CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

JORGE LUIS MEDINA LOBO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2022

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

JORGE LUIS MEDINA

JOHN FREDDY QUINTERO
DIRECTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2022

TABLA DE CONTENIDO

Pag.

LISTA DE IMÁGENES

Pag.

RESUMEN

En el seminario especializado de equipos estratégicos de Seguridad Red Team & Blue Team se llevó a cabo la realización de distintas actividades que fueron parte de investigación, implementación, análisis, pruebas, resultados y documentación. Todas estas actividades realizadas fueron distribuidas en cuatro diferentes etapas progresivas, las cuales dependían de un desarrollo óptimo y unos buenos resultados para obtener éxito en la interpretación y realización de lo expuesto. Estas etapas fueron:

Etapa 1 - Conceptos equipos de Seguridad: Leyes informáticas en Colombia e instalación banco de trabajo.

Etapa 2 - Actuación ética y legal: Procesos ilegales y no éticos estipulados en un acuerdo de confidencialidad y los artículos de la Ley 1273 del 2009 que se vulneran.

Etapa 3 - Ejecución pruebas de intrusión: RedTeam - Intrusión a sistema operativo Windows 7 de 64 bits mediante Nmap y Metasploit de Kali Linux.

Etapa 4 - Contención de ataques informáticos: BlueTeam – Implementación, configuración, adaptabilidad y establecimiento de procesos seguros.

Para esto se hizo necesario establecer bancos de trabajo, instalaciones, configuraciones, investigaciones, documentaciones y todo lo necesario para realizar cada una de las etapas que hicieron parte de las actividades que le corresponde a un miembro Blue Team, Red Team y los aspectos legales que se deben tener presente al momento de ejercer el cargo en una empresa como Whitehouse Security. Los escenarios fueron claros y enfocados a lo que se requería en cada etapa.

Se mencionará además en el presente informe los aspectos más relevante e importante de lo realizado en cada una de estas etapas, dando así las conclusiones

y recomendaciones pertinentes para entender, implementar y reconocer estas situaciones en actividades profesionales futuras.

GLOSARIO

Ataque: Hace referencia a la acción de acceder de manera no permitida a activos o pasivos informáticos de una persona u organización.

Blueteam: Es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva.

Copnia: Es el Consejo Profesional Nacional de Ingeniería, encargada de controlar, verificar, inspeccionar y garantizar que la ingeniería se esté desempeñando correctamente. Por medio de esta se gestiona la tarjeta profesional como ingeniero y se conoce el código de ética que debemos respetar como ingenieros. También involucra profesiones a fines y profesiones auxiliares en general.

Escaneo: Crea una copia con el fin de exacta con el fin de ser estudiada para diversos beneficios.

Ética profesional: Son todos los valores y las acciones correctas que deben caracterizar a los profesionales cuando estén desempeñando un cargo laboral. Por medio de esta ética se identifica la calidad como trabajador o miembro de una organización.

Exploit: es un ataque que usa una vulnerabilidad de software para causar algún tipo de efecto no deseado en el sistema objetivo, como instalar malware o dar al hacker el control u otro tipo de acceso.

Firewall: es el dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente entre dos ordenadores

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

Intrusión: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas.

Kali Linux: es el sistema operativo utilizado para realizar las pruebas se seguridad, auditorías y hacking ético de los sistemas.

Malware: es todo tipo de amenazas informáticas o software hostil

Meterpreter: es un programa malicioso y utilizado para poder controlar de manera remota un sistema.

Nmap: es la herramienta utilizada en sistemas operativos como Kali Linux, la cual sirve para obtener las direcciones IP de una red, los puertos disponibles de los equipos que encuentra en la red, características de sistemas y mucha información que viaja por la red.

Phishing: estafa que tiene como objetivo obtener a través de internet datos privados de los usuarios

Redteam: Es el equipo encargado de actuar como atacantes, con el fin de realizar todos los análisis, descubrir vulnerabilidades, realizar ataques y realizar de una manera ética todo lo que un atacante podría hacerle a un sistema.

Vulnerabilidad: es la debilidad encontrada en un proceso. Cuando se habla de vulnerabilidad se habla de peligro, de que no está preparada o que no es lo suficientemente capaz para enfrentar algo. Si algo es vulnerable puede ser fácilmente atacado y no solo para destruir sino para utilizarse como acceso al sistema.

