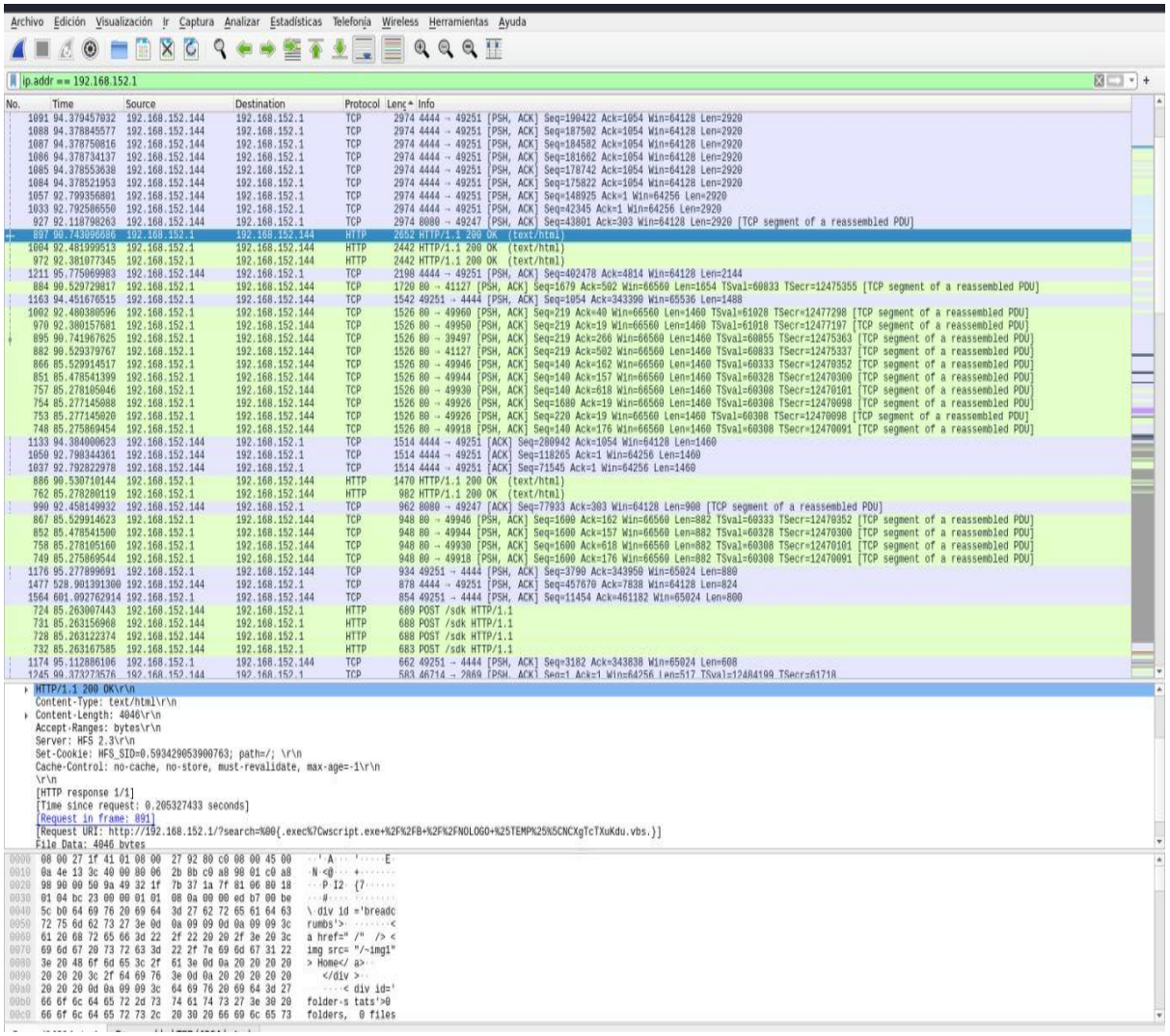
En ese orden es posible observar dicho análisis en las figuras 14, 15 y 16.

