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

GAMALIEL MUÑOZ IMBACHI

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI-ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2022

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

PRESENTADO POR:
GAMALIEL MUÑOZ IMBACHI

PRESENTADO A:
LUIS FERNANDO ZAMBRANO HERNANDEZ
DIRECTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTA ROSA DE VITERBO
2022

RESUMEN

Por medio del presente documento se realiza el presente resumen de las anteriores etapas que se desplegaron a lo largo del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team identificado con código de Nro. 202337164, donde se evidencia y se plantea las respuestas a los diferentes interrogantes planteados por medio de las diferentes guías y rubricas de las unidades de la uno a la cuarta e incluso a esta que se tipifica como etapa cinco.

Actividades que se desarrollaron a lo largo del seminario por parte de un estudiante de la especialización en seguridad de la información, actividades con las cuales se amplía el conocimiento y se afianza para en un futuro como experto y especialista se debe tener presente para el desarrollo de las diferentes actividades a desplegar, toda vez que es constante la actividad de amenaza, vulnerabilidad en las que se observan inmersas las empresas sin discriminar sus actividades o productos.

El futuro profesional de seguridad de la información debe manejar las diferentes herramientas tecnológicas puestas con fines de validar, identificar, llegar a comprender y buscar posibles soluciones a las problemáticas que se presentan en las organizaciones, es por ello la importancia que se le debe otorgar a los grupos expertos que se dedican a mantener las redes, los componentes tecnológicos, quienes recepcionan y atienden los diferentes incidentes informáticos.

Prevenir entre otros aspectos los accesos no permitidos, manejo de usuarios de dominio, usuarios administradores, entre otras actividades de la política de seguridad de la información que se debe implementar en la organización con fines únicos y exclusivos de evitar que se presente fuja de los activos de información, además que en caso de que se presente se debe recepcionar y atender, dejando los soportes y documentar para futuros ataques que se presenten.

PALABRAS CLAVES: Actividades, desarrolladas, mejora del conocimiento, apropiación de la temática, RED Team & Blue Team.

ABSTRACT

Through this document, the present summary of the previous stages that were deployed throughout the Specialized Seminar is made: Strategic Cybersecurity Teams: Red Team & Blue Team identified with code No. 202337164, where the answers are evidenced and proposed. to the different questions posed by means of the different guides and rubrics of the units from one to the fourth and even to this one that is typified as stage five.

Activities that were developed throughout the seminar by a student specializing in information security, activities with which knowledge is expanded and strengthened for the future as an expert and specialist should be kept in mind for the development of the different activities to be deployed, since the threat activity is constant, vulnerability in which companies are observed immersed without discriminating their activities or products.

The future information security professional must manage the different technological tools put in place in order to validate, identify, understand and seek possible solutions to the problems that arise in organizations, which is why the importance that should be given to the expert groups that are dedicated to maintaining the networks, the technological components, who receive and attend to the different computer incidents.

Prevent, among other aspects, unauthorized access, management of domain users, administrator users, among other activities of the information security policy that must be implemented in the organization for the sole and exclusive purpose of preventing the leakage of assets. of information, in addition that in case it occurs, it must be received and attended to, leaving the supports and documenting for future attacks that may arise.

KEY WORDS: Activities, developed, improvement of knowledge, appropriation of the theme, RED Team & Blue Team

ÍNDICE

Pág.

TABLA DE ILUSTRACIONES

Pág.

GLOSARIO

Vulnerabilidad: hace referencia a una posible falla dentro de un sistema de información, donde se evidencia las posibles falencias de las que se está inmerso el equipo sistema o cualquier componente tecnológico, evidenciándose que es viable realizar un ataque con éxito de fuja de información dentro de ese sistema.

Información: activo que no es tangible, donde se evidencia, datos ya sean personales, cuentas, datos de la empresa tanto privados, como públicos, entre otros que son de un valor incalculable y es deber de la organización su protección.

Delito informático: actividad que dentro de la justicia penal colombiana se denomina ilícita, que atenta contra un bien jurídico titulado como es el sistema informático, obteniendo de forma ilegal abusiva por parte del que vaya a vulnerar la información dentro de una organización.

Amenaza: es toda acción que se despliega por parte de los atacantes según las vulnerabilidades evidenciadas, además existen con fines de atentar contra los sistemas puestos en funcionamiento al servicio de la información de la organización.

Máquina virtual: software que permite la simulación de un sistema operativo, mediante el cual se puede laborar y ejecutar diferentes sistemas operativos dentro de una herramienta de cómputo.

METASPLOIT: se conoce como una herramienta que permite la utilización con el fin de realizar actividades de penetración o pentesting, además esta trabaja con sistema denominado Ruby, con el cual se puede realizar actividades de escribir, programar mediante código de explotación, de igual manera cuenta con una serie de diferentes herramientas, que permiten la verificación, de las vulnerabilidades de seguridad.

EXPLOIT: permite la verificación de diferentes vulnerabilidades en algunas aplicaciones, en los sistemas informáticos, en activos de información, el uso en algunas ocasiones se realiza de manera no autorizada.

Pentesting: es la actividad que se realiza con fines de penetrar en los sistemas informáticos, que permiten la verificación de las diferentes vulnerabilidades el riesgo y las amenazas que este posee o tiene.

Sistema operativo: es el software con el cual una herramienta de tecnología, computador, Tablet, smartphone, entre utiliza para dar inicio o arranque para presentar sus recursos ante algún usuario.

ENTORNO DE PRUEBA: es la actividad que se realiza ya sea en los simuladores o en entornos reales con fines de comprobar que riesgos, vulnerabilidades tiene un sistema informático o una herramienta de tecnología.

TICS: hace referencia a las diferentes tecnologías que se emplean con fines de la información además única y exclusivamente hacia las comunicaciones, que se emplean para las redes o lo que se denomina sistemas de información.

INTRODUCCIÓN

En las diferentes organizaciones se debe tener presente que las actividades se deben en caminar dentro de la prevención y conservación de los diferentes activos de la información, generando la necesidad de mantener de manera constante implementados métodos de seguridad informática, protección de la información ya sea física o electrónica, mediante los diferentes métodos efectivos de conservación a su vez generar copias de respaldo que contribuyan a la preservación de la información de la empresa.

El conocer como las instituciones coadyuvan a proteger los activos de información, mediante las evaluaciones que se realizan de las diferentes acciones que se ejecutan mediante los equipos Red Team y los de Blue Team, dentro de las cuales se evidencian tanto de marco legal como el ético, además poseen herramientas para poder mitigar el riesgo y las vulnerabilidades.

Dentro de las diferentes actividades desplegadas y realizadas a lo largo del seminario se puede evidenciar que efectivamente existen métodos, herramientas para verificar el riesgo, las vulnerabilidades y además como mitigarlas para así mejorar la seguridad tanto de los documentos, archivos, bases de datos que pertenecen a los activos dentro de una empresa.

JUSTIFICACIÓN

El crecimiento de las empresas, así como las nuevas tecnologías y comunicaciones ha revolucionado en el mundo, logrando que hoy en día, en la gran mayoría de las organizaciones, se encuentren procesos de automatización de labores, las nuevas tecnologías se posicionan cada vez más en el mundo empresarial de tal manera que hoy en día no sería posible ser competitivo a nivel empresarial sin ellas.

Además, se debe tener en cuenta que la información es un activo muy importante en toda empresa en los diferentes niveles, desde bases de datos, hasta movimientos financieros, podemos asegurar que se requiere un soporte a nivel tecnológico para cada dispositivo que hay dentro de la organización.

Puesto que los avances y requerimientos actuales son necesarios para asegurar el activo más valioso de cualquier negocio. La información y para ser efectivos en esta labor se requiere una serie de pasos organizados a nivel de ciberseguridad, con el fin de proteger y garantizar los objetivos organizacionales.

OBJETIVOS

1.1 Objetivos General

Estructurar mediante un informe escrito que permita de manera técnica a la organización la toma de decisiones, a su vez dar a conocer las estrategias por parte de los equipos tanto de BlueTeam como el de RedTeam, con la finalidad de identificar vulnerabilidades, riesgos y amenazas dentro de una organización.

1.2 Objetivos Específicos

- Identificación de la normatividad nacional e internacional, con el fin de realizar la plena verificación de vulnerabilidades, riesgos y amenazas dentro de una empresa, para que la organización tome las decisiones pertinentes según lo presentado.

- Validar las diferentes herramientas que son útiles para la verificación de vulnerabilidades dentro del sistema de una empresa, para que la misma desarrolle e implemente mejoras a la infraestructura que actualmente cuenta la organización.

- Analizar las herramientas o aplicaciones que permiten la mitigación de las vulnerabilidades de los riesgos, amenazas dentro de una empresa, con el fin de implementarlas a su vez que estás reduzcan los ataques a los activos de información.

DESARROLLO DEL INFORME

2 ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

Con el fin de generar respuesta a una serie de interrogantes que se plantean en la guía y rubrica de la UNAD de la presente unidad así:

3 DENTRO DEL MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES REDACTE CON SUS PROPIAS PALABRAS QUE LEGISLACIÓN "LEYES, DECRETOS" EXISTEN ACTUALMENTE Y LAS CARACTERÍSTICAS PRINCIPALES DE CADA LEY.

Con el fin de generar respuesta al presente interrogante es necesario dar a conocer que Colombia es un país que su Constitución Política[1] fue actualizada en el año de 1991; que es la norma de normas y que se conoce que sobre ella no hay ninguna otra norma que pueda sobre pasar la misma, es decir que no puede contradecirla y por el contrario se deben someter a ella, según lo manifestado en su artículo cuarto.

En su artículo 61 la Constitución Política de Colombia manifiesta mediante el estado debe proteger la propiedad intelectual, es por ello que se crea leyes en contra de delitos informáticos además de protección de datos personales, en caso de hacer uso de alguno de ellos se debe contar con la aprobación de sus autores, referenciar entre otras medidas.

Según lo manifestado por el artículo 74 en la Constitución Política de Colombia del año 1991 mediante el cual manifiesta "***que las personas tienen derecho a acceder a documentos públicos genera la excepción de los casos que establezca la ley"*** la interpretación de este artículo en mención es sobre la administración de recursos públicos es decir de aquellos que el estado posee y entrega a sus gobernantes mediante elección popular y no de actividades realizadas por particulares mediante una organización u empresa.

Además, es necesario manifestar que, aunque el uso de las redes sociales es público, este contenido que un particular publicó, no deja de ser privado, aunque transcienda a lo público mediante su publicación es decir tiene un autor original, que, aunque es difícil de proteger su contenido las leyes en Colombia lo protegen y sancionan a quien no lo reconoce.

[1] COLOMBIA. CONGRESO DE LA REPÚBLICA. Constitución Política de Colombia, (4 de julio de 1991), por la cual se actualiza la Constitución Política de Colombia. Consultado el (01 de agosto del 2022) publicado mediante el Diario Oficial Nro. 52143 del (31 de agosto de 2022) puede ser consultado mediante el siguiente internet: http://www.secretariasenado.gov.co/constitucion-politica

En Colombia desde el mes de enero el día 28 del año 1982 se reconoce el derecho sobre el autor ya sea de obras literarias, científicas y artísticas, protegiendo en todo momento y reconociendo a quienes se dedican a escribir, cantar, desarrollar es por ello la importancia de este tipo de leyes que no pueden ser obsoletas o de no aplicabilidad en el orden nacional puesto que la necesidad es constante de no ser vulnerados sus derechos como autores de todas las obras

LEY 1273[2] (cinco de enero del 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".
desarrolladas dedicando tiempo, espacio, recursos entre otros aspectos de relevancia.

En Colombia desde el mes de agosto el día 18 del año 1999 se creó la ley 527[3] "***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***" demostrándose con este tipo de leyes que existen controles de todo tipo que garantizan la libertad de expresión y de comunicación.

En Colombia en su Código Penal ley 599 del 2000[4] en su artículo 195 hace referencia a que ***"el que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo"*** este se verá inmerso en una sanción pecuniaria es decir una multa, sanción que aunque es poca en el ámbito penal permite observar que efectivamente existe por parte del estado

---

[2] COLOMBIA. CONGRESO DE LA REPÚBLICA. Creación del nuevo daño antijuridico mediante la ley 1273 del (05 de enero del 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". Consultado el (23 de agosto del 2022) se puede consultar en internet;* ***https://www.lexbase.co/lexdocs/indice/2009/l1273de2009#:~:text=%22%20LEY%201273%20DE%202009%20(enero,y%20las%20comunicaciones%2C%20entre%20otras***

[3] COLOMBIA. CONGRESO DE LA REPÚBLICA. reglamenta el acceso y uso de los mensajes de datos mediante la Ley 527 del (18 de agosto 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" consultado el (22 de agosto del 2022) puede ser consultado en internet: https://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013

[4] COLOMBIA. CONGRESO DE LA REPÚBLICA. Código penal de Colombia mediante la Ley 599 del (24 de julio del 2000) "Código Penal Colombiano", mediante la cual se tipifica el Código Penal de Colombia", consultado el (20 de agosto del 2022) puede ser consultado mediante el internet: https://www.oas.org/dil/esp/codigo_penal_colombia.pdf

colombiano, sus fuerzas de control una sanción a quien de forma abusiva ingresa al sistema informático de otra persona ya sea natural o jurídica.

Otro de sus artículos de la ley 599 del 2000 “código penal colombiano” que se creó bajo el capítulo séptimo es el 192 que manifiesta que ***“el que ilícitamente sustraiga, oculte, extravié, destruya intercepte controle o impida una comunicación privada dirigida a otra persona o se entere indebidamente de su contenido”*** tendrá una sanción penal de 1 a 3 años de prisión es decir que será privado de su libertad en establecimiento penitenciario y carcelario, además hace referencia a que si la conducta es constituida delito sancionatorio con pena mayor se le debe aplicar esa pena mayoritaria.

Haciendo referencia al artículo 192 del código Penal Colombiano existe un agravante como es divulgar el contenido de la comunicación con fines ya sean propios o ajenos, esta sanción se aumentará a pena privativa de 2 a 4 años en establecimiento penitenciario y carcelario, es decir privado de la libertad con medida de aseguramiento en estos establecimientos conocidos como cárceles.

El artículo 193 de la ley 599 del 2000 manifiesta que el que ofrezca, venda o compra de instrumentos para interceptar la comunicación privada entre las personas sin la previa autorización de la autoridad competente, incurrirá en multa siempre y cuando esta conducta no constituya falta mayor, es decir que no sea sancionada como un agravante dentro de una conducta tipificada como delito con mayor sanción penal.