WM Virtual Box: es un software de máquina virtual utilizado para los bancos de trabajo. Por medio de Virtual Box se pueden instalar sistemas operativos en el equipo y controlar todos estos ambientes. Se comparten los recursos del equipo y de este dependen la eficiencia de la máquina virtual.

INTRODUCCIÓN

En el siguiente informe se identificará los más relevantes de cada una de las etapas que se realizaron durante el seminario especializado: equipos estratégicos en ciberseguridad: Red Team & Blue Team, en la cual se resaltaron los aspectos legales, las actividades realizadas como miembros Red Team y Blue Team y los respectivos análisis de los resultados y procesos que se realizaron en cada una de estas etapas.

En la primera etapa se resaltan los conceptos básicos de equipos de seguridad, en la segunda etapa la actuación ética y legal, luego en la tercera etapa la ejecución de pruebas de intrusión y finalmente en la cuarta etapa la contención de ataques informáticos.

Lo anterior como estrategia para optar por el título de especialista en seguridad informática en la Universidad Nacional Abierta y a Distancia Unad.

1. OBJETIVOS

1.1 General

Elaborar informe técnico de los aspectos más relevante de lo realizado en cada una de las etapas del seminario especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, incluyendo los aspectos legales que deben considerarse.

1.2 Específicos

Reconocer las actividades teórico practicas realizadas en el seminario de ciberseguridad en los equipos de Red Team y Blue Team

Describir las actividades teórico practicas desarrolladas en el seminario de ciberseguridad en los equipos Red Team y Blue Team.

2. DESARROLLO DEL INFORME TÉCNICO

2.1 ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD.

Esta etapa se desarrolló de la siguiente manera:

De manera individual consultó y se brindó respuesta a unas preguntas orientadoras las cuales fueron:

2.1.1 Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras qué legislación "leyes, decretos" existen actualmente y las características principales de cada ley.

Colombia ha sido un país que en el ámbito de la ciberseguridad ha implementado leyes y normativas que han permitido regular y sancionar todo tipo de incidente que se ha presentado relacionado con ataques cibernéticos, pero que debe mejor aún más en este aspecto, ya que constantemente se han presentado múltiples ataques a la ciberseguridad y es necesario que se refuerce los medios de protección existentes con el fin de garantizar el correcto manejo de la información.

Las normas, decretos y leyes que actualmente existen en Colombia relacionados con la ciberseguridad y delitos informáticos son las siguientes:

- Ley 527 de 1999

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. Es una ley que se aplica a todo tipo de información encapsulada como mensaje de datos, exceptuando obligaciones contraídas por el Estado Colombiano y las advertencias escritas que por solicitud legal deban ir impresas.

- Ley 962 de 2005

En esta ley se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios. Fue expedida en Colombia el 8 de julio de 2005.

- Ley 1273 de 2009

Se modifica el Código Penal, creando un nuevo bien jurídico dirigido a 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. Fue expedida en Colombia el 5 de enero de 2009.

Su estructura se encuentra conformada por los siguientes artículos:

• Artículo 269A Acceso abusivo a un sistema informático.
• Artículo 269B Obstaculización ilegítima de un sistema informático
• Artículo 269C Interceptación de datos informáticos
• Artículo 269D Daño informático
• Artículo 269E Uso de software malicioso
• Artículo 269F Violación de datos personales.
• Artículo 269G Suplantación de sitios web para capturar datos personales
• Artículo 269H Circunstancias de agravación punitiva
• Artículo 269I Hurto por medios informáticos
• Artículo 269J Transferencia no consentida de activos.

- Ley 1341 de 2009

Se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se

crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Fue expedida en Colombia el 30 de julio de 2009.

- Ley 1581 de octubre 17 de 2012

Se dictan obligaciones generales para la protección de datos personales donde su principal objetivo es desarrollar el derecho constitucional que tienen las personas de conocer, actualizar y rectificar la información que se hayan recogido sobre ellas en bases de datos o archivos. Fue expedida en Colombia el 17 de octubre de 2012.

- Documento CONPES 3701 de 2011

Este documento fue expedido por el CONPES y trata sobre los “Lineamientos De Política Para Ciberseguridad Y Ciberdefensa”; el problema se centra en la capacidad actual del Estado para enfrentar las amenazas cibernéticas. Donde se detectan debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas.