Figura 14. Verificación Paquetes transferidos



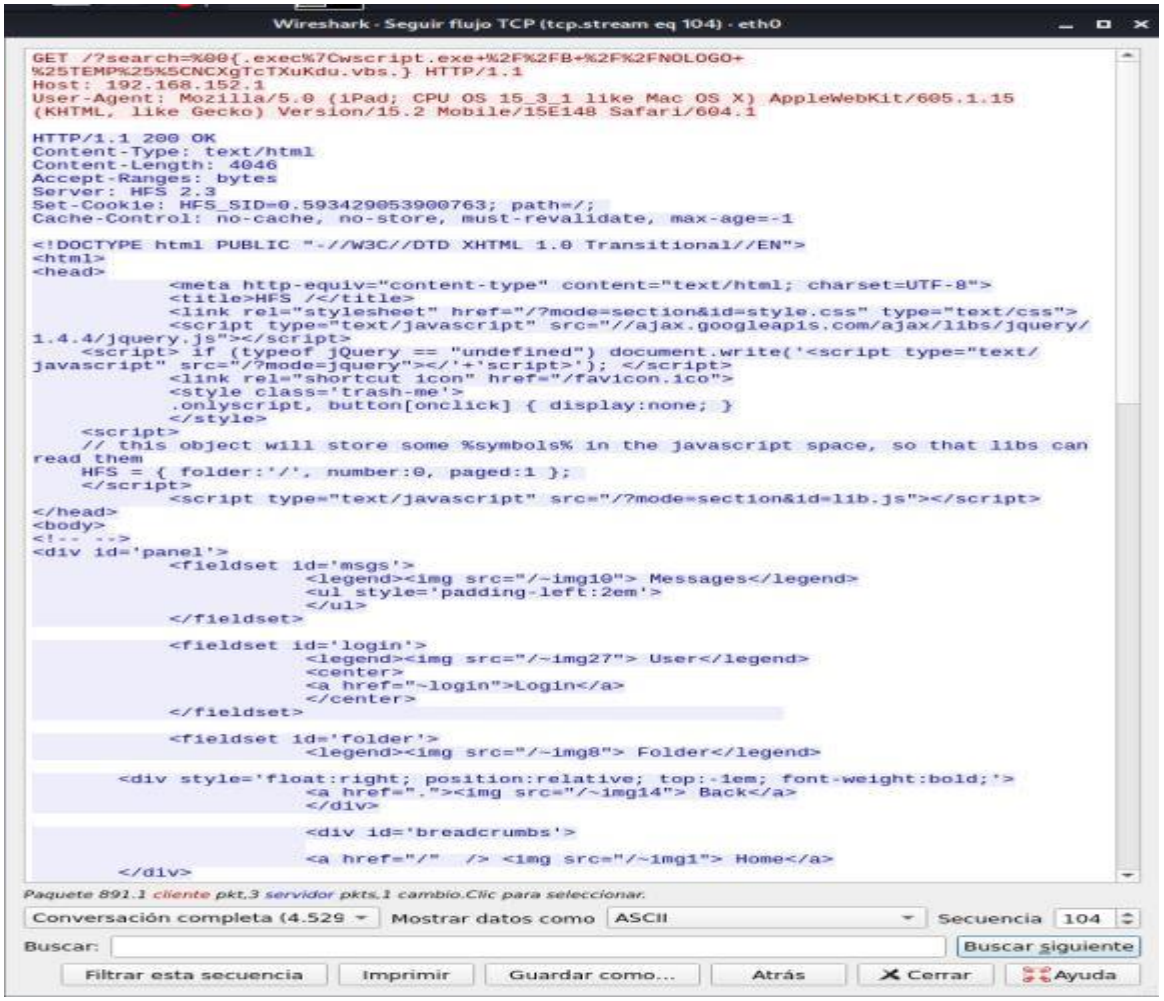
Fuente el usuario

Figura 15. Scrip Capturado



Fuente el usuario

Figura 16 – Analisis Frame Capturado



Fuente el usuario

Informe

Para el desarrollo de la actividad fue relevante conocer la información preliminar aportada por la organización aspecto que se encaja en la parte inicial llamado contacto que para efectos de este informe fue un documento, ejecutados los pasos de un pentesting se logró confirmar que la máquina de Windows 7 es afectada con la obtención de información y elevación de privilegios toda vez que el escaneo de puertos a partir de la herramienta NMAP determina que el puerto 80 es una puerta abierta para que puedan irrumpir en la seguridad.