En el artículo 194 de la “ley 599 del 2000 Código Penal Colombiano”, hace referencia a la divulgación y empleo de documentos reservados con fines para sí, o para un tercero es decir lucros pecuniarios, o de carácter beneficioso además perjudiciales ante otra persona y violentando el derecho a la reserva de dicho documento es donde se hace merecedor a una sanción tipo multa.

En el artículo 196 de la “ley 599 del 2000 Código Penal Colombiano”, hace referencia que el servidor público o funcionario con condición publica es decir que trabaje para el estado y su salario sea con pecunio público, ilícitamente sustraiga oculte, extravié, destruya intercepte, controle o impida comunicación o correspondencia de carácter oficial incurrirá en sanción penal, de prisión de 3 a 6 años con pena privativa en establecimiento carcelario, es decir pierde su libertad y es objeto de pena privativa.

En el artículo 197 de la “ley 599 del 2000 Código Penal Colombiano”, manifiesta que el que con fines ilícitos posea o haga uso de aparatos de radiofonía o televisión para emitir o recibir señales incurrirá en prisión de 1 a 3 años y si este se hace con fines terroristas manifiesta la norma que la pena se aumentará en una tercera parte de la mitad, todos estos artículos hacen referencia a que Colombia está siempre con sus leyes a la vanguardia y a la protección de sus ciudadanos.

El cinco de enero del 2009 se creó la LEY 1273 “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”.

Es una adicción al Código Penal Colombiano ley 599 del 2000 en forma de título denominado VII BIS “De la Protección de la información y de los datos” En su capítulo I, de la LEY 1273, hace referencia a los atentados contra la confidencialidad, la integridad y la disponibilidad de los diferentes datos y de los sistemas informáticos, en su artículo 269A, manifiesta que el que sin autorización o fuera de lo acordado acceda en todo o en parte de un sistema informático protegido incurrirá en prisión de 48 a 96 meses además de una sanción pecuniaria de 100 a 1.000 salarios mínimos legales mensuales vigentes, contribuyendo a proteger a propietarios y administradores de este tipo de sistemas informáticos.

De esta manera se es evidente la forma como el estado colombiano realiza aportes significativos de protección, respaldo y apoyo a todos los desarrolladores de plataformas tecnológicas puestas al servicio de las personas, además que está adelantando de forma continua procesos de seguridad informática, ya que estas se actualizan de forma permanente.

4 EN EL MUNDO DE LA CIBERSEGURIDAD EXISTEN PROCESOS DEFINIDOS PARA PODER EJECUTAR DE FORMA ORGANIZADA LO QUE SE CONOCE COMO PRUEBAS DE PENETRACIÓN O PENTESTING; USTED COMO FUTURO EXPERTO DEBERÁ REDACTAR CON SUS PALABRAS Y DEFINIR CADA UNA DE LAS ETAPAS DEL PENTESTING, DENTRO DE LA DEFINICIÓN INCORPORARÁ UN EJEMPLO DE UNA HERRAMIENTA QUE SE UTILICE PARA CADA UNA DE LAS ETAPAS DEL PENTESTING.

Para el presente interrogante que se plantea se consultan los diferentes métodos de penetración de pentesting[5], de igual manera se incorporan ejemplos de las herramientas de las etapas, conforme lo requerido por el docente mediante la guía y rubrica de evaluación a ejecutar en la presente unidad objeto de estudio así:

Las etapas del pentesting o penetración[6] se ejecutan mediante siete fases las cuales se dan a conocer de la siguiente manera.

[5] COLOMBIA. CONGRESO DE LA REPÚBLICA. Código penal de Colombia mediante la Ley 599 del (24 de julio del 2000) “Código Penal Colombiano”, mediante la cual se tipifica el Código Penal de Colombia”, consultado el (20 de agosto del 2022) puede ser consultado mediante el internet: https://www.oas.org/dil/esp/codigo_penal_colombia.pdf

[6] Ciberseguridad, Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas, ¿qué es cve? explicación de las vulnerabilidades y exposiciones comunes, consultado (el 15 de septiembre del 2022). Disponible en: https://ciberseguridad.com/herramientas/marco-mitreatt-ck/cve-vulnerabilidades-exposiciones-comunes/

Fase previa al compromiso: La fase previa al compromiso: se conoce como la fase de reuniones de las partes involucradas, donde lo que se da a conocer que alcance es lo que se busca con la presente prueba y hasta donde se puede realizar la misma.

La fase de recopilación de la información: donde se adelanta el respectivo análisis de los activos recepcionados, haciendo uso de las diferentes herramientas para la recopilación de la información en todos los sistemas de la empresa u organización.

Fase de modelado de amenazas: es la que busca llevar a cabo los diferentes planes de desarrollo, además de adelantar los ataques a los sistemas de información.

Fase de los análisis de las vulnerabilidades: es en la que se evalúan además como se encuentra la organización y como solucionar esas posibles debilidades con las que cuenta la empresa.

Explotación: es la fase en la se lleva a cabo la ejecución de los diferentes exploits (que además son los que permiten evidenciar los ataques de los que se aprovechan para evidenciar las vulnerabilidades de la red, equipos de cómputo, en fin, el hardware y software con los que cuenta la organización.

Post Explotación: mediante la presente fase se permite la recopilación de toda la información sobre los diferentes sistemas, información que se recolecto mediante la fase de explotación, evitando que se realice alguna fuga de los activos de información.

Reporte: Es conocida como la fase final con las que se adelanten las pruebas y se plasma el informe final donde se constata todo lo presentado, vulnerabilidades, fortalezas entre otros aspectos de alto valor para la organización, se podría decir que es el informe final de la actividad de penetración.

5 LAS HERRAMIENTAS DE CIBERSEGURIDAD SON DE VITAL IMPORTANCIA, ADEMÁS QUE EXISTE UN GRAN ABANICO DE POSIBILIDADES DE HERRAMIENTAS EXISTENTES Y SOFTWARE ESPECIALIZADO PARA DESARROLLAR HERRAMIENTAS PROPIAS. USTED COMO FUTURO EXPERTO DEBE DEFINIR Y EXPLICAR LAS SIGUIENTES HERRAMIENTAS:

METASPLOIT: Se conoce como una herramienta que permite el desarrollo a su vez la ejecución de diferentes exploits[7] que pueden ser utilizados en una

[7] F Jagrey Funlnformatique- Ahmed publicado el (13de agosto de 2022). Metasploit: ¿qué es y cómo usarlo? Consultado el (20 de agosto del 2022) el cual

herramienta de forma remota, a su vez permite realizar auditorías de seguridad de la información dentro de un sistema de una organización o empresa, además es de resaltar que esta herramienta se desarrolló inicialmente en un sistema denominado PERL, posteriormente en el lenguaje RUBI.

Esta herramienta es utilizada de manera recurrente con la finalidad de realizar pruebas de vulnerabilidades y verificar la protección con la que cuenta la empresa, visualizar las falencias y entrar a corregir o dar a conocer a los administradores que deben mejorar dentro del sistema de la organización, es una herramienta de gran uso y con unas características que la hacen importante dentro de las empresas con fines de desaparecer las vulnerabilidades y atacar de manera efectiva las fallas que se presentan dentro de los sistemas de las organizaciones.

Esta herramienta es compatible con un buen número de sistemas operativos, situación por la que es de gran utilidad y de uso en el desarrollo y ejecución de exploits, seguidamente permite esta herramienta llevar a cabo el escaneo y recopilación de la información de una máquina (computadores de escritorio o portátiles).

La escala de datos y la fuga de los mismos, permite realizar la instalación de puertas, hacer el escape de virus, eliminar registros y seguimientos entre otras actividades propias de la seguridad de la información, para la instalación de esta herramienta se deben llevar a cabo algunos pasos en lo que incluye recursos que no son tan difíciles de encontrar en las herramientas tecnologías con las que cuentan los dispositivos que se ofrecen en el mercado.

NMAP: Es una multiplataforma que su código es abierto[8], además es utilizado en el escaneo de puertos de las redes, es fiable y de gran utilidad dentro de una organización se utiliza dentro de la seguridad de la información, dado que es un software gratuito[9] es de bastante uso por parte de expertos al momento de realizar escaneo de puertos y monitorización de redes, con finalidad de obtener información valiosa para controlar y realizar monitoreo constante en la seguridad de las redes y en especial de los activos de información.

OPENVAS SERVICIOS EN LÍNEA: Es un conjunto de herramientas, con la finalidad de dar al público en general unos servicios de solución integral, buscando las vulnerabilidades de los diferentes sistemas operativos, además se conoce como un escáner de seguridad real, ejecutado de forma permanente, este software es gratuito la licencia es pública de GNU GPL, permitiendo estar atento y pendiente ante las vulnerabilidades detectadas, existe el openVAS

puede ser consultado desde el: https://www.funinformatique.com/es/que-es-metasploit-y-como-usarlo-bien/

[8] NMAP, software consultado (09 de agosto del 2022) puede ser descargo el software mediante internet a través de: https://nmap.org/download#linux-rpm

[9] NMAP, recuperado de https://nmap.org/download#linux-rpm

manager que permite un servicio central, además consolida el escaneo de las vulnerabilidades, dando un servicio integral efectivo y eficaz a las organizaciones.

Posee un sin número de características dentro de algunas categorías como son; escáner del software, con capacidad de realizar el escaneo de varios hosts de manera simultánea, cuenta con el protocolo OTP, soporta el SSL, el WMI, el OMP, base de datos de SQL, permite diferentes tareas de escaneo de forma frecuente, a su vez escaneos programados entre otros que lo hacen uno de los mejores softwares gratuitos actuales en el mercado.

EXPLOITDB: Para dar inicio como tal para exploitdb, es necesario dar a conocer que es un exploit, se define como un software, aplicación de escript, creado con el fin de hacer uso completo de errores conocidos, vulnerabilidades o servicios de otros, que lo realizan que el software se presente de forma inesperada, ahora sí, es posible manifestar que el exploitdb, es la bases de datos, es decir la acumulación de muchos de ellos, que lo que buscan es ser una colección para la investigación de las vulnerabilidades y pruebas de pentesting.

CVE: Es una lista de vulnerabilidades se divulgan de manera pública con fines de ayuda, fue lanzado en el año de 1999 por la corporación MITRE, que proporciona un diccionario gratuito, con fines de mejorar por parte de las empresas u organizaciones en términos de seguridad informática, en cuanto a MITRE, es una organización de investigación sin ánimo de lucro, que con dinero y recursos de los Estados Unidos de Norte América se financia.

6 PARA FINALIZAR ESTA ACTIVIDAD ES IMPORTANTE QUE USTED RECONOZCA, ANALICE Y CONFIGURE “BANCO DE TRABAJO” LO SOLICITADO EN EL ANEXO 1 – ESCENARIO 1 SOBRE EL CUAL DEBERÁ TRABAJAR ACTIVIDADES QUE CONTIENEN UN ALTO GRADO DE TECNICIDAD. LO SOLICITADO EN EL ANEXO 1 – ESCENARIO 1 ES LO SIGUIENTE:

• PASO A: DESCARGAR LA HERRAMIENTA VIRTUALIZADORA “VIRTUALBOX” EN SU ÚLTIMA VERSIÓN.

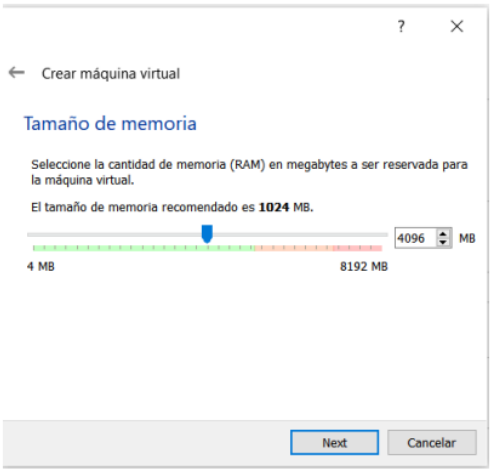

Ilustración 1 Máquina Virtual VIRTUALBOX

Se procede a instalar y configurar la máquina virtual conforme lo requiere la presente guía y rubrica de evaluación.

• PASO B: UNA VEZ SE REALICE APERTURA DEL FORO PARA EL DESARROLLO DE LA ACTIVIDAD SE PROCEDERÁ A COMPARTIR ENLACE DE DESCARGA DE LO REQUERIDO PARA EL MONTAJE DEL BANCO DE TRABAJO, LAS IMÁGENES EN FORMATO. OVA LAS CUALES SE ENCUENTRAN YA PRECONFIGURADAS PARA SER UTILIZADAS EN LAS ACTIVIDADES DE CARÁCTER TÉCNICO. EN LAS IMÁGENES. OVA EXISTE: UN WINDOWS 7 X86, UN WINDOWS 7 X64, UN KALI LINUX.

• PASO C: DEBE VALIDAR QUE EXISTA COMUNICACIÓN ENTRE CADA UNA DE LAS MÁQUINAS WINDOWS CON LA MÁQUINA DE KALI LINUX, RECUERDE POR FAVOR NO ENCENDER LAS TRES MÁQUINAS AL TIEMPO YA QUE PUEDE COLAPSAR LOS RECURSOS HARDWARE DE SU EQUIPO HOST, ENCIENDA PRIMERO UNA MÁQUINA WINDOWS Y POSTERIOR A ELLO ENCIENDA LA MÁQUINA KALI LINUX.

• PASO D: EVIDENCIAR CON PRINTSCREEN EL MONTAJE DEL BANCO DE TRABAJO Y EXPLICAR CÓMO SE ENCUENTRA DESPLEGADO “CARACTERÍSTICAS TÉCNICAS DE HARDWARE”.

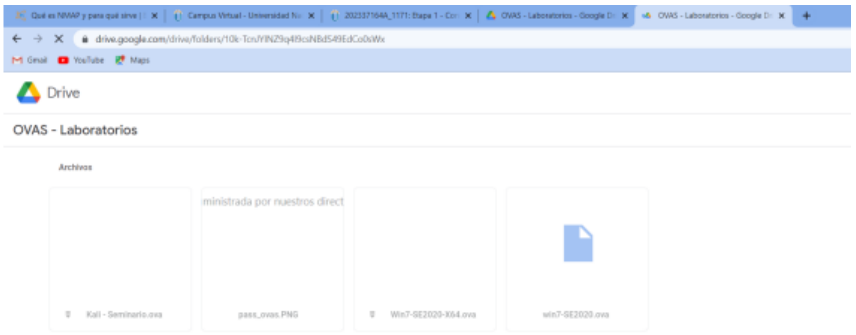

Ilustración 2 Imágenes OVA a instalar

Se visualizan las imágenes entregadas por parte del docente mediante drive, a instalar y dar inicio de la misma en la máquina Virtual Vox, según lo requerido por el docente mediante la guía y rubrica de evaluación.