- Ley 842 de octubre 9 de 2003 de COPNIA

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 Ética Profesional y se dictan otras disposiciones.

2.1.2 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.

Existen tres tipos de pentesting que pueden realizar:

- Pentesting de caja blanca: Es el Pentest más completo. El pentester conoce toda la información de la organización y por ende realiza un análisis completo de la estructura informática identificando los sistemas que pueden ser modificados o mejorados según la infraestructura tecnológica.

- Pentesting de caja negra: Es parecido a una prueba a ciegas, pues sigue la premisa de no poseer gran cantidad de información disponible sobre la corporación. Simula un ambiente real donde el pentester no conoce ningún tipo de información de la empresa y su intención es actuar como un ciberdelincuente para intentar detectar vulnerabilidades y amenazas.

- Pentesting de caja gris: Es una mezcla del pentesting blanco y negro donde el pentester conoce un mínimo de información de la empresa y desde allí parte para realizar el test.

Para llevar a cabo estas fases el pentester debe seguir una serie de etapas que garanticen que el examen realizado cumple con los requerimientos de la organización, estas fases son las siguientes:

- Recogida de información: Se evaluará la información que se tiene de la empresa y el tipo de pentesting a realizar para determinar cómo efectuar el test. Dependiendo de este se pueden emplear diferentes herramientas teniendo en cuenta si se tiene información de la organización, en el caso de que no se tenga se pueden implementar herramientas como DnsRecon, Dig, Maltego, Pastenum. Para aquellos casos donde se tiene acceso a la información se puede hacer uso de herramientas como Metasploit y Snmpwalk.

- Análisis de vulnerabilidades y amenazas: Se deben realizar pruebas para verificar las vulnerabilidades del sistema, posibles fugas de información, amenazas potenciales, esto teniendo en cuenta también el factor humano y sus fallos. Para esta fase se pueden utilizar herramientas como Nmap, Nessus, Burp suite.

- Acceso al sistema: Una vez analizada la información recogida, se establecen qué tipos de ataque se ejecutarán y el objetivo de estos. Para esta fase se utilizan herramientas como Metasploit para aprovechar las vulnerabilidades detectadas.

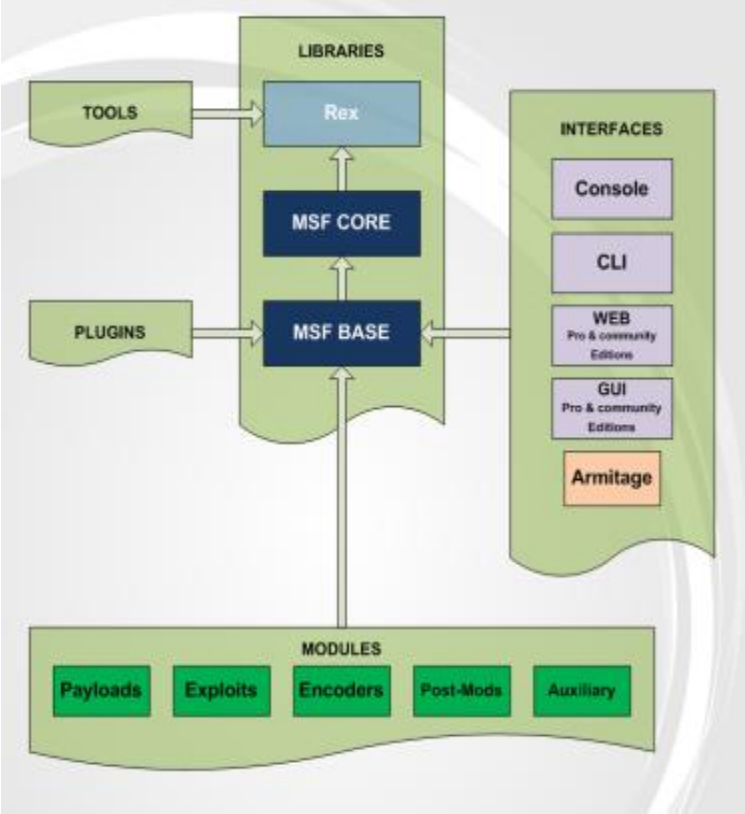
- Elaboración del informe: Se deben evidenciar al alcance los fallos de seguridad detectados, el impacto que podrían tener y se debe incluir recomendaciones para mitigar estas fallas y mejoras de medidas de seguridad. Para esta fase existe una herramienta llamada PWNDoc desarrollada en Node.js la cual permite agilizar el desarrollo de los informes.