Argumentos Técnicos ante un ataque en tiempo real

Conocedora de las funciones de un BlueTeams y desde mi rol como integrante de este, es importante mencionar algunas de ellas que serán la base para abordar la situación planteada. Establecer medidas de seguridad alrededor de los activos clave más importantes para una organización, permite tener plenamente identificados los activos críticos, y por ende las consecuencias que sufriría la organización si alguno de ellos falla. La evaluación de Riesgo periódicas nos permite identificar las amenazas contra cada activo, priorizarlas y elaborar con ello un plan de acción para establecer controles que reducen el impacto de cada amenaza. Habiendo dicho esto, teniendo claro el objetivo de WhiteHouse Security, como miembro del equipo y en procura de proteger los activos de la empresa las acciones a realizar serían las siguientes:

- ✓ Activar los protocolos alrededor de cada activo crítico.
- ✓ Aislar los activos críticos mencionados inicialmente de la red y/o de la fuente del ataque en curso en este caso equipo con sistema operativo Windows 7.
- ✓ Documentar cada detalle del evento.
- ✓ Ejecución del plan de acción para Mitigar el impacto y trabajar para la recuperación del sistema, operando por un canal de respaldo garantizando con esto la disponibilidad de la información.

Propuestas de medidas de hardenización para un ataque no se repita

Hadernizar o endurecer las medidas de seguridad es la necesidad de toda organización más cuando es víctima de un ataque informático, en esta oportunidad teniendo en cuenta las condiciones actuales en las que se produjo el ataque, se listan algunas recomendaciones o medidas que se propone implementar en WhiteHouse Security:

✓ Instalar en el 100% de las maquinas un Sistema Operativo reciente y con los parches de seguridad.

✓ Adquirir y configurar WSUS para monitorear que todas las maquinas cuenten actualización del sistema operativo

✓ Adquirir, Instalar y monitorear un Antivirus que contenga las ultimas bases de amenazas para que todos los equipos se encuentren protegidos.

✓ Proteger la red con un FORTINET para filtrar el tráfico, restringiendo sitios no seguros y que los usuarios de la organización navegación hacia paginas previamente filtradas.

✓ Definir usuario y clave de Administrador local SEGURA conocida únicamente por el equipo de Tecnologías (Líder y Encargado de instalar software)

✓ Instalar un Agente de inventario que permita monitorear el Software instalado en cada máquina Ejemplo OCS

✓ Escanear los puertos y cerrar los que no van a ser utilizados por los procesos del usuario para evitar el acceso a cualquier atacante.

✓ Definir un proceso para el software autorizado

✓ Definir y ejecutar auditorias periódicas.

✓ Implementar un servidor de dominio Active Directory, el cual permitirá gestión de usuarios, Roles de usuarios, Cambios de contraseñas de forma periódica y segura.

✓ Definir Política de bloqueo de Puertos, Lectura de CD y DVD

✓ Políticas:

A continuación, en la Tabla 1 se listan un compendio de políticas que deben ser implementadas en la organización

Tabla 1. Listado de Políticas

NOMBRE DE LA POLITICA	DESCRIPCION
Política de Seguridad de la Información	Establecer lineamientos que permitan resguardar la información y los recursos destinados para su gestión y consumo. Lo anterior liderando y fortaleciendo la seguridad y privacidad de la información a partir del acceso, uso y apropiación de la información teniendo en cuenta los requisitos legales de la entidad y las obligaciones contractuales de quienes la manipulan ya sean colaboradores, proveedores y partes interesadas.
Política de clasificación de información	Define los lineamientos y mecanismos para una adecuada clasificación y manejo de la información teniendo en cuenta el tipo, medio e importancia. La información puede ser Publica, de uso interno, Restringida y Confidencial y su almacenamiento varía según su calificación ya que una organización puede contar con documentos digitales, documentos en papel,