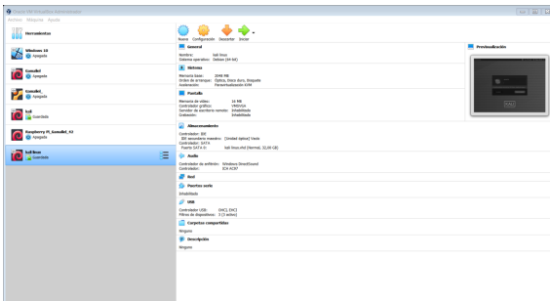

Ilustración 3 Máquinas Virtuales instaladas

Se procede a instalar las diferentes máquinas virtuales requeridas y se visualiza la activación de las mismas observando su compatibilidad, a su vez estas se encuentran listas como banco de trabajo para continuar con el desarrollo de las actividades, dentro del seminario especializado.

7 ETAPA 2 ACTUALIZACIÓN ÉTICA Y LEGAL

8 ¿UNA VEZ LEÍDO EL ANEXO 2 – ESCENARIO 2 Y EL ANEXO 3 - ACUERDO USTED LOGRA EVIDENCIAR ALGÚN PROCESO ILEGAL Y NO ÉTICO QUE SE ESTÉ ESTIPULANDO EN DICHO ACUERDO? DEBERÁ ARGUMENTAR SU RESPUESTA Y SEÑALAR LOS FRAGMENTOS ILEGALES DEL ANEXO ACUERDO EN CASO DE EXISTIR ALGUNA IRREGULARIDAD.

En el tema de las consideraciones más exactamente en el numeral segundo se presenta una irregularidad toda vez que hace exclusivo el tema de los activos de información manifestando que Hackers Security, datos de chuzadas vulnerando los diferentes derechos de los trabajadores toda vez que justifica esa irregularidad desde el ámbito de confidencialidad, pero no es así,

Debido a que las personas tienen derecho a su intimidad, el tema de la interceptación no es avalada en Colombia salvo que la autoridad competente lo ordenado por que haya indicios de actividad delictiva es decir un delito tipificado en la ley 599 del 2000 “por el cual se expide el código penal colombiano” en cuanto a exceder de forma abusiva a sistemas informáticos atenta contra los diferentes funcionarios operadores del sistema de tecnología en la empresa.

Actividades completamente ilícitas y tipificadas como delitos actuales en Colombia que tiene pena privativa, hasta carcelaria toda vez que atenta contra la dignidad humana y además vulnera derechos hasta fundamentales consagradas en la Constitución Política de Colombia actualizada en el año de 1991, afectando directamente a la calidad de vida y pensar, de las personas que laboran en la empresa Hackers Security.

En cuanto al numeral tercero de la definición de información confidencial, se presentan una irregularidad puesto que manifiesta que debe guardarse la información asiendo alusivo a omisión de denunciar ante alguna irregularidad que es lo que se presenta para los funcionarios públicos o que por su conducta o código ético juraron no omitir dicha información que es oportuna para denunciar, ante autoridad legítima competente.

En cuanto al numeral cuarto acerca de las obligaciones de la parte receptora: en su numeral tres manifiesta que se debe abstener de denunciar y publicar información confidencial, siendo que si es un delito el funcionario que la conozca y la calle estar catalogado según el código penal colombiano en sus apartes un cómplice de dicha irregularidad ilegal.

En el numeral octavo acerca de las obligaciones de la parte receptora: manifiesta que debe asumir la responsabilidad de la información que se encuentre en su poder es decir que va a ser activo responsable penal, disciplinaria y administrativamente de una información que no le corresponde y desconoce con qué fin se allego a la misma, es decir que puede verse inmerso de un delito sin grado de dificultad solo por el hecho de ser quien porte o tenga estos activos de información.

En el numeral sexto acerca de la responsabilidad, manifiesta que se debe asumir la responsabilidad por la inobservancia del presente acuerdo es decir se asume, todos los perjuicios morales, económicos, por incumplir el acuerdo o sea no se tiene derecho a reclamar por que quien cometió el error fue quien acepta el acuerdo.

9 SI LA RESPUESTA ES AFIRMATIVA Y USTED ENCONTRÓ ALGÚN PROCESO ILEGAL EN EL ANEXO 3 - ACUERDO DEBERÁ MENCIONAR QUE ARTÍCULOS DE LA LEY 1273 SE PODRÍAN VULNERAR EN DICHO ACUERDO Y ESPECIFICAR PORQUÉ VULNERA ARTÍCULOS DE LA LEY 1273.

Desde luego que se encuentran conductas delictivas en el acuerdo realizado por parte del funcionario que laboró en la empresa Hackers Security, en algunos aspectos como son:

Haciéndose un análisis más profundo acerca de la ley 1273 de 2009 “por medio de la cual se le realizaron modificaciones a la ley 599 Código Penal Colombiano”, a su vez se crea un nuevo bien jurídico que se denomina “de la protección de la información y de los datos”, cuyo fin primordial es la preservación de los diferentes sistemas que se utilizan por medio de las tecnologías de la información y las comunicaciones de una forma integral y única.

Es así que dentro de la ley 1273 del 2009, se contemplan una serie de delitos informáticos que se tipifican y se ven inmersos en el contrato como son;

• La cláusula primera, segunda, cuarta y el parágrafo tercero, en su artículo 269A, donde hace anuncio al acceso abusivo a un sistema informático, donde se debe observar y analizar los accesos no autorizados, donde se debe incluir lo que se denomina en el contrato “chuzada” donde se debe utilizar una serie de herramientas que no son permitidas y atenta completamente con la dignidad e irrespeto humano.

• Artículo 269A: Acceso abusivo a un sistema informático; que según lo manifestado por el acuerdo la empresa podría según el numeral dos de la segunda cláusula de la definición de información confidencial que puede acceder abusivamente a sistemas informáticos y el artículo 269a de la ley 1273, manifiesta que el que sin autorización o por fuera de lo acordado acceda en todo o en parte a un sistema informático, incurrirá en prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos mensuales vigentes.

• Lo que manifiesta que efectivamente la empresa y su representante legal se ve inmerso en la comisión de actividad ilegal, si realiza la actividad que para el abogado que realizo el anexo tres o contrato es legal o una cláusula que puede incluir en el mismo, se observa que es una conducta que se tipifica ilegal y con pena privativas de la libertad, en establecimiento carcelario. Además, inmerso en el pago de multa económica.

• Otra actividad ilícita que se observa en la ley 1273 es la del 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. Se ve inmerso en la cláusula segunda del presente acuerdo sobre la definición de información confidencial.

• Otra actividad delictiva en la incurriría la empresa al aplicar las diferentes clausulas organizadas en el acuerdo objeto de estudio es la del 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, 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.

• Puesto que una de sus cláusulas manifiesta que la información producto de interceptación puede usar o aplicada como información confidencial, situación que no es oportuna ni viable dado que la misma es de carácter ilegal puesto que no es avalada ni amparada por la autoridad competente en el caso de Colombia Fiscalía General de la Nación o un juez de la república.

• En la Cláusula segunda se observa que violenta como tal el Artículo 269C el cual manifiesta que no es legal la interceptación de los datos informáticos dado que, en ningún punto de origen o destino, de igual manera que contempla la no

interceptación de ondas electromagnéticas, este contrato lo refiere como actividad legal desconociéndose en su totalidad la norma citada.

• En el Articulo 269D de la ley 1273 del 2009, en sus apartes indica que es ilegal cualquier tipo de alteración o daño a nivel de software y hardware, ya sean memorias o dispositivos de almacenamiento, para tener en cuenta ante posibles ataques a los que sean víctimas los equipos de la organización.

• En el artículo 269E de la ley 1273 del 2009 en sus apartes se indica el no uso de software maligno o malware, pero ante no indica claramente cuáles son los tipos de Malware. Lo que deja un vacío que puede ser mal intencionado o usado con fines de hacer daño dentro de una red.

• El Articulo 269F dentro de la ley 1273 del 2009, se contempla la protección de datos personales, los contenidos en bases de datos, los diferentes ficheros, los cuales en ningún momento pueden ser sustraídos, vendidos, interceptados, por ningún ente u organización lo que es evidente que este contrato no se encuentra ajustado a lo normado. Según lo escrito y contemplado por la ley.

• En cuanto a la suplantación de sitios Web, que se estipula en el contrato con el fin de obtener datos de carácter personal este enunciado en el artículo 269G, referente a personas que clonen, o se apropien de páginas legales o realicen el desvió de los activos de información para beneficio propio o de terceros cuya actividad es contemplada por parte del contrato como una actividad normal.

• En cuanto a el articulo 269 I y J contempla la fuja de información, hurto de los activos de información, por medios netamente informáticos y además la no transferencia de no consentida de los activos, archivos de la información de la organización.

10 ¿EXISTIENDO PROCESOS POCO CONFIABLES EN EL ANEXO 3 – ACUERDO? ¿USTED COMO EXPERTO EN CIBERSEGURIDAD APLICARÍA A ESTE TRABAJO EN HACKERS SECURITY, DONDE LA ORGANIZACIÓN DISPONE DE UN SUELDO DE $15.000.000 DE PESOS COLOMBIANOS MENSUALES Y CONTRATO VITALICIO? DEBE ARGUMENTAR SU RESPUESTA YA SEA AFIRMATIVA O NEGATIVA Y TENER EN CUENTA EN LA ARGUMENTACIÓN LO QUE SE DISPONE EN COPNIA EN SU CÓDIGO DE ÉTICA PARA INGENIEROS.

Dado que la empresa tiene una vacante para el cargo, como especialista en seguridad informática, lo primero que se debe realizar es el acuerdo por parte de tanto de la empresa como el funcionario y dado que existe una serie de actividades irregulares y no éticas puesto que, desde el orden jurídico y legal, dentro de lo normado en Colombia según lo enunciado en el punto anterior haciéndose referencia a la ley 1273 del 2009.

Seguidamente dado que es un ejercicio de identificación y argumentos acerca del porque se acepta la vacante o no, como profesional se debe tener presente

el código ético que dispone COPNIA[10], para ingenieros, según como se presenta las cláusulas y parágrafos no se aceptaría el trabajo por los siguientes argumentos así.

Dado que si bien es de anotar y de resaltar que es una oportunidad excelente de laborar y adquirir un contrato vitalicio es notorio que sus formas de laborar o realizar la contratación de sus empleados no legal y además carece de principios éticos, como ingeniero y teniendo en cuenta los diferentes valores y principios inculcados en casa, escuela, colegio y universidad, según lo plasmado en el presente contrato carece de toda ética e induce a delitos y actividades no legales.

No hay respeto por la dignidad humana, respeto por los trabajadores o funcionarios que laboran en la empresa, no se vela por que los funcionarios tengan un valor más allá de lo que produzcan o hagan por la organización, es decir como personas, ya que no respeto por la intimidad, no existirá respeto por las familias o núcleos familiares toda vez que hasta las conversaciones de los empleados van hacer objeto de investigación. Entre otros que definitivamente desdibujan una imagen como empresa u organización.

Haciéndose referencia a COPNIA lo que se "busca en sí, es que los ingenieros, profesionales y actividades propias" de la asignación del cargo o vacante existente en esta empresa, es según el código ético ser personas integras con principios y valores que no se sometan a realizar o permitir hechos delictivos dentro de una organización.

Ya que el código emitido por la empresa COPNIA, para el ejercicio de la ingeniería en términos generales en su capítulo II, dentro de los deberes y obligaciones en su artículo 31 dentro de su parágrafo indica "son deberes generales de los profesionales los siguientes"

Literal F) denunciar los delitos, contravenciones y además las faltas que se encuentren y que contraríen el código ético, del como tal se tenga conocimiento con ocasión del ejercicio de la profesión, además se tiene el deber de aportar todas las pruebas e información para la investigación pertinente, que se desarrollara para esclarecer los posibles hechos punibles.

Dado que la investigación arrogue que el ingeniero plenamente conocía y sabía lo que se estaba presentando y no lo informó será causal de vinculación a la investigación e incurriría en una conducta delictiva, seguidamente afectaría tanto la persona como la profesión, el entorno familiar, la comunidad académica donde desarrollo y curso como tal la carrera profesional.

[10] COLOMBIA. CONGRESO DE LA REPÚBLICA. Código de ética para ingenieros mediante la ley 842 del año 2003 Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Etica Profesional y se dictan otras disposiciones, (9 de octubre del 2003). Consultado el (25 de agosto del 2022) el cual puede ser consultado en https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

En el capítulo II de los deberes y obligaciones de los profesionales. Artículo 34 del código de ética de COPNIA, se encuentra en el parágrafo que indica las “prohibiciones especiales a los profesionales respecto de la sociedad” literal A) manifiesta ofrecer o aceptar actividades laborales que vayan en contravía, de las disposiciones y el ordenamiento legal.

En el caso objeto de estudio se evidencia que el aceptar este empleo tal como se encuentra el contrato organizado, va hacer objeto de investigación de tipo penal, disciplinario, entre otras, ya que es evidente la falta de principios, valores, argumentos para la tipificación de conductas delictivas.

Seguidamente en el Código de Ética que fue desarrollado por la empresa COPNIA, para el ejercicio de la Ingeniería en general, además de profesiones afines y auxiliares, en el Capítulo II, de los deberes y obligaciones de los profesionales. En el artículo 39. Se encuentra en el parágrafo, “Son deberes de los profesionales para con sus clientes y el público en general”.

a) Mantener el secreto y la confidencial de la reserva, con respecto a todas las circunstancias con relación cliente, trabajadores, entre otras partes que se involucren con la actividad netamente laboral siendo, así las cosas, existe una excepción la cual es la de la obligación legal de revelarla o con requerimiento de autoridad competente se debe rendir tanto declaración juramentada o aporte de las pruebas correspondientes para que obren dentro del proceso como EMP-EF en el mismo.

Para terminar dentro de lo escrito del código ético para el ejercicio y desarrollo de las actividades propias de la profesión de ingeniería y especialista en seguridad de la información, se contempla las faltas gravísimas en el artículo 53 de la ley 842 del 2003 dentro de los literales E y F así:

e) incurrir en alguna conducta tipificada como delito, atentando en contra de los clientes, compañeros, autoridades de la república de Colombia, conducta que de alguna manera se observa está inmersa de la profesión de ingeniería o alguna profesión auxiliar.

f) cualquier conducta que violente los principios de protección y seguridad de la información de actividades que, según criterio del consejo respectivo de ingenieros, o que atente contra los deberes, obligaciones y prohibiciones que establecen tanto en el código de ética, como en las leyes que se encuentran vigentes para el país de Colombia.