2.1.3 Las herramientas de ciberseguridad son de vital importancia, además, 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: Herramientas.

- Metasploit

Es una herramienta desarrollada en Perl y Ruby que permite ejecutar exploits contra una máquina remota, permite realizar auditorías de seguridad, probar y desarrollar sus propios exploits. Creado originalmente en lenguaje de programación Perl, el Metasploit Framework ha sido completamente reescrito en lenguaje Ruby.

Imagen 1: Estructura de metasploit



Fuente: https://fzuckerman.wordpress.com/2016/10/08/944/

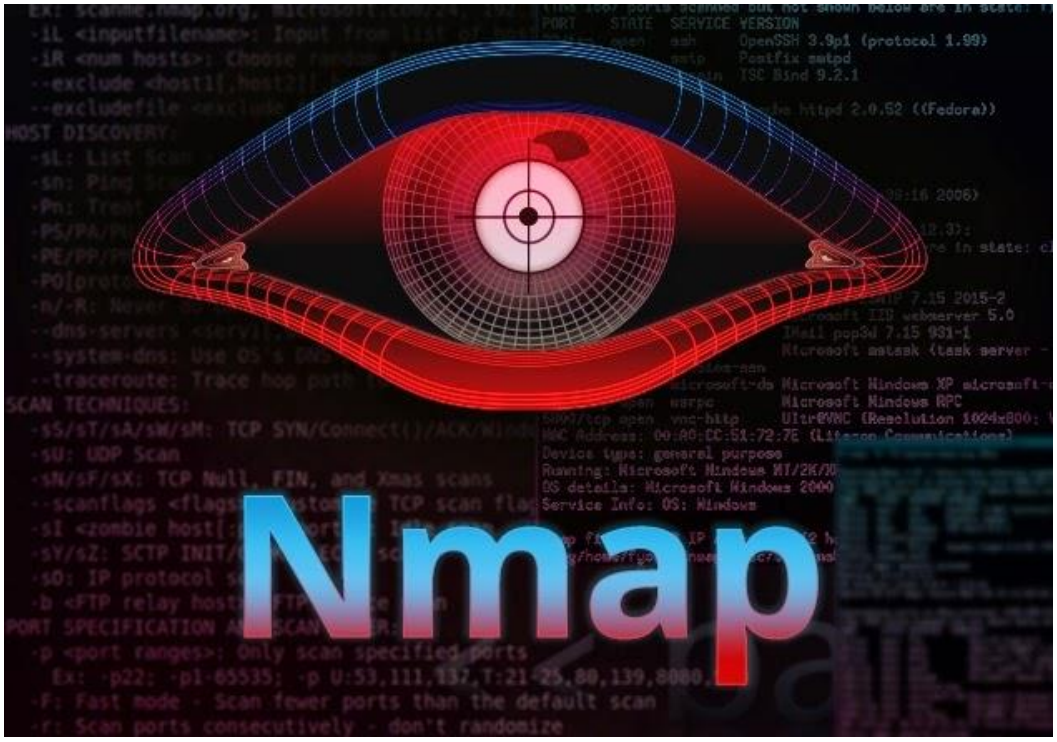
- Nmap

Es una herramienta opensource utilizada para el escaneo de redes, puertos y vulnerabilidades de servicios que pueden servir como punto de entrada a los sistemas utilizada comúnmente en auditorías de seguridad y monitoreo de redes.

La base de Nmap es el análisis de puertos, pero también cuenta con otras capacidades como:

- Mapeo de red
- Detección de SO
- Descubrimiento de servicios
- Auditorías de seguridad.