	Sistemas de información , Correos Electrónicos, Información almacenada en Discos Externos, USB, y por último y no menos importante información verbal de conocimientos del personal que interactúa con ella.
Política de protección de datos	Define los criterios para la recolección, almacenamiento, Uso y protección de los datos teniendo en cuenta su nivel de criticidad. Para ello se tiene en cuenta la legislación: Constitución Política de Colombia, artículo 15. Ley 1266 de 2008, en la que se dictan las disposiciones generales de habeas data y se regula el manejo de la información contenida en las bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Las instrucciones impartidas por la Superintendencia de Industria y Comercio en ejercicio de la función establecida en el artículo 21 de la Ley

1581.

Política de destrucción de información	A través de esta política el CSIRT define sobre la periodicidad de destrucción de la información. Se debe disponer de un documento avalado por la alta dirección y de conocimiento de la organización que describa de forma clara el periodo de destrucción de cada Tipo de información.

Política de retención de información	A través de esta política el CSIRT define sobre la retención de la información garantizando que esta esté disponible según su ciclo de vida. Para garantizar la conservación, se hace necesario disponer de un anexo que describa el Tipo de información y el tiempo en años de conservación y utilidad. La información se divide en cuatro categorías generales: (1) Información que legalmente debe ser conservada por periodos de tiempo prescritos, (2) Información necesaria para la operación del negocio y proyectos. (3) Información incidental y de otros tipos generada en el curso del negocio. (4) Información personal o no relacionada con el negocio.
Política sobre el acceso a la información	A través de esta política el CSIRT define sobre el acceso de la información teniendo en cuenta el tipo de usuarios.

	Para asegurar el acceso se implementa un controlador de dominio que permita gestionar los usuarios, su acceso y permisos sobre las máquinas y sistemas de información de acuerdo con su rol. A través del Log es posible auditar los accesos.
Política de capacitación y entrenamiento.	Define lineamientos para Uso y apropiación de información a los usuarios del CSIRT sobre temas de interés.
Política de copias de seguridad.	Procedimiento para realización de Copias de seguridad de la información relevante.
Política de gestión de contraseñas	La política establece el procedimiento para asignación de contraseñas, condiciones para contraseñas seguras.
Política de uso de correo electrónico	La política establece los criterios de utilización del correo electrónico por los destinatarios, con el fin de garantizar su uso correcto. Informar de las obligaciones que asumen como consecuencia de su uso.
Política de seguridad de la red.	Define los lineamientos para prevenir accesos no autorizados a la red garantizando la seguridad la seguridad

	de la red.
Política de Definición de incidentes, Vulnerabilidades y Eventos	Esta política describe los criterios que determinan la definición de una incidencia, vulnerabilidad o evento y su clasificación según su prioridad.
Política de Gestión de Incidentes y Vulnerabilidades	La política define como se gestionará un incidente o vulnerabilidad, los tiempos de respuesta y procedimiento a aplicar
Política de gestión de riesgos:	Identificación y mitigación de que un riesgo se materialice.
Políticas de gestión de activos	Mantener la protección adecuada de los activos de información de las empresas
Política de licenciamiento de software	Documentar la regulación de las licencias usadas por las empresas
Política de cumplimiento:	Documentar la política de cumplimiento de los servicios y establecer las sanciones legales del no cumplimiento, establecidas en la constitución colombiana
Política de seguridad física de en las instalaciones:	Mantener una adecuada protección de física de equipos, transmisión e integridad de la información y el soporte adecuado del procesamiento

	de esta
Política de control de acceso lógico:	Proteger los sistemas de la empresa teniendo en cuenta los perfiles, permisos, cuentas, contraseñas y protectores de pantalla
Política de adquisición, desarrollo y mantenimiento de sistemas	Documentar las normas y procedimientos que se aplicaran en el ciclo de vida de aplicativos, equipos e infraestructura de la empresa
Política de gestión de servicios:	Documentar los lineamientos necesarios que permitan evaluar cómo se realiza la gestión y el soporte de los servicios tecnológicos de las empresas.