11 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.

Desde el punto ético una actividad que carecía totalmente de principio ya que lo que buscaba era generar espacios de esparcimiento y de relajo a cambio de apropiarse de conocimientos y actividades originales de quienes asistían a dichos eventos que aparentemente eran de carácter gratuita pero la finalidad salían costosas ya que se empleaba un software maligno para hacer hurto de información confidencial e íntima, personal de quienes asistían a dicha actividad en los sitios propios de la empresa o fachada de empresa.

Desde el punto legal una actividad completamente ilegal que carecía de todo principio de norma puesto que su finalidad no es legal, nada que pudiese ser obtenido de forma irregular o sin el consentimiento de los autores es imposible que se pueda denominar legal[11], en la ley 1273 del año 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".***

Manifiesta que Artículo 269E: Uso de software malicioso. El que, sin estar facultado o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, 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 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, 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.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, enlaces o ventanas emergentes, 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, siempre que la conducta no constituya delito sancionado con pena más grave.

Los anteriores artículos tipifican la comisión de delitos en los que se ve inmerso el Ejército Nacional de Colombia con la operación Andrómeda puesto que fue quien llevo a cabo la actividad ilícita[12] y operaba los diferentes espacios donde se desarrollaron las actividades ilegales.

---

[11] Peñaredonda José Luis Enter.co. Detrás de Buggly: la historia de la fachada Andrómeda, transformación digital realizado el (09 de diciembre del 2015) consultado el (25 de agosto de 2022) puede ser consultado mediante internet: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

[12] EL TIEMPO (23 de enero del 2015). Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [En línea]. Consultado el (25 de agosto del 2022) puede ser consultado en internet en: https://www.eltiempo.com/archivo/documento/CMS-15141236

12 ETAPA 3 EJECUCCIÓN PRUEBAS DE INTRUSIÓN

13 DESCRIBA DE MANERA ESPECÍFICA LAS HERRAMIENTAS SOFTWARE QUE UTILIZÓ PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3 ENFOCADO A REDTEAM. DEBERÁ ADJUNTAR EVIDENCIA DE LOS COMANDOS UTILIZADOS Y RESULTADOS QUE ARROJÓ CADA HERRAMIENTA UTILIZADA, ESTAS HERRAMIENTAS DEBEN ESTAR CLASIFICADAS SEGÚN LOS PASOS DE UN PENTESTING.

Para dar respuesta a este interrogante, es necesario manifestar que para el desarrollo de la actividad de laboratorio simulado-practico se procede a instalar los diferentes softwares que se mencionan a continuación así:

VirtualBox: en la versión requerida y actualizada según la guía y rubrica de evaluación, entregada por parte del docente, es de anotar que es una herramienta de simulación en la que se puede dar inicio a varios sistemas operativos[13], ejecutar la actividad requerida los comandos a tener presente para instalar el mismo, es la descarga y la ejecución del software, además este permite que se instalen y ejecuten los diferentes sistemas operativos como sea posible, lo que se conoce como máquinas virtuales que si bien es cierto no se ejecutan todas a la vez porque colapsaría el software, si permite el desarrollo de la actividad máquina a máquina, es decir de forma individual.

Dado que el host o máquina ocuparía la totalidad de los recursos que se le asignen a cada una, además que los comandos a utilizar son los de instalación asignación de recursos y a ejecutar como tal, para que la herramienta tecnológica “computador” inicie la ejecución de la actividad en sí, no es viable la reproducción de todas las máquinas que se encuentren instaladas en el software VirtualBox.

Kali Linux: es el sistema operativo con el que se desarrolla e instala la máquina virtual requerida, para poder adelantar el laboratorio con fines de evidenciar la fuja de la información de la cual la empresa es víctima y la sospecha es única y exclusiva de dos computadores que cuyo sistema operativo se encuentra obsoleto.

Sistema Operativo Windows 7 X86 y X64; sistema operativo que se hace necesario para el desarrollo de la actividad simulada, además es un software que fue desarrollado y puesto en marcha desde el año 2009[14], que a la fecha no se encuentra con soporte técnico por parte de Windows, haciendo que la empresa

[13] Niño Ordoñez, José Rafael, artículo sobre las Capacidades Técnicas, Legales y de Gestión para Equipos BlueTeam y RedTeam. Consultado el (29 de septiembre del 2022) fue publicado en el 2020.
[14] Niño Ordoñez, José Rafael, artículo sobre las Capacidades Técnicas, Legales y de Gestión para Equipos BlueTeam y RedTeam. Consultado el (29 de septiembre del 2022) fue publicado en el 2020.

sufra de manera constante diversos ataques de seguridad y sea víctima de fuga de los activos de información.

Nmap; software que se requiere para generar la simulación y dentro de la misma hacer que se realice el escaneo de los puertos e IPS, que se encuentran dentro de la red, es de resaltar que los comandos a utilizar dentro del software son inicialmente los de instalación, seguidos de los de escaneo de las IPS del sistema, entre otros que se anexan a continuación así:

NMAP 6: Listado de comandos

ESPECIFICACIÓN DE OBJETIVOS			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
-iL <fich>	Objetivos en fichero	Se pasan los objetivos en un fichero, cada uno en una línea[1].	
-iR <num>	Objetivos aleatorios	Elige los objetivos de forma aleatoria.	
--exclude <hosts>	Lista exclusión	Indica equipos a excluir del análisis.	
--excludefile <fich>	Fichero exclusión	Se pasan en un fichero los equipos a excluir del análisis[1].	

DESCUBRIMIENTO DE EQUIPOS			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
-Pn	No ping	No realiza ninguna técnica de descubrimiento. Pasa directamente al análisis de puertos.	Considera a todos los objetivos como aptos para un análisis de puertos.
-sL	List Scan	Sólo lista equipos. No envía ningún paquete a los objetivos.	Hace resolución inversa DNS.
-sn	Ping Sweep	Implica un *-PE + -PA 80 + -PS 443*. Si misma subred, también *-PR*. No hace análisis de puertos posterior.	Si usuario sin privilegios: *connect()* a 80 y 443. Hace resolución inversa DNS.
-PR	Ping ARP	Sólo para objetivos de nuestra red local (activo por defecto). Envía un ARP Request.	*Host Up:* Se recibe un ARP Reply. *Host Down*: Expira el *timeout*.
-PS<ports>	Ping TCP SYN	Envía un SYN, por defecto al puerto 80. Acepta lista de puertos. Se ejecuta este si usuario sin privilegios.	*Host Up*: Se recibe un SYN/ACK o RST. *Host Down:* Expira el *timeout*.
-PA<ports>	Ping TCP ACK	Envía un ACK vacío, por defecto al puerto 80. Acepta lista de puertos. Traspasa cortafuegos sin estado.	*Host Up:* Se recibe un RST. *Host Down:* Expira el *timeout*.
-PU<ports>	Ping UDP	Envía un UDP vacío al puerto 31338. Acepta lista de puertos. Traspasa cortafuegos que sólo filtran TCP.	*Host Up:* Se recibe un ICMP port unreachable. *Host Down:* Otros ICMPs, expira el *timeout*.
-PY <ports>	Ping SCTP	Envía un paquete SCTP INIT al puerto 80. Acepta lista de puertos. Solo usuarios privilegiados.	*Host Up:* Se recibe ABORT o INIT-ACK. *Host Down:* Expira el *timeout*.
-PE	Ping ICMP Echo	Envía un *ICMP Echo Request*. Poco fiable. Filtrado en la mayoría de cortafuegos.	*Host Up:* Se recibe ICMP Echo Reply. *Host Down:* Expira el *timeout*.
-PP	Ping ICMP Timestamp	Envía un *ICMP Timestamp Request*. Muchos cortafuegos no filtran este ICMP.	*Host Up:* Se recibe ICMP Timestamp Reply. *Host Down:* Expira el *timeout*.

Ilustración 4 NMAP: Listado de comandos tomado de CSIRT[15]-cv: Centro de Seguridad TIC de la Comunidad Valenciana. Recuperado de CSIRT- http://www.csirtcv.gva.es - http://www.facebook.com/csirtcv - http://twitter.com/csirtcv

[15] Ciberseguridad, Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas, ¿qué es cve? explicación de las vulnerabilidades y exposiciones comunes, consultado (el 15 de septiembre del 2022). Disponible en: https://ciberseguridad.com/herramientas/marco-mitreatt-ck/cve-vulnerabilidades-exposiciones-comunes/

-PM	Ping ICMP Address mask	Envía un *ICMP Address Mask Request*. Muchos cortafuegos no filtran este ICMP.	*Host Up:* Se recibe ICMP AddMask Reply. *Host Down:* Expira el *timeout*.
-PO<proto>	IP Protocol Ping	Envía sondas IP con protocolo 1, 2 y 4. Acepta lista de protocolos.	*Host Up:* Respuesta o ICMP Prot. Unreachable. *Host Down:* Expira el *timeout*.
Modificadores			
-n	DNS	No realiza nunca resolución inversa de DNS.	Más sigiloso y más rápido.
-R		Realiza la resolución inversa de DNS incluso a los objetivos que aparecen como *Down*.	
--dns-servers <srv>		Especifica la lista de servidores DNS a utilizar para hacer la resolución	
--system-dns		Utiliza el sistema de resolución DNS del sistema operativo	
--tracetoute	Ruta	Descubre la ruta seguida por los paquetes hasta el equipo objetivo.	

Ilustración 5 NMAP: Listado de comandos tomado de CSIRT-cv: Centro de Seguridad TIC de la Comunidad Valenciana. Recuperado de CSIRT- http://www.csirtcv.gva.es

ANÁLISIS DE PUERTOS			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
-sT	Connect	Envía un SYN, luego un RST para cerrar conexión. Puede utilizarse sin privilegios de root . Se utilizan llamadas del SO. Menos eficiente que SYN Stealth.	*Closed*: Recibe RST. *Open:* Recibe SYN/ACK. *Filtered: ICMP unreachable* o expira el *timeout*.
-sS	SYN Stealth	Envía un SYN. Es la técnica usada por defecto. Rápida, fiable y relativamente sigilosa. También denominada *half-open scan*.	*Closed:* Recibe RST. *Open:* Recibe SYN/ACK. *Filtered: ICMP unreachable* o expira el *timeout*.
-sU	UPD Scan	Envía UDP vacío. Más lento que un análisis TCP. Se puede realizar en paralelo a otras técnicas. Para diferenciar entre *Open* y *Filtered* se puede usar el detector de versiones (*-sV*).	*Closed:* Recibe *ICMP port unreachable*. *Filtered:* Recibe otros *ICMP unreachable*. *Open:* Ha habido una respuesta. *Open|Filtered:* Expira el timeout.
-sI <zombie[:port]>	Idle Scan	Compleja. Usa IP origen de un equipo intermedio (Zombie) para analizar el objetivo. Según los cambios en el IPID del zombie, se deduce el estado de los puertos del objetivo.	Técnica muy avanzada y sigilosa. No queda registro de ningún paquete directo al objetivo.
-sA	TCP ACK	Envía ACK vacío. Sólo determina si los puertos están o no filtrados.	*Unfiltered*: Recibe RST. *Filtered: ICMP error*; expira el *timeout*.
-sN	TCP NULL	Envía TCP con todos los *flags* a 0.	*Closed*: Recibe RST. *Filtered*: Recibe *ICMP unreachable*. *Open|Filtered*: expira el *timeout*.
-sF	TCP FIN	Envía TCP con el *flag* FIN a 1.	
-sX	XMas Scan	Envía TCP con los *flags* FIN, PSH y URG a 1.	
-sM	TCP Maimon	Envía ACK con el *flag* FIN a 1.	
-sW	TCP Window	Envía ACK vacío. Muy parecido a ACK Stealth. Diferencia entre puertos open y closed. No siempre es fiable.	*Open*: Recibe RST con *Window size* positivo. *Closed*: Recibe RST con *Window size* cero. *Filtered: ICMP error*; expira el *timeout*.
--scanflags <flags>	TCP Personal.	Envía TCP con los *flags* que se indiquen. Por defecto, trata estado de puertos como lo hace *-sS*, pero se puede especificar otro *scan*.	*Flags posibles:* URG, ACK, PSH, RST, SYN, y FIN. Sin espacios.
-sO	IP Protocol	Envía paquetes IP con la cabecera vacía (excepto para TCP, UDP e ICMP) iterando sobre el campo *IP Protocol*. Determina los protocolos de transporte soportados por el objetivo.	*Open*: Recibe cualquier respuesta (no error). *Closed*: Recibe *ICMP protocol unreachable*. *Filtered*: Recibe otros *ICMP unreachable*. *Open|Filtered*: expira el *timeout*.
-sY	SCTP INIT	Envía paquetes SCTP INIT (inicio conexión). Equivalente a TCP SYN.	*Open:* Recibe SCTP INIT-ACK. *Closed:* Recibe SCTP ABORT. *Filtered:* Recibe *ICMP unreachable* o expira el *timeout*.
-sZ	SCTP Cookie Echo	Envía paquetes SCTP Cookie Echo (3ª fase conexión). Útil si hay cortafuegos sin estado.	*Closed:* Recibe SCTP ABORT. *Open|Filtered:* Expira timeout. *Filtered:* Recibe *ICMP unreachable*.
-b <ftpsrv>	FTP Bounce	Usa la funcionalidad Proxy-FTP para recorrer puertos del objetivo. Las respuestas FTP indican estado del puerto. Parámetro: *username:pwd@server:port*	Explota las conexiones *Proxy-FTP, poco extendidas*. Se usa para traspasar cortafuegos.

Ilustración 6 NMAP: Listado de comandos tomado de CSIRT-cv: Centro de Seguridad TIC de la Comunidad Valenciana. Recuperado de CSIRT- http://www.csirtcv.gva.es - http://www.facebook.com/csirtcv - http://twitter.com/csirtcv

Metasploit Framework: es una de las herramientas que se utilizan para desarrollar pruebas de penetración o pentesting[16], normalmente este tipo de herramientas son las que utilizan los auditores, con fines de realizar la llamada informática forense, además permitirá realizar la explotación de las vulnerabilidades mediante sus exploits, que la herramienta posee, es decir que ella una vez se descargue e instale trae consigo las vulnerabilidades ya conocidas en el mundo de la ciberseguridad, este herramienta es la que se desarrollará en el simulador con el sistema operativo Kali Linux.