Imagen 2: Nmap



Fuente: https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/

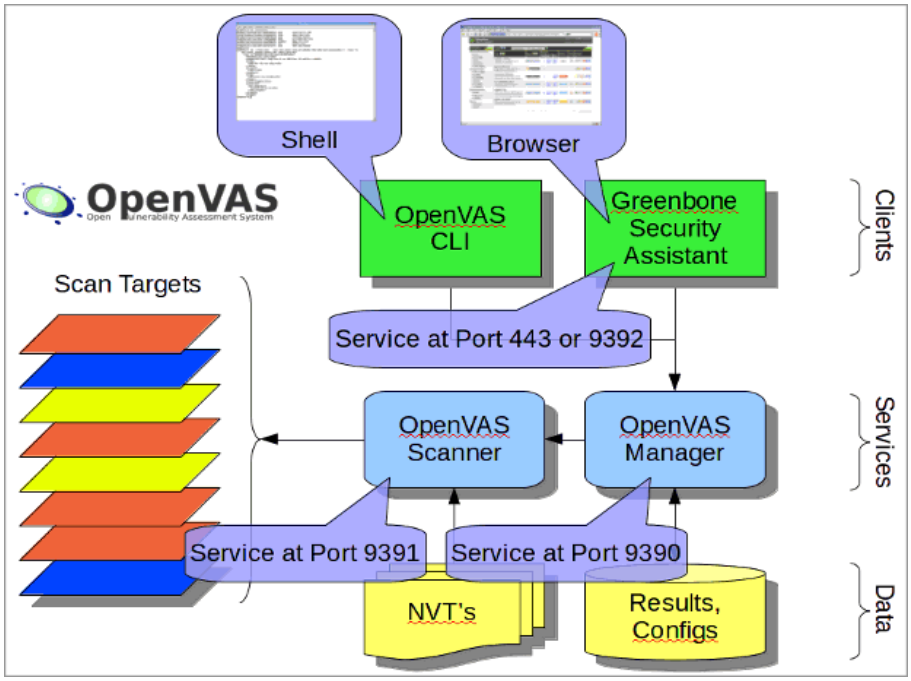
- OpenVas

Es una herramienta que permite encontrar fallas de seguridad e información detallada de vulnerabilidades que pueden ser explotadas para poner en peligro la confidencialidad, la disponibilidad y la integridad de los datos almacenados y procesados en nuestros equipos. Abajo encontrarás los pasos de instalación requeridos.

Esta herramienta tiene diversas funciones como son:

- Pruebas autenticadas
- Pruebas no autenticadas
- Protocolos industriales y de internet
- Ajustes personalizados
- Desarrollo de un potente lenguaje de programación interno

Imagen 3: Herraienta OpenVas



Fuente: https://partyhack.cl/2018/05/31/herramienta-gratuita-para-buscar-vulnerabilidades-con-openvas-en-kalilinux/

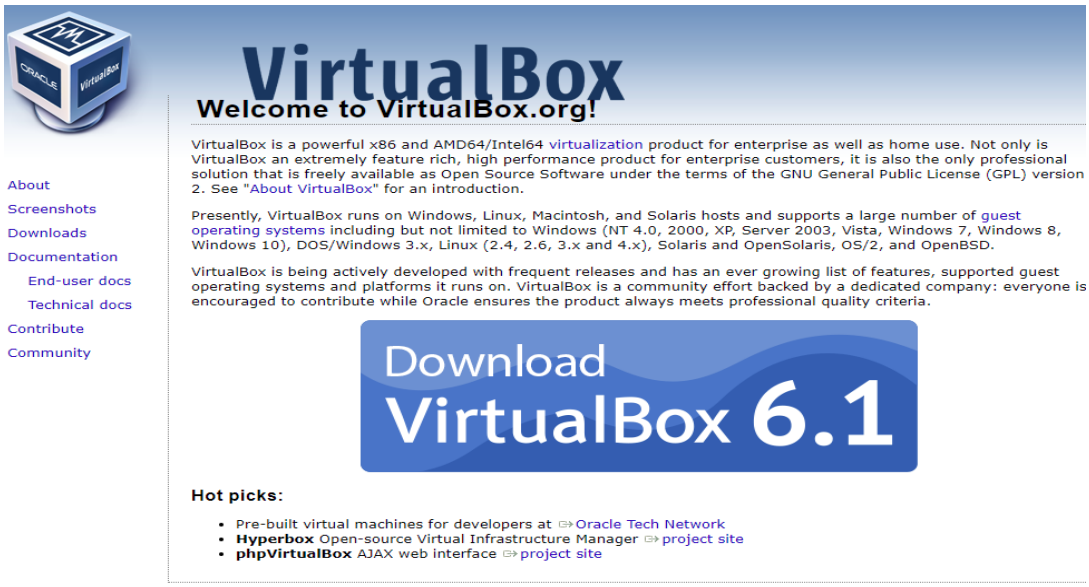
- ExploitDB: es básicamente una base de datos de vulnerabilidades en donde en comunidad se comparten las vulnerabilidades de aplicaciones, comparten como explotarlas y sacarles provecho.