Fuente El autor

Es importante mencionar que los atacantes siempre están trabajando y la labor de toda organización es entender que la seguridad es dinámica por ello de manera continua deben fortalecer la seguridad de sus sistemas para que si bien con ellas no salga ileso si pueda tener la capacidad de recuperarse mucho más rápido y el impacto del presunto ataque se reduzca. Si bien el Anexo 5 enfatiza en que no se cuenta con presupuesto, el equipo cumpliendo con su función aporta las sugerencias para su futura adquisición y una concientización en el ejercicio actual.

Diferencias entre un equipo blue team y un equipo de respuesta a incidentes informáticos

Un CSIRT se traduce en una serie de ventajas competitivas entre otros controles más eficientes en la organización, optimización de tiempo para restaurar los servicios, Mejor productividad y niveles de satisfacción de usuarios, optimización en el uso del personal, posibilidad de crear base de conocimiento y que pueda estar disponible para otros clientes que enfrenten los mismos incidentes o vulnerabilidades. Para su correcta operación los CSIRT deben estar lo suficientemente preparados para atender situaciones críticas, realizar acciones preventivas y actuar de manera rápida. La Ciberseguridad y los CSIRT son temas de tendencia y de gran importancia para las organizaciones que se han interesado por el tema de la Seguridad consientes de los grandes riesgos a los que se deben enfrentar como resultado de su posicionamiento en un mercado interconectado. Dicho de otra forma, un Equipo de Respuesta de incidentes es un grupo cuyo servicio es prestar soporte para prevenir, gestionar y responder ante un incidente de seguridad de la información. BlueTeams también es un equipo conformado por expertos en Ciberseguridad cuya función es defender a las organizaciones de ataques, a diferencia del anterior este únicamente actúa de forma defensiva, realizan monitoreo constante y trabajan en la Mejora continua. Su propósito se cumple en la medida que identifican vulnerabilidades y las ponen al descubierto, se caracterizan por detectar las vulnerabilidades con rapidez, estudiar a los atacantes y su comportamiento, utilizar señuelos para llevar a cabo su misión.

CIS “center for internet security” dentro de un equipo blue teams

Entendiendo que CIS son un conjunto de mejores prácticas en seguridad Cibernética y que actúa bajo el principio de la DEFENSA, se convierte en un gran aliado para un Blue Teams para alcanzar sus objetivos La claridad con la que está definido un CIS le permitirá a BlueTems realizar sus auditorías y análisis de forma

más sencilla y sobre todo respetando los lineamientos legales. Las buenas prácticas a las que se refiere CIS serán útiles para el equipo azul quien podrá enfocarse de manera efectiva en mejorar la defensa de la organización ante ciberataques. Ajustado a las recomendaciones brindadas en el punto anterior, por ejemplo, las buenas prácticas reforzarían la elaboración e implementación de un compendio de políticas de seguridad.

Funciones y características principales de lo que es un SIEM.

Un SIEM es una herramienta que brinda respuesta inmediata y eficiente a una organización que enfrenta un ataque a los sistemas. Su función principal es lograr gracias al monitoreo, recopilación de información la detección eventos sospechosos en tiempo real, lo que hace que su acción sea inmediata y permite minimizar sus consecuencias. Debido a que actualmente grandes, medianas y pequeñas empresas están igualmente expuestas debido a su dependencia de la tecnología, estos serían los beneficios que le aportaría un SIEM Respuesta rápida y efectiva a amenazas Control total de los eventos Detección temprana de posibles amenazas Mantener a salvo sus activos ante ataques externos Como quiera que SIEM se implemente en una organización serán muchas las ventajas para esta en materia de Seguridad, costos, Capacidad de respuesta y confianza para los usuarios. Características:

✓ Trabaja en tiempo real por lo que tiene alto grado de reacción

✓ Identifica entre amenazas reales y falsos incidentes.