14 A CONTINUACIÓN, DESCRIBA LOS DATOS E INFORMACIÓN DEL ANEXO 4 – ESCENARIO 3 QUE LE FUERON DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 7 X64.

Para el desarrollo de la actividad además para dar a conocer cómo se logra identificar las falencias que se presentaron en la empresa es importante dar a conocer que se desarrollan una serie de eventos en unas fases como son;

Fase de recolección de información: donde se recibe el informe del anexo 4 escenario 3, donde la empresa da a conocer lo que se evidenció o presento, además se da inicio a el análisis de la información allegada. Es de anotar que la evidencia inicial que se tiene, es que se presentó una fuja de información con dos equipos que cuyo sistema operativo es Windows 7 con la arquitectura x64.

Además, es necesario dar a conocer que este sistema operativo ya se encuentra obsoleto y no cuenta con actualizaciones desde el año 2020 por parte de Microsoft, debido a que este sistema operativo ya cumplió con el tiempo de servicio. Realizándose un análisis rápido se puede concluir que el uso de este sistema operativo por parte de la organización se convierte en un riesgo latente y permanente además que efectivamente estas vulnerabilidades son usadas para la fuja de la información de los atacantes.

Fase de búsqueda de vulnerabilidades: se puede decir que esta fase permite realizar una búsqueda detenidamente y minuciosa para observar y analizar qué fue lo que permitió en si la fuja de la información, según el informe suministrado por la empresa la vulnerabilidad se desato por parte del SMBv1 activo para compartir impresoras y algunos archivos dentro de la red.

Dado que el SMBv1[17] es un protocolo que si bien es cierto que permite compartir activos de información con las impresoras a su vez estando activo permite la fuja de la información, es decir de los archivos propios de la organización, según expertos de la ciberseguridad manifiestan que este tipo de protocolos no se

[16] Pastor Ricós, Fernando. Trabajo de grado titulado el Pentesting y generación de exploits con Metasploit. Consultado el (15 de agosto del 20229 trabajo realizado y actualizado en el año 2020.
[17] Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287). Artículo desarrollado el año del 2014. Consultado el (22 de septiembre del 2022) y puede ser consultado en internet a través de; https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

deben tener activos, como se evidencia en lo manifestado por parte de Pérez Gomez, según publicación del 28/06/2017 en su página de internet donde efectivamente, manifiesta que es un riesgo de alta vulnerabilidad toda vez que los sistemas pueden ser atacados o penetrados con la finalidad de hacer fuga de la información que contienen, dado esta situación era eminente que se desarrollará un ataque para realizar el hurto de los activos de los sistemas de cómputo de la empresa.

A continuación, se presenta lo manifestado por parte de expertos en ciberseguridad acerca del protocolo SMBv1 y el grado de dificultad que este tiene para hacer deshabilitado.

Sin embargo, en este caso (también con el anterior brote de WannaCry), se hacía mención del protocolo de comunicación SMB en su versión 1. Microsoft, además, recomendaba eliminar (o deshabilitar) la versión 1 de este protocolo de todos los equipos y servidores.

Merece la pena mencionar que esta versión tiene publicada una vulnerabilidad que los creadores de malware pueden aprovechar para atacar a los equipos de la misma red local donde se encuentra el equipo infectado inicialmente. Y, lo más importante, **todas las versiones de Windows tienen habilitado este protocolo por defecto**. Esto, en la práctica, lo que quiere decir es que un equipo infectado buscará en la red equipos que tengan activo SMB v1 y lo infectarán encriptando todos los archivos. Dicho en el sentido opuesto: si un equipo se infecta, no podrá propagarse por la red local si todos los equipos y servidores tienen desactivado SMB v1.

Dicho esto, la solución parece fácil: vamos a quitar el protocolo SMB v1. Pero… ¡siempre hay un pero!

En una red informática, habitualmente, no solo acceden al servidor los PCs o portátiles; hay otros dispositivos que deben interactuar con el servidor: por ejemplo, equipos multifunción que escanean documentos y los envían a alguna carpeta del servidor. Y el problema aparece cuando se comprueba que al deshabilitar el protocolo SMB v1, la multifunción deja de poder enviar documentos.

Ilustración 7 Deshabilitar el protocolo SMB v1 ¿por qué no es tan fácil? 28/06/2017 recuperado de https://japerezgomez.org/2017/06/28/deshabilitar-el-protocolo-smb-v1-por-que-no-es-tan-facil/

Es así como la vulnerabilidad se observa en mencionado protocolo que cumple con las funciones de enviar y compartir archivos con las impresoras[18], pero que

[18] Pérez Gómez José Antonio. Experiencias de un ingeniero del software. Deshabilitar el protocolo SMB v1 ¿por qué no es tan fácil? Articulo realizado el (28 de junio del 2017) consultado

a su vez permiten que exista fuja de la información en los activos de información dentro de una organización, como la que se estudia en el ejemplo objeto de la temática enviada por el docente.

15 ¿QUÉ HERRAMIENTA UTILIZÓ PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA "MÁQUINA WINDOWS 7"? ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

La herramienta que permite poder hacer el escaneo de los puertos y las IPS, es el software Nmap, además de poder hacer un escaneo en general de que dispositivos se encuentran en la red, debido a este software se realiza la detección de los equipos que de alguna manera se consideraban sospechosos que manejaban Windows 7 que por situaciones directamente de actualización y además de vulnerabilidad se observa que generan un riesgo constante y permanente.

De igual manera es de resaltar que en cuanto al puerto que abre la aplicación especifica en el anexo en el sistema operativo con el comando IP-CONFIG- permite la visualización de las IP, además que con los comandos netsat se podría visualizar los puertos abiertos, anexados en el estado de LISTENING dentro de la consola de Windows denominada (CMD).

16 EXPLIQUE CON SUS PALABRAS Y DE MANERA ESPECÍFICA CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64), HAGA USO DE GRÁFICOS PARA EXPLICAR EL ATAQUE.

Un atacante dentro de la red y una vez pueda evidenciar que equipos se encuentran dentro del sistema y haciendo uso de la verificación de los sistemas operativos con los que cuenta el quipo en el caso en particular de Windows 7, dado que este no tenía para el momento actualizaciones ni soporte alguno, es evidente el ataque y la vulneración.

Las vulnerabilidades para esta organización eran bastante toda vez que se encontraba realizando trabajos y desarrollos propios de la misma, con equipos y aplicaciones, obsoletas, sin poderse actualizar, además que no contaba con equipo de incidentes informáticos que pudiesen haber advertido y mejorado este tipo de riesgos.

Dado que la organización no cree que los activos de la información es decir los archivos extraviados o hurtados, hacen parte de lo más valioso ya que sin ellos la organización puede estar siendo dado en quiebra o su producto final, plagiado y puesto al mercado en un costo menos o mejorado en su calidad.

el (10 de septiembre del 2022) se puede consultar en https://japerezgomez.org/2017/06/28/deshabilitar-el-protocolo-smb-v1-por-que-no-es-tan-facil/

Debido a ello y al protocolo que estaba en uso en los diferentes equipos como es el SMBv1[19] además activo, permitió que el atacante se apropiara de una buena parte de activos de información de la organización como se evidencia en el grafico anexo así:

Ilustración 8 Imagen de como el atacante realizó la acción, fuente de lucichard.

Como se evidencia en la imagen o grafica una empresa con altos niveles de desarrollo y progreso[20] pero que lamentablemente dejo sin proteger sus activos de información, no le dio la importancia debida a los mismos y permitió que un atacante tomara el control de sus archivos por las ventanas abiertas que en esta oportunidad se podría manifestar y considerar que son los protocolos de SMv1 quedaron activos y los sistemas operativos Windows 7 obsoletos sin respaldo de actualización.

Seguidamente se permitió que se ejecutara el plan del atacante consiste en realizar el hurto de la información y que desde la distancia tomara archivos de la empresa, sin que fuera detectado y neutralizado ese ataque.

17 DOCUMENTE CADA UNO DE LOS PASOS QUE EJECUTÓ Y SUS RESPECTIVAS EVIDENCIAS PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS 7.

Para dar respuesta al presente interrogante es necesario manifestar que la organización Hackers Security, permite la simulación de los equipos y a su vez busca es que se demuestre como se realizó el ataque a sus sistemas de cómputo

[19] Pérez Gómez José Antonio. Experiencias de un ingeniero del software. Deshabilitar el protocolo SMB v1 ¿por qué no es tan fácil? Articulo realizado el (28 de junio del 2017) consultado el (10 de septiembre del 2022) se puede consultar en https://japerezgomez.org/2017/06/28/deshabilitar-el-protocolo-smb-v1-por-que-no-es-tan-facil/

[20] Lucichard; imagen realizada, recuperado de Imagen explicativa empresa: Lucidspark

así las cosas se proceden a realizar la ejecución de la explotación de las vulnerabilidades de los equipos del sistema operativo Windows 7.

Es necesario dar a conocer que se ejecuta la explotación mediante fases así:

Fase de Explotación de vulnerabilidades: se implementa el laboratorio simulado con la recreación del escenario, mediante la máquina virtual, dando inicio al sistema operativo de Windows 7 con la arquitectura x64 (victima) según informe de la empresa ellos fueron las victimas a quienes el atacante le hurto la información.

Estos sistemas operativos de los equipos víctimas se implementan dentro del mismo segmento de red, evidenciando como opera y trabajan los atacantes para hacer efectivo el hurto o la fuja de la información de la organización victima que se denomina Hackers Security.

Seguidamente se hace uso del software Nmap con el que se ejecuta el escaneo de los puertos que se encuentran dentro del segmento de red, además de los que se encuentran abiertos que permiten la vulneración y evidencian las falencias y fallos que el sistema está expuesto.

Fase de Post - explotación: en esta fase se permite evidenciar la manera en que el atacante desarrollo como tal el hurto de la información, como la empresa fue víctima de la fuga de la información, además que alcance podría tener el atacante hasta donde pudo penetrar, dentro de los sistemas de cómputo de la organización, si ingreso con usuario de dominio, de administrador tuvo el alcance de poder tomar y tener el control de información privilegiada entre otros aspectos de relevancia.

Para terminar la ***fase del informe***: que es donde el auditor informa lo encontrado mediante la ejecución de las fases, en este caso es evidente que la empresa carecía de la implementación de un sistema de seguridad de la información, con unas políticas claras y precisas del cómo mantener segura la información de la organización.

Seguidamente para la explotación de las vulnerabilidades se desarrolló en el simulador las siguientes actividades así;

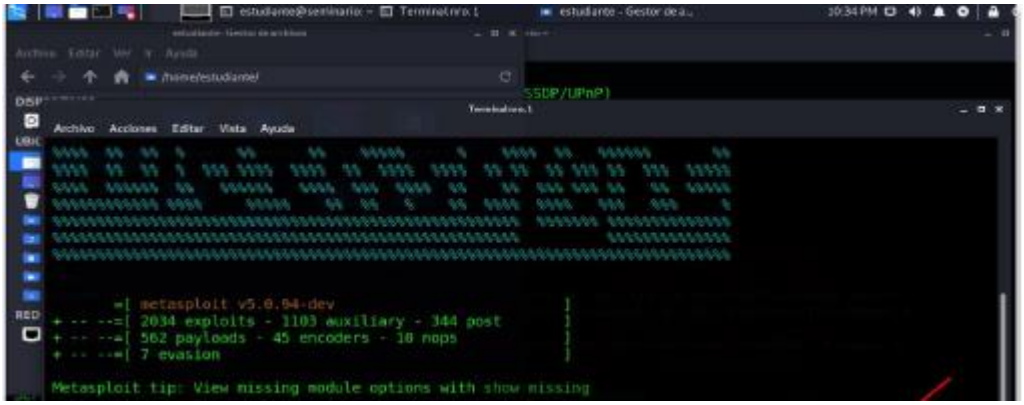

Ilustración 9 Metasploit de Windows 7

Se observa el desarrollo del software de Metasploit con el que se dará inicio y ejecución de la actividad de simulación del laboratorio para llevar a cabo la explotación de las vulnerabilidades[21].

Seguidamente se debe ingresar a la base de datos de la herramienta para ingresar al contenido de los exploits, es decir de las vulnerabilidades ya conocidas por parte de los softwares. A continuación, se procede a cargar el payload con la finalidad de que una vez se lleva a cabo la explotación de las vulnerabilidades en los equipos en este caso el servidor se haga lo que se conoce como una conexión reversa al equipo atacante, en el simulador es el sistema operativo Kali Linux.

Una vez se lleva a cabo y se realiza el paso a paso anteriormente ejecutado con el nombre del archivo como es el “winse20w0.exe”[22] se podrá explotar la vulnerabilidad. Seguidamente se evidenciará la vulnerabilidad de cómo la misma se ejecutará del código en el respectivo servidor, mediante el CMD (de Windows consola de programación o de comandos), con el comando Shell.

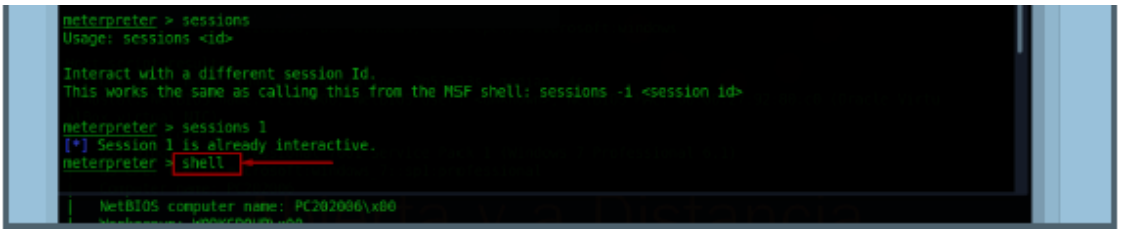

Ilustración 10 Ejecución del comando shell en Windows 7

[21] Salomón David; Data Privacy and Security: Encryption and Information Hiding; Departtment of Computer Science, California State Unvirsity, Northridge, Recovered from; https://books.google.es/books?hl=es&lr=&id=z-3foyEoo-UC&oi=fnd&pg=PR9&dq=security+of+the+information&ots=5DY6HKdbHT&sig=RJbE-VmZ_aotasE37DxDBIzoWTs#v=onepage&q&f=false

[22] Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). CVE-2014-6287CVE-111386. 2016.
https://www.exploit-db.com/exploits/39161
https://www.exploit-db.com/exploits/34852

Seguidamente con el acceso al equipo atacante se procede a llevar a cabo la recolección de los activos de información, donde se observa que el atacante ya se encuentra con acceso en el equipo de la víctima en este caso en particular en los equipos del Windows 7, que presentan la vulnerabilidad.