- CVE: es el número de identificación que se le asigna a una falla común en sistemas TI, permiten que se aúnen esfuerzos grupales entre organizaciones para resolver y mejorar dichas vulnerabilidades.

2.1.4 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:

Procederemos a descargar nuestra máquina Virtual Box en su página oficial https://www.virtualbox.org/wiki/Downloads y seleccionar el SO correspondiente donde se instalará el programa.

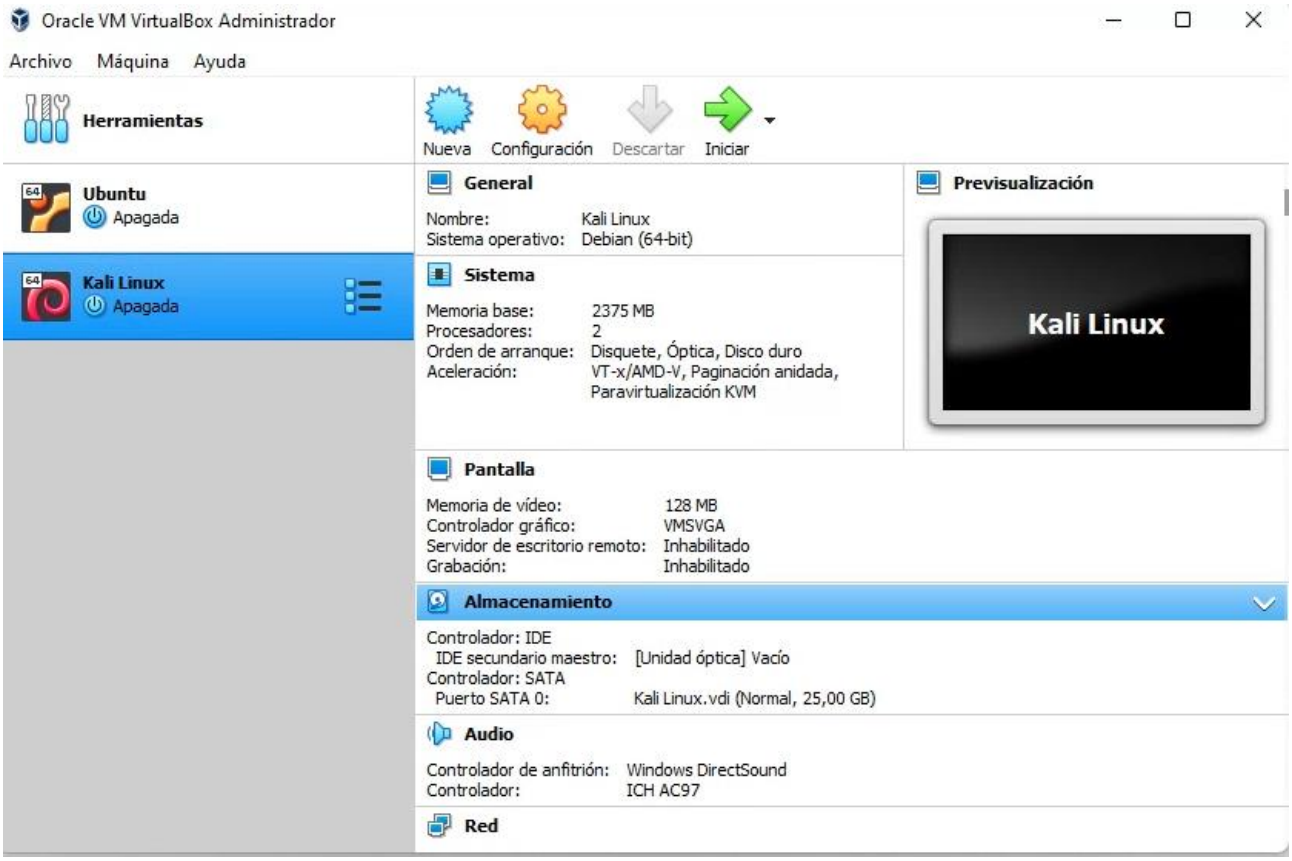
Imagen 4: Descarga de Virtual Box



Fuente: Propia