✓ Monitorea de forma centralizada todas las amenazas potenciales.

✓ Redirecciona u orienta la actuación a personal cualificado para resolverlas.

✓ Aporta alto grado de conocimiento sobre los incidentes para facilitar su resolución.

✓ Documenta todo el proceso de detección, actuación y resolución. ✓ Cumple con las normas y legislaciones vigentes en cuestión de protección de datos y seguridad.

Herramientas de contención de ataques informáticos “hardware o software”.

Antes de mencionar herramientas de contención es importante comprender que contener busca evitar que una amenaza se propague.

Firewall - FortiGate Mantiene seguras las redes corporativas de una forma unificada, integral y automatizada, a través de su hardware y software, permiten Gestionar Amenazas, actúan como firewalls, detección de intrusiones, filtrado web y protección contra un programa maligno o correos no deseados. No solo brinda seguridad a la red sino, acceso seguro, Seguridad física y virtual, de aplicaciones, Protección de dispositivos.

Antivirus Disponer de un antivirus permitirá la detección, bloqueo y denegación a actividades sospechosas o ejecución de programas no autorizados, gracias a una base de datos actualizada permitirá a la organización evitar eventuales ataques o intrusiones.

Controles de acceso Este método de contención física permitirá mantener a salvo los equipos activos del acceso a terceros sin autorización a un centro de datos.

CONCLUSIONES

La necesidad por seguir comunicados y disfrutando de las ventajas de poder realizar trámites de forma virtual sin filas y desplazamientos son algunas de las razones por las cuales seguiremos dependiendo del internet.

Las empresas continuarán soportando sus procesos en herramientas tecnológicas.

Los ciberdelincuentes por su lado seguirán perfeccionando ataques persiguiendo cada avance tecnológico con una acción delictiva

En virtud de lo anterior, se hace necesario que las empresas puedan pensar en implementar técnicas de pentesting que les permita enfrentar los incidentes de seguridad y poder evitar algunos de ellos.

Colombia ha avanzado en la prevención de delitos cibernéticos desde dependencias del gobierno como Política Nacional de Seguridad Digital y su COlCERT.

Un evento como la Operación Andrómeda, fachada de la Central de Inteligencia Técnica del Ejército Nacional claramente dejo en entredicho el rol de los dirigentes del país en la línea delgada entre lo legal y lo ético. Lo realmente polémico es que este caso que inicialmente fue descrito como un ‘hackerspace’ inocente. ‘Bender’ creado por un cabo del Ejército Nacional era toda una operación robusta con suficientes recursos económicos que le permitían a este grupo de aparentes jóvenes curiosos de la seguridad informática llegar a objetivos como los grupos armados (ELN y FARC); fueron capaces de infiltrarse y obtener información de alto valor incluso se presumió que tuvieron acceso a archivos del proceso de paz.

En el anterior seminario, se realizaron prácticas de intrusión y vulneración a sistemas conectados a la red con dos distribuciones sobre máquinas virtuales diferentes, en donde se pudo obtener de la maquina victima información sensible

(fuga de información a partir de puerto en estado open) con ayuda de herramientas del SO Kali Linux, NMAP y Exploit y que de ser usadas de manera no autorizada más adelante que puede poner en riesgo la integridad de una empresa, organización o compañía.

Lo descrito nos lleva a confirmar que la interconexión tecnológica expone a las organizaciones a un sin número de ataques para vulnerar la seguridad informática y como expertos en Seguridad informática nos corresponde buscar prevenir y/o contener este tipo de sucesos. La protección de los activos es la misión y para ello Bue Team aplica técnicas para detectar, explotar y dar solución al manejo de los incidentes de Seguridad. Con el desarrollo del presente trabajo se brindaron las orientaciones correspondientes para que la compañía WhiteHouse Security cuente con las herramientas necesarias para contener un ataque en tiempo real y ofrezca la continuidad de sus servicios.