Seguidamente se inserta el comando de ipconfig y seguidamente se realiza la acción desde el equipo de Windows 7 para visualizar las IPS del sistema atacante como lo evidencia la gráfica.

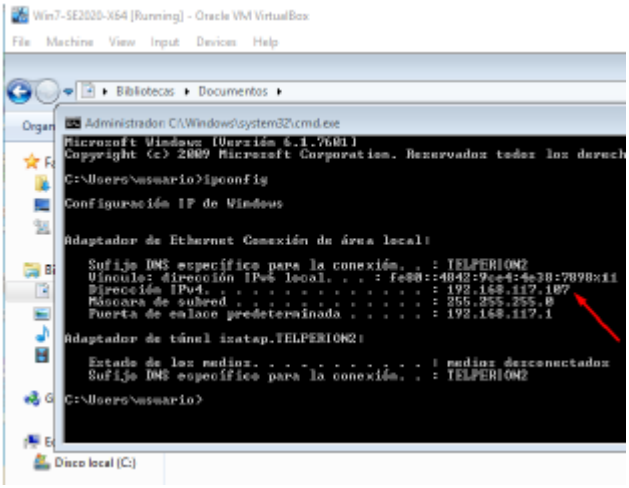

Ilustración 11 IPS del equipo víctima

Donde se permite la visualización de que IPS, se encuentran en el segmento y además el control del equipo.

Para terminar, se realiza el POC con el primer nombre del estudiante Gamaliel y el primer apellido Muñoz como lo solicita la guía y rubrica de evaluación, además que efectivamente se presenta una falla en el sistema y los equipos de cómputo de la organización y presentarse ante los altos directivos como muestra de lo realizado.

18 ETAPA 4 CONTECIÓN DE ATAQUES INFORMÁTICOS

19 ¿QUÉ SERÍA LO PRIMERO QUE INDAGARÍA Y HARÍA SI LLEGARA A ENCONTRARSE UN ATAQUE EN TIEMPO REAL? ESPECIFIQUE SU RESPUESTA CON ARGUMENTOS TÉCNICOS.

Para dar respuesta a este interrogante se plantea una serie de actividades a desarrollar como son;

Monitoreo; para poder hacer el monitoreo previamente se debe contar con softwares o hardware, que permitan realizar el monitoreo de una forma amplia y organizada, a su vez que este sea efectivo, capaz de mostrar posibles afectaciones e intrusos en la red, que se evidencia la normalidad o lo anormal la irregularidad de alguna actividad dentro de los sistemas de cómputo.

Alerta; se debe contar con un sistema que informe en tiempo real lo que acontezca, ya sea alarma o de alerta, para que el personal que se encuentre en la zona a proteger este informado además se tomen las acciones correspondientes.

Identificación; este hace alusivo de que lo que se evidencie ya sea en el monitoreo o alarma, con este sistema se pueda desarrollar la actividad de identificar el atacante, el origen entre otros aspectos de relevancia.

Contención; posterior a las otras etapas es necesario contar con un sistema que permita contener o mitigar el inminente ataque que se está desarrollando o se prevé que va hacer victima la infraestructura.

Proteger; desarrollar un sistema de protección de los diferentes activos de información del sistema o de las herramientas puestas al servicio de la organización.

Responder: esta actividad es la que permite hacer o ejecutar una serie de actividades tendientes a hacerle frente al atacante y con las mismas de forma contundente mitigar el daño y cerrar las puertas o ventanas que permitan la fuga de información.

Recuperar; esta es las herramientas encargadas de resolver y dar tranquilidad a la organización cuando es víctima de un ataque, que sea capaz de controlar y volver todo a la calma, generando los respectivos soportes que permitan esclarecer mediante una investigación lo sucedido.

20 ¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM QUÉ MEDIDAS DE HARDENIZACIÓN PROPONDRÍA PARA QUE EL ATAQUE NO SE REPITA?

Para dar respuesta al presente interrogante que se plantea por parte del docente, es necesario dar a conocer que se debe tener presente las siguientes actividades así;

- Actualización desde el desarrollador o controlador de los sistemas operativos con los que cuenta las herramientas de la organización (computadores, smartphone, tablets, portátiles entre otros).

- Un parcheo constante a las vulnerabilidades detectadas, en lo posible eliminación de las mismas o generar control permanente.

- Mantener la opción de acceso remoto desactivada.

- Ejecutar las diferentes actividades con usuario de dominio y no de administrador.

- Mantener los antivirus actualizados, de todo el componente tecnológico.

- Actualizar los escudos protectores, no hacer entrega de dominios a personal ajeno a la organización.

- Manejo de herramientas capaces de ofrecer una seguridad perimetral, escudos protectores como el firewall activo y prestos a enfrentar un eventual ataque y mitigarlo.

- En lo posible manejar la información privilegiada con encriptación, códigos de seguridad y plataformas seguras y no al público en general.

- Manejo de las herramientas que permitan generar alertas, seguimientos, entre otros aspectos capaces de brindar seguridad en la información.

Es de anotar y resaltar que en cuanto al hardening este se puede llevar a cabo desde varias, capas, desde el perímetro local, hasta los equipos de almacenamiento o servidores como son;

- ***Perímetro;*** es la integración de posibles soluciones de protección mediante servicios como aplicaciones web, las políticas de los firewalls, que permiten proteger el acceso de las redes mediante la detección de las IP entre otros servicios.

- ***Zona de DMZ;*** es la integración del servidor con los equipos con un alto nivel de riesgo.

- ***Endpoint***: punto que se conoce como el final del destino de una conexión.

- ***Firewall***; elementos de un alto contenido de protección perimetral dentro de una red, además son políticas establecidas por el desarrollador del mismo.

- ***UTM;*** dispositivo de redes capaz de unificar las amenazas, se debe manejar un solo proveedor del mismo con la finalidad de manejar las políticas de control, gestión y manejo de los servicios de seguridad.

- ***NGFW;*** dispositivo de seguridad de última generación[23], cuenta con un servicio capaz de brindar una seguridad a un alto nivel de confiabilidad.

[23] Mendoza Marco, Hacking y más. Las mejores bases de datos de exploits para investigadores de seguridad, consultado el (26 de septiembre del 2022) puede ser consultado en internet: https://hackingymas.com/lasmejores-bases-de-datos-de-exploits-para-investigadores-de-seguridad/

- ***Firewall de las bases de datos;*** es una herramienta que en su nombre manifiesta que es exclusivo para brindar una seguridad efectiva[24], eficaz, para las bases de datos ya que cuenta con restricciones del tráfico y emplea unas políticas estrictas para ingresar a las bases de datos. Mitigando una amenaza o un ataque a las mismas.

21 ¿DESCRIBA CON SUS PALABRAS LAS DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS?

Para dar respuesta al presente interrogante es necesario dar a conocer que el Blue Team hace una defensa de seguridad de los activos de la información, basándose en hallazgos del Red Team de una forma que es proactiva.

Teniendo en cuenta la seguridad perimetral, las diferentes políticas de la seguridad, las políticas con fines preventivos de los llamados intrusos (IPS) y las políticas de WAF, con la finalidad de brindar una amplia protección de los servicios de la web.

En cuanto a la seguridad de las DMZ, permite el aislamiento de manera automática de los diferentes servidores comprometidos e inmersos a una contención del atacante.

Seguidamente en cuanto a la seguridad de los edpoint, permite la integración de las herramientas de la seguridad en la correlación de los diferentes eventos, se evidencia que el Blue Team, mantiene de forma permanente una seguridad constante sobre los diferentes sistemas de cómputo y de la red en general.

En cuanto a los llamados equipos de respuesta a los incidentes informáticos (CSIRT-CERT) son aquellos que se organizan por parte de las entidades ya sean públicas o privadas, con fines únicos de atender un incidente informático que se presenta además ser fuente de información para la recepción y atención de los incidentes que se presenten al interior de la organización. Debido a lo manifestado sus funciones se encuentran de la siguiente manera así:

- Dar a conocer información sobre hallazgos.

- Alertar de forma permanente las vulnerabilidades a las que puede verse inmersa la organización.

- Dar instrucción y hacer entrega de como mitigar una amenaza e incluso hacer entrega de pautas para la configuración de las herramientas puestas al servicio de la organización.

- Gestionar los diferentes incidentes informáticos de la organización.

[24] Opennac- solución NAC de código abierto, consultado el (01 de octubre del 2022) puede ser consultado mediante internet a través del link: http://www.opennac.org/opennac/en/solution/screenshots-opennac.htmlOpen

- ❖ Por último, gestionar las diferentes vulnerabilidades que se presentan en la empresa.

22 ¿SI DENTRO DE UN EQUIPO BLUETEAM LE INDICAN QUE DEBE TRABAJAR CON CIS "CENTER FOR INTERNET SECURITY" USTED LO UTILIZARÍA PARA QUÉ FIN?

Para dar respuesta al presente interrogante es preciso y necesario manifestar que es CIS, en ingles Center for Internet Security[25], en español centro de seguridad en internet, es el principal estándar reconocido a nivel mundial por parte de las industrias con finalidad de configuración segura, además desarrolla listas de verificación con fines de ayuda para identificar y mitigar las vulnerabilidades de seguridad.

Además, genera un banco de información útil para todo el sector de la ciberseguridad, que es utilizado con fines de conocer, mitigar y prevenir ser víctimas de hurto, fuja de información en las pequeñas, medianas y grandes organizaciones.

Ya conociendo que es CIS, desde luego que laboraría con este tipo de políticas, puesto que son de gran ayuda y de gran importancia en el sector de la seguridad de la información, poniéndolas en ejecución la organización gana y apropiarse de las mismas hace que una empresa, mantenga un gran nivel de seguridad y este a la vanguardia de seguridad.

23 EXPLIQUE Y REDACTE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LO QUE ES UN SIEM.

En cuanto a que es un SIEM (Security Information and evento Management) en ingles lo que en español traduce a Gestión de Eventos e Información de Seguridad[26], es un software que lo que realiza es la recopilación, además el monitoreo de los diferentes logs de las herramientas tecnológicas y los elementos de seguridad.
Los SIEM están en la capacidad de realizar una serie de actividades de seguridad en los activos de información como son:

- ✓ Centralizar los activos de información sobre las posibles amenazas.

[25] Salomón David; Data Privacy and Security: Encryption and Information Hiding; Departtment of Computer Science, California State Unvirsity, Northridge, Recovered from; https://books.google.es/books?hl=es&lr=&id=z-3foyEoo-UC&oi=fnd&pg=PR9&dq=security+of+the+information&ots=5DY6HKdbHT&sig=RJbE-VmZ_aotasE37DxDBIzoWTs#v=onepage&q&f=false

[26] Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). CVE-2014-6287CVE-111386. 2016.
https://www.exploit-db.com/exploits/39161
https://www.exploit-db.com/exploits/34852

- ✓ Llevar a cabo la determinación que las amenazas, son verdaderas y de no ser pues desecharlas.
- ✓ Escalar la temática a los diferentes analistas de la información, para que se resuelva la vulnerabilidad lo antes posible.
- ✓ Documentar la situación presentada con fines de organizar base de datos, para solución de futuras situaciones similares.
- ✓ Documentar en informe de auditoría los incidentes informáticos presentados a su vez la solución que se dio al mismo.
- ✓ Dar cumplimiento en la totalidad de las regulaciones según ley vigente de protección de datos.

Existen una serie de SIEMS, como son los de open source, que es intuitivo, fácil de instalar, otra ventaja del software que es gratuito, ejemplo de un SIEM Open Source.

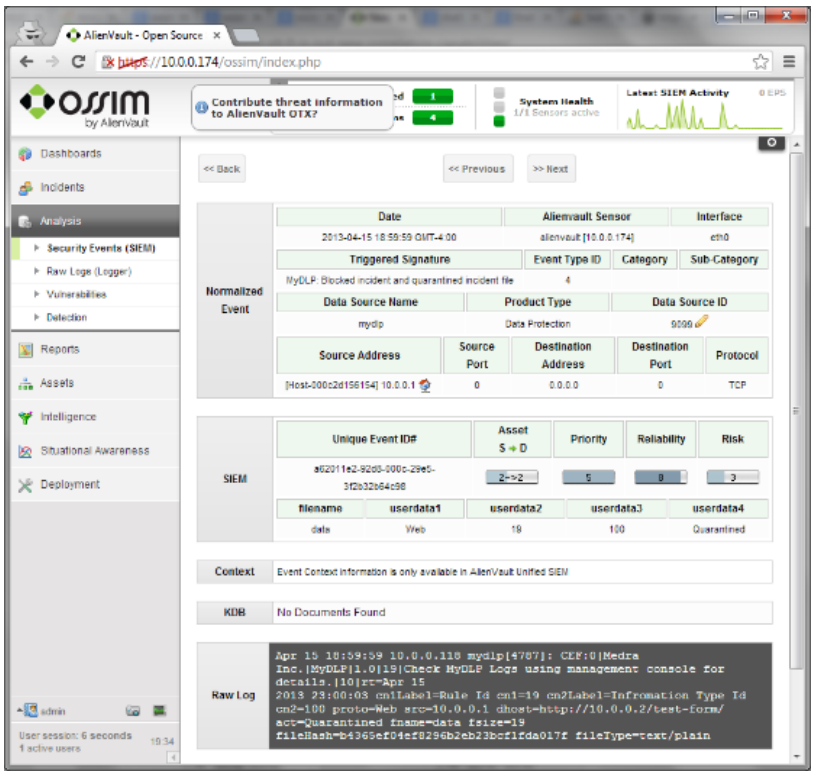

Ilustración 12 Ejemplo SIEM Open Source con OSSIM de Alien Vault recuperado de https://mydlp.com/mydlp-ossim/

SIEM comercial: es de carácter privado, desarrollado por parte de empresa netamente privada, es extenso, el soporte y actualización está a cargo del fabricante, ejemplo de SIEM comercial.

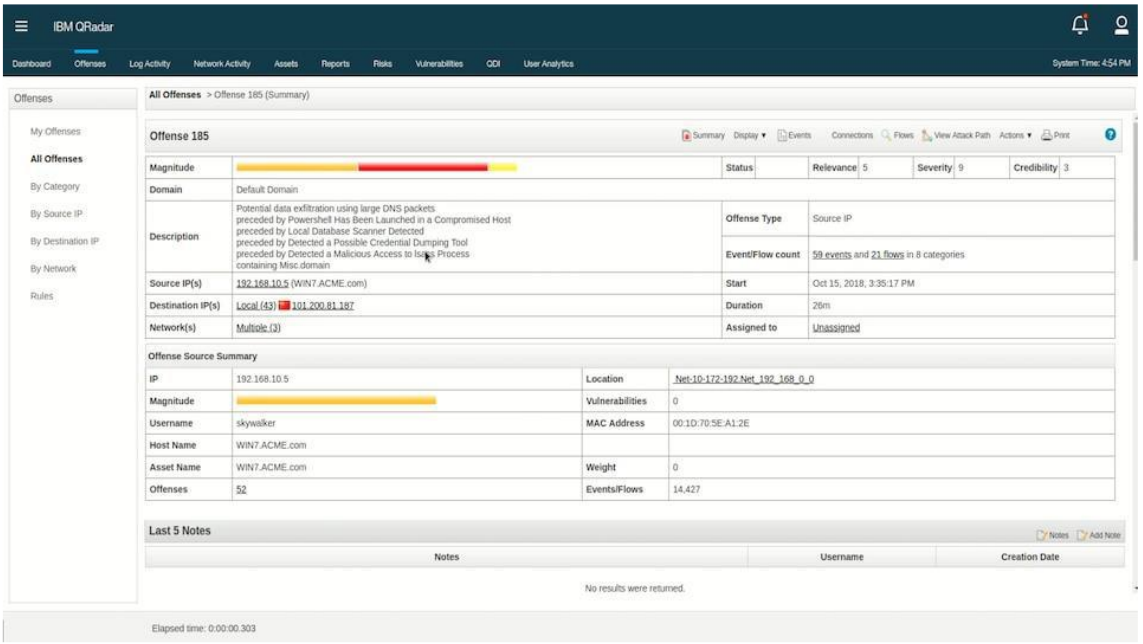

Ilustración 13 Ejemplo SIEM comercial -IBM QRadar fuente https://itbutler.com.au/qradar/

Como se visualiza en la imagen es un tipo de SIEM, comercial privado, que tiene un costo para su uso y de igual manera cuenta con un respaldo y actualización.

24 DEFINA POR LO MENOS 3 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS “HARDWARE O SOFTWARE”, RECUERDE QUE LAS HERRAMIENTAS DE CONTENCIÓN SON DIFERENTES A LAS HERRAMIENTAS DE DETECCIÓN.

Para dar respuesta al presente interrogante se procede a analizar los siguientes softwares que a continuación se dan a exponer así;

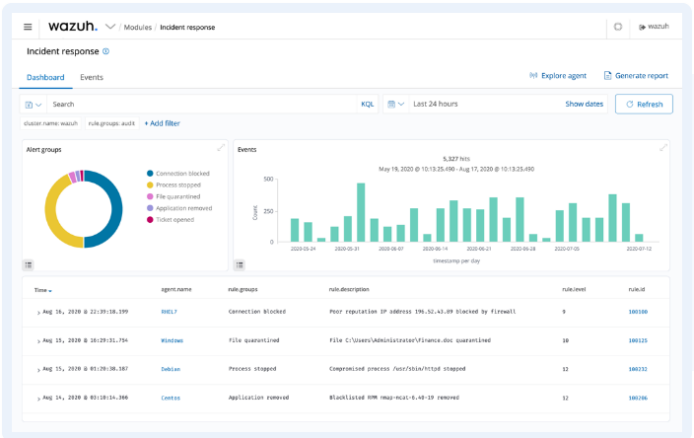

Ilustración 14 Interface Wazuh Fuente: https://wazuh.com/

WAZUH EDR (Endpoint Detection and Response); es un software y herramienta que permite analizar la correlación en tiempo real, alcanzando una remediación en los dispositivos se mantengan protegidos, limpios y activos.

Otro de los softwares a tener presente en este informe es uno de los más comunes como se relaciona a continuación así;

OSSEC (IDS); Es un software, que permite el desarrollo de unas actividades con el fin de realizar correcciones a eventos, con capacidades permanentes de monitoreo, análisis de las diferentes vulnerabilidades y con una respuesta automatizada de las amenazas.

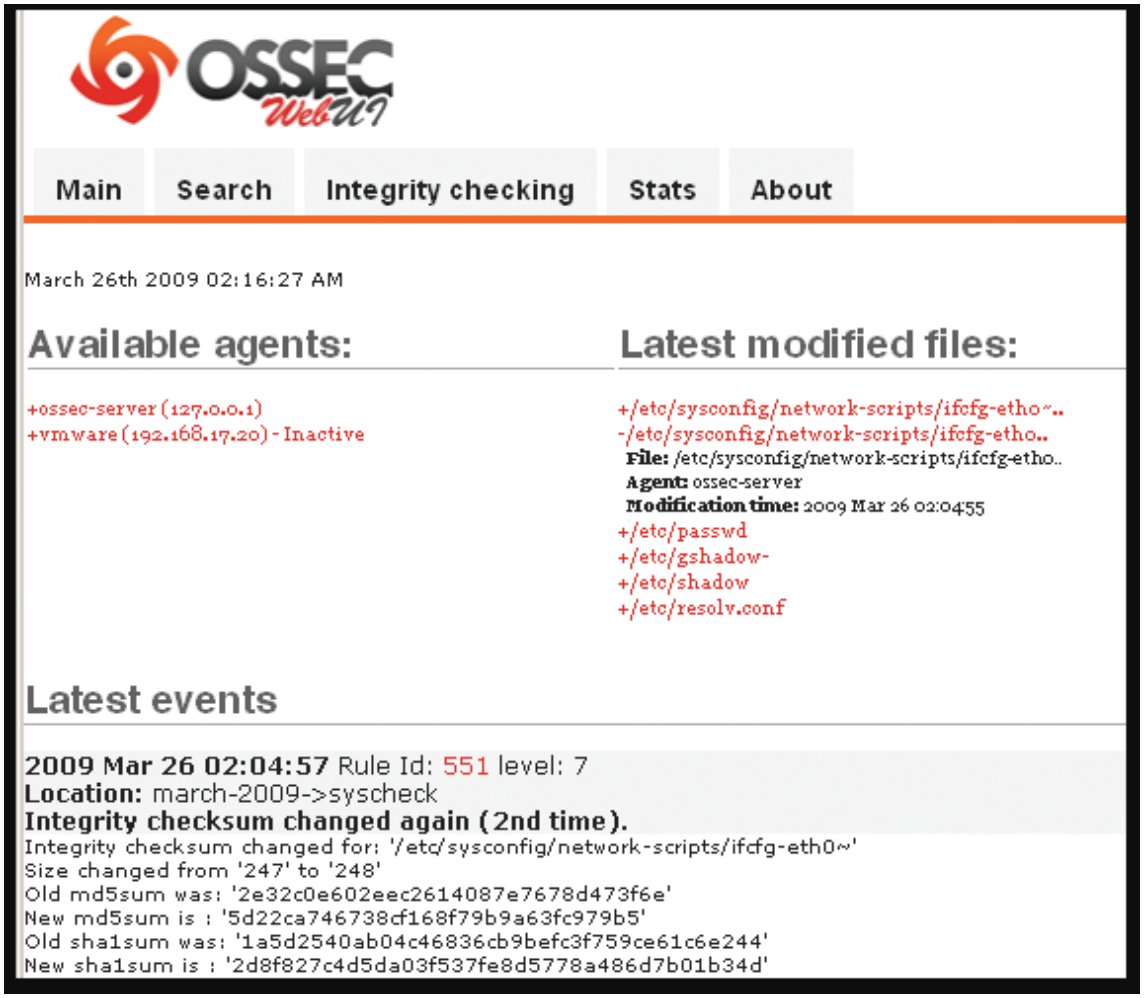

Ilustración 15 interfaz server OSSEC fuente http://2.bp.blogspot.com/-ZcuFMvaffeg/T1eMQ9gX_cI/AAAAAAAAAGU/bEIx12RD_gQ/s1600/Figure-1.png

Por último, el software **Open NAC (NAC – Network Access Control);** es una herramienta

Open NAC (NAC – Network Access Control)
Esta herramienta su funcionalidad es integrar con otras herramientas de análisis con fines de detectar en los componentes tecnológicos, anomalías o alertas que refieran actividades de interés y necesarias de corregir ya que se observan comportamientos anómalos, de ser necesario se debe colocar el equipo de cómputo en cuarentena o aislarlo de la red, entre otras políticas que brinden seguridad en los activos de información.

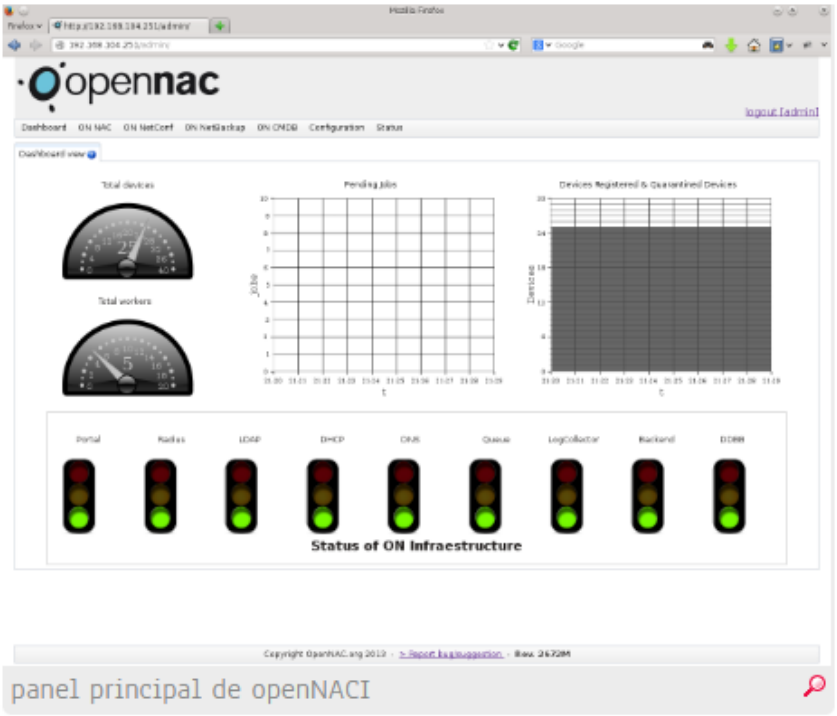

Ilustración 16 interfaz de gestión openNAC fuente http://www.opennac.org/opennac/en/solution/screenshots-opennac.htmlOpen

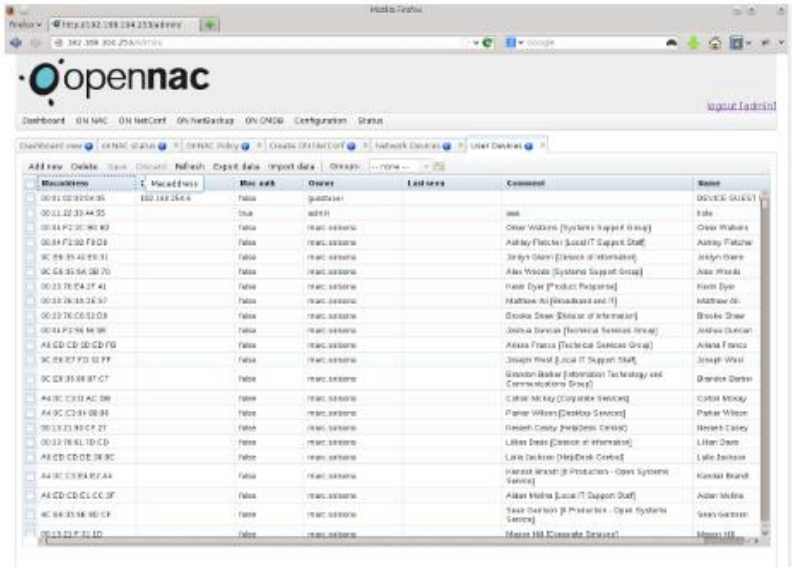

Ilustración 17 Pantalla de gestión de dispositivos de usuario fuente; http://www.opennac.org/opennac/en/solution/screenshots-opennac.htmlOpen

En la imagen se visualiza la pantalla de gestión de los diferentes dispositivos mediante el software opennac[27].

[27] Opennac- solución NAC de código abierto, consultado el (01 de octubre del 2022) puede ser consultado mediante internet a través del link: http://www.opennac.org/opennac/en/solution/screenshots-opennac.htmlOpen

25 ETAPA 5 SOCIALIZACIÓN DE INFORME TÉCNICO

26 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM.

Para dar respuesta al presente interrogante es necesario dar a conocer que efectivamente la importancia de este tipo de actividades e implementación lo que en sí realiza es el aprovechamiento de los conocimientos de la totalidad del recurso humano, además la verificación de las herramientas que se tienen para identificar, analizar y contrarrestar las amenazas, vulnerabilidades de los sistemas de información.

Buscando en todo momento la mitigación, de la amenaza, el riesgo latente de existe ser víctima de fuga de información mitigarlo y reducirlo al máximo, además de eliminar toda actividad que atente o genere riesgo en las redes e infraestructura dentro de una organización, el RedTeam, y BlueTeam lo que buscan en si es poder generar actividades en pro y beneficio de una organización; aunque tengan estrategias, metodologías, diferente su finalidad es una sola.

Por último, es necesario agregar que las estrategias de los equipos de RedTeam, y BlueTeam, buscan evitar siempre al máximo que las organizaciones, empresas sean victimas de hurto o fuja de información, mediante la identificación de las diferentes vulnerabilidades y mitigación de los riesgos que se evidencian en la organización.

27 RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN.

Para dar respuesta al presente interrogante es necesario dar a conocer que el planteamiento de las diferentes estrategias para mejorar la seguridad de las herramientas tecnológicas, puestas al servicio y en pro de la empresa requiere de unas políticas de seguridad de la información que se desarrollarán y darán a conocer en los siguientes criterios.

- ***Mantener actualizado los sistemas operativos:*** aspecto que se debe mantener en todo instante, dado que no hacerlo puede ser vulnerable, generando, riesgos y amenaza con posible ataque ante el sistema, de no tener actualización, este sistema es vulnerable y debe ser cambiado dentro de la máquina que se está usando.

- ***Parcheo de verificación de vulnerabilidades:*** es necesario mantener activo un software que permita realizar y verificar las vulnerabilidades del sistema que se usa en la organización, con la finalidad de detectar las vulnerabilidades y tomar decisiones que permita mitigarlas.

- ***Activación de antivirus:*** se debe mantener software de protección lo que se conoce como antivirus, pero que estos se encuentren siempre activos y con licencias vigentes, fin alertar y no permitir que softwares malignos, malwares quieran ingresar al sistema y apoderarse de los activos de información.