ENLACE DEL VIDEO

https://drive.google.com/file/d/16nw0-9oUOa6bJ7zX0R4pdQS8HLRYXtU7/view?usp=sharing

RECOMENDACIONES

Decidir formarse como experto en seguridad informática es una responsabilidad con el mundo y debido que es una labor sensible un profesional de esta área debe:

Documentarse en la más reciente legislación sobre la Ciber Seguridad y desarrollar habilidades en esta área que le permitan blindarse de los riesgos propios de su misión.

Entender que las acciones de un experto en Seguridad son tan importantes que requieren del componente Jurídico permanente para hacer que su intervención en una organización realice un aporte integral.

Preparar escenarios de pruebas limpios que permitan no solo escenarios seguros sino evitar posibles problemas legales por malos procedimientos.

Documentar cada acción mediante actas de reunión, Autorizaciones, Procedimientos entre otros, dan cuanta de la trasparencia de un experto en Seguridad y a la vez en caso de algún inconveniente futuro mantener organizados y conservados dichos soportes serán material probatorio utilizado para su defensa.

No omitir lineamientos de seguridad hace parte de la ética de un profesional y protege tanto su hoja de vida como las organizaciones que represente

BIBLIOGRAFIA

PIÑARREDONDA, José Luis “Detrás de Buggly: la historia de la fachada Andrómeda". {En línea}. {9 diciembre de 2015} disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda

GARAVITO, Cristian “Caso Andrómeda y sus interrogantes”. {En línea}. {4 enero de 2018} disponible en: https://www.elespectador.com/judicial/caso-andromeda-y-sus-interrogantes-article-731765/

GUTIÉRREZ, José Antonio “El informe que sacudió el caso de la fachada Andrómeda” {En línea}. {24 enero de 2015} disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

DUEÑAS, Mauricio “Andrómeda, la sala de inteligencia que enreda al Ejército”. {En línea}. {4 febrero de 2014} disponible en: https://www.elespectador.com/judicial/andromeda-la-sala-de-inteligencia-que-enreda-al-ejercito-article-472918/

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Enero, 2009. Nro. 47223. p.5.

LESAND. Ataque a Windows 7 con Metasploit Kali Linux. 2019. Disponible en:

https://www.lesand.cl/foro/ataque-windows-7-con-metasploit-kali-linux

JASWAL. Nipun. Vulnerability analysis of HFS 2.3. En: Mastering Metasploit. 2a. ed. 2016. Disponible en:

https://subscription.packtpub.com/book/networking_and_servers/9781786463166

INFOLAFT. Anticorrupción, fraude y LA/FT. ¿Qué hacer antes, durante y después de un ataque informático?.2014. Disponible en: https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

CIBERSEGURIDAD.NE Las fases de un test de penetración (Pentest) (Pentesting I) Disponible en: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

MANAGEENGINE BLOG Descubra las amenazas de los puertos abiertos y mejore la seguridad con las herramientas de análisis de puertos https://blogs.manageengine.com/espanol/2021/07/07/descubrimiento-amenazas-puertos-abiertos-htas-analisis-puertos.html

THEBRIDGE, ¿Qué es un Blue Team? {En línea} {19 octubre de 2021} disponible en https://www.thebridge.tech/blog/que-es-un-blue-team

MANAGEENGINE, ¿Qué son los controles de CIS®? {En línea} {19 octubre de 2020} disponible en https://www.manageengine.com/latam/controles-de-seguridadcritica-cis.html

UNIR, Red team, Blue team y Purple team, ¿sabes qué son y cómo ayudan a mejorar la seguridad informática? En UNIR abordamos sus funciones y objetivos. {En línea} {19 octubre de 2020} disponible en https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

IT DIGITAL SECURITY ¿Qué es un Blue Team y cómo trabaja? {En línea} {30 mayo de 2018} disponible en https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-comotrabaja.

AMBIT, ¿Qué significa SIEM y cómo funciona? {En línea} {30 abril de 2020} disponible en https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-yc%C3%B3mo-funciona

IT GOVERNANCE, What is Cyber Security? Definition and Best Practices {19 marzo de 2022}, disponible en https://www.itgovernance.co.uk/what-is-cybersecurity.