- ***Firewall:*** hacer uso de licencias vigentes de herramientas de seguridad perimetral DMZ, UTM, que permitan generar de manera positiva escudos protectores dentro del sistema, además que mitiguen y eliminen malwares o cualquier activa que se alerte como peligro u amenaza dentro del sistema.

- ***Hacer uso de la encriptación:*** cuando los activos de información se requieren enviar o almacenar y son de carácter confidencial, lo ideal es hacer uso de la encriptación es decir hacerlos con código que solo el remitente y destinatario los conozcan y en el momento que se requieran puedan descifrar.

- ***Implementar el SGSI:*** es necesario que en las organizaciones se desplieguen los diferentes paso a paso, para encaminarse a la implementación del sistema de gestión de seguridad de la información, dado que con este sistema se desarrollaría la mejora continua en cuanto a capacitación de los empleados y usuarios dentro de la empresa, conocimiento a aplicar con fines de no permitir dejar abiertas las ventanas o el segmento para que, hackers no éticos atenten o busquen penetrar en el sistema.

28 CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.

- Para un profesional en el área de seguridad de la información requiere conocer cuales son los delitos tipificados como informáticos por la justicia en este caso por Colombia, como aquellos que se denominan en la ley 1273 -2009 donde se crea un daño antijuridico y se modifica la ley 599 del 2000 Código Penal Colombiano.

- Llevar a cabo el desarrollo de actividades de simulación en entornos que se asemejan a la realidad es de vital importancia toda vez que se adquiere un conocimiento amplio del como se va a comportar el sistema en una penetración o pentesting; como detener el ataque o mitigarlo es relativamente importante y necesario.

- Estar a la vanguardia en un sistema dentro de una red, comprender que por el hecho de permitir que una aplicación se ejecute o se desarrolle, dentro de un sistema obsoleto, la vulnerabilidad, el riesgo que se genera es constante y no se debe permitir, puesto que puede ocasionar una

perdida considerable de los activos de información; un riesgo que de ser desarrollado y llevado con éxito el ataque puede ocasionar perdidas de información incalculables.

- Conocer que normatividad acobija, protege a las organizaciones a que no sean victimas de hurto o fuja de información, es necesario puesto que se podría en un futuro tener presente cuando sea víctima de un ataque; de hurto de la información, para desarrollar el paso a paso conforme lo estipula la norma, para aportar en una investigación de la cual se pueda extraer y ejecutar la explotación, ubicando al posible delincuente que atento y hurto información.

- Por último, la información y las actividades desarrolladas en el seminario hacen que el profesional este en la capacidad de resolver los futuros casos o problemas dentro de una empresa u organización.

29 LINK VIDEO PRESENTACION

https://screencast-o-matic.com/watch/c3623jVtJ2G

25 PANTALLAZO DEL SOFTWARE TURNITIN

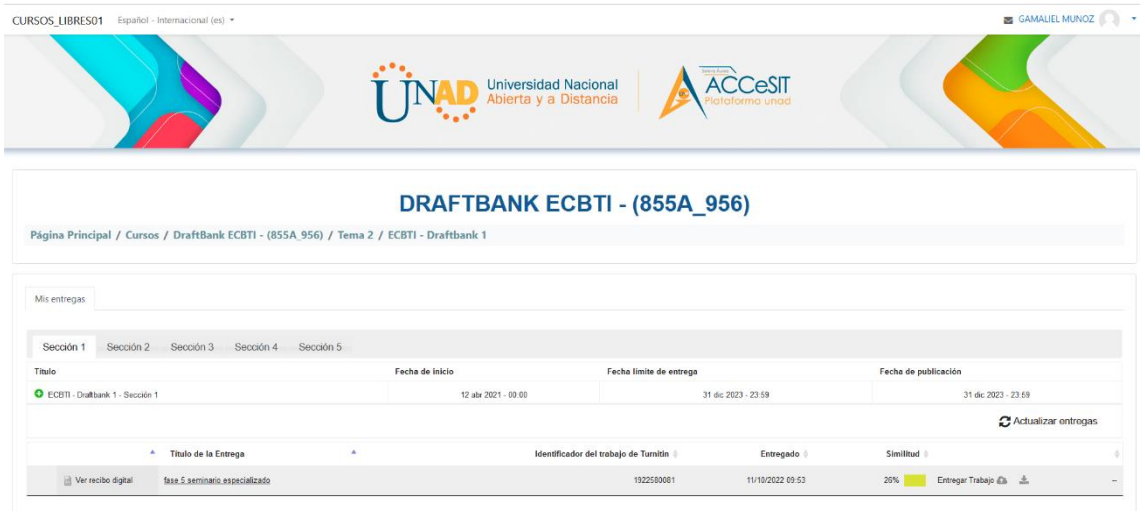

Ilustración 18 pantallazo del software Turnitin

CONCLUSIONES

Es de vital importancia el desarrollo de las diferentes actividades establecidas mediante la guía y rubrica de evaluación, toda vez que con ellas se logra adquirir un aprendizaje amplio sobre la temática objeto de estudio, analizar el contexto de como una empresa puede estar siendo mal dirigida y desconocer estas fallas pueden ser causales de una quiebra o eventual perdida de balance que la lleve a la banca rota.

La información en las organizaciones se debe considerar como un activo valioso, teniendo en cuenta que es de vital importancia pues se encuentra datos confidenciales de los diferentes clientes internos y externos, debe ser un objetivo principal para la organización, del cómo cuidar los activos de información, elevarlos a título de tesoro importante y de un precio incalculable, pues la norma ISO 27001:2013 debe ser implementada y convertirla en un escudo protector de toda organización.

Darle la importancia a la actualización de las herramientas puestas al servicio tanto para el cliente interno como externo, hacer la inversión en pro de la mejora de los sistemas de red, de cómputo y de la oficina de desarrollo tecnológico puesto que es uno de los pilares de la empresa.

BIBLIOGRAFÍA

Ávila Guadrón, Miguel Andrés. Estudio de las mejores prácticas de Ethical Hacking. Trabajo de grado para generar un nuevo método que facilité la ejecución de análisis de seguridad enfocados a pruebas de penetración. Desarrollado en el año 2018 paginas 65-70.

Cita de documentos y centros de seguridad TIC. Conselleria de Hacienda y Modelo Económico, Valencia España. CSIRT-CV Aplicaciones: (año 2021) Acceda y consulte todas nuestras aplicaciones que ponemos a su disposición. Consultado el 20 de agosto de 2022. 14:15 disponible en https://www.csirtcv.gva.es/

Ciberseguridad, Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas, ¿qué es cve? explicación de las vulnerabilidades y exposiciones comunes, consultado (el 15 de septiembre del 2022). Disponible en: https://ciberseguridad.com/herramientas/marco-mitreatt-ck/cve-vulnerabilidades-exposiciones-comunes/

COLOMBIA. CONGRESO DE LA REPÚBLICA. Constitución Política de Colombia, (4 de julio de 1991), por la cual se actualiza la Constitución Política de Colombia. Consultado el (01 de agosto del 2022) publicado mediante el Diario Oficial Nro. 52143 del (31 de agosto de 2022) puede ser consultado mediante el siguiente internet: http://www.secretariasenado.gov.co/constitucion-politica

COLOMBIA. CONGRESO DE LA REPÚBLICA. Código de ética para ingenieros mediante la ley 842 del año 2003 Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Etica Profesional y se dictan otras disposiciones, (9 de octubre del 2003). Consultado el (25 de agosto del 2022) el cual puede ser consultado en https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

COLOMBIA. CONGRESO DE LA REPÚBLICA. Derechos de autor sobre la ley 23 del (20 de enero de 1982), “ley sobre derechos de autor”. Diario oficial Nro. 35949 del (19 de febrero de 1982) consultado el (24 de agosto del 2022) puede ser consultado en internet del link: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30035790

COLOMBIA. CONGRESO DE LA REPÚBLICA. reglamenta el acceso y uso de los mensajes de datos mediante la Ley 527 del (18 de agosto 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” consultado el (22 de agosto del 2022) puede ser consultado en internet: https://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013

COLOMBIA. CONGRESO DE LA REPÚBLICA. Código penal de Colombia mediante la Ley 599 del (24 de julio del 2000) “Código Penal Colombiano”,

mediante la cual se tipifica el Código Penal de Colombia", consultado el (20 de agosto del 2022) puede ser consultado mediante el internet: https://www.oas.org/dil/esp/codigo_penal_colombia.pdf

COLOMBIA. CONGRESO DE LA REPÚBLICA. Creación del nuevo daño antijuridico mediante la ley 1273 del (05 de enero del 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". Consultado el (23 de agosto del 2022) se puede consultar en internet;* ***https://www.lexbase.co/lexdocs/indice/2009/l1273de2009#:~:text=%22%20LEY%201273%20DE%202009%20(enero,y%20las%20comunicaciones%2C%20entre%20otras***

DENIS, Matthew; ZENA, Carlos; HAYAJNEH, Thaier. Penetration testing: Concepts, attack methods, and defense strategies. Trabajado de grado realizado En (2016 mediante el formato IEEE) Long Island Systems, Applications and Technology Conference (LISAT). IEEE, se consulta el 25 de septiembre del 2022). Páginas. 1-6.

EL TIEMPO (23 de enero del 2015). Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [En línea]. Consultado el (25 de agosto del 2022) puede ser consultado en internet en: https://www.eltiempo.com/archivo/documento/CMS-15141236

Felipe Hostingplus. Artículo de Qué es NMAP y para qué sirve, consultado el (20 de agosto de 2022) desarrollado el (09 de noviembre del 2021), puede ser consultado en internet: https://www.hostingplus.com.co/blog/que-es-nmap-y-para-que-sirve/

Jagrey FunInformatique- Ahmed publicado el (13de agosto de 2022). Metasploit: ¿qué es y cómo usarlo? Consultado el (20 de agosto del 2022) el cual puede ser consultado desde el: https://www.funinformatique.com/es/que-es-metasploit-y-como-usarlo-bien/

Lucichard; imagen realizada, recuperado de Imagen explicativa empresa : Lucidspark

Mendoza Marco, Hacking y más. Las mejores bases de datos de exploits para investigadores de seguridad, consultado el (26 de septiembre del 2022) puede ser consultado en internet: https://hackingymas.com/lasmejores-bases-de-datos-de-exploits-para-investigadores-de-seguridad/

Naval research lab washington dc center for high assurance computing systems; Security Models and Information Flow, consulted (August 22, 2022) and can be consulted through the internet:https://apps.dtic.mil/sti/citations/ADA462529

NMAP, software consultado (09 de agosto del 2022) puede ser descargo el software mediante internet a través de: https://nmap.org/download#linux-rpm

Niño Ordoñez, José Rafael, artículo sobre las Capacidades Técnicas, Legales y de Gestión para Equipos BlueTeam y RedTeam. Consultado el (29 de septiembre del 2022) fue publicado en el 2020.

Opennac- solución NAC de código abierto, consultado el (01 de octubre del 2022) puede ser consultado mediante internet a través del link: http://www.opennac.org/opennac/en/solution/screenshots-opennac.htmlOpen

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, consultado el (01 de octubre del 2022) páginas de la 11(28).

Pastor Ricós, Fernando. Trabajo de grado titulado el Pentesting y generación de exploits con Metasploit. Consultado el (15 de agosto del 20229 trabajo realizado y actualizado en el año 2020.

Pérez Gómez José Antonio. Experiencias de un ingeniero del software. Deshabilitar el protocolo SMB v1 ¿por qué no es tan fácil? Articulo realizado el (28 de junio del 2017) consultado el (10 de septiembre del 2022) se puede consultar en https://japerezgomez.org/2017/06/28/deshabilitar-el-protocolo-smb-v1-por-que-no-es-tan-facil/

Peñaredonda José Luis Enter.co. Detrás de Buggly: la historia de la fachada Andrómeda, transformación digital realizado el (09 de diciembre del 2015) consultado el (25 de agosto de 2022) puede ser consultado mediante internet: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). CVE-2014-6287CVE-111386. 2016.
https://www.exploit-db.com/exploits/39161
https://www.exploit-db.com/exploits/34852

Rejetto HFS versions 2.3, 2.3a, and 2.3b are vulnerable to remote command execution.2014., recuperado de; https://www.kb.cert.org/vuls/id/251276

Salomón David; Data Privacy and Security: Encryption and Information Hiding; Departtment of Computer Science, California State Unvirsity, Northridge, Recovered from; https://books.google.es/books?hl=es&lr=&id=z-3foyEoo-UC&oi=fnd&pg=PR9&dq=security+of+the+information&ots=5DY6HKdbHT&sig=RJbE-VmZ_aotasE37DxDBIzoWTs#v=onepage&q&f=false

Salazar, J. F. Situación normativa de la Sociedad de la Información en Colombia. Trabajo desarrollado en el año (2011). Consultado el (15 de septiembre del 2022) Criterio Jurídico, páginas de la 9-11.

Steven Fuernell; why users cannot use security; network research group, school of computig, comunications and electronics, university of Plymouth, united kingdom; Recovered from; https://reader.elsevier.com/reader/sd/pii/S0167404805000532?token=C9499637E55199C153206B9AF75451CD86D47576F1CD00C88F78E1F12A1FA1090B3A822D631C5C06DF91EC5B28D5EF5D&originRegion=us-east-1&originCreation=20221008220543

Security vulnerabilities of Rejetto Http File Server: List of all related CVE security vulnerabilities, recuperado de; https://www.cvedetails.com/vulnerability-list/vendor_id-14180/product_id-29196/Rejetto-Http-File-Server.html

TINOCO LINARES, Ana, et al. Trabajo de grado de Análisis y clasificación de los ataques y sus exploits: Framework Metasploit como caso de estudio. Desarrollado en el año 2020. Consultado el (28 de septiembre del 2022). Paginas de 19-22.

Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287). Artículo desarrollado el año del 2014. Consultado el (22 de septiembre del 2022) y puede ser consultado en internet a través de; https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

Wazuh. La plataforma de seguridad de código abierto, Protección Active XDR contra amenazas modernas. Consultado el (20 de septiembre del 20229 el cual puede ser consultado mediante internet a través de; https://wazuh.com/

Yan Chen, K Carnero, Ramamurth and Kaung Wen; Journal of Computer Information Systems, Impacts of Comprehensive Information Security Programs on Information Security Culture. Consultado el (20 de septiembre del 2022) desarrollado el (10/12/2015) recovered from https://www.tandfonline.com/doi/abs/10.1080/08874417.2015.11645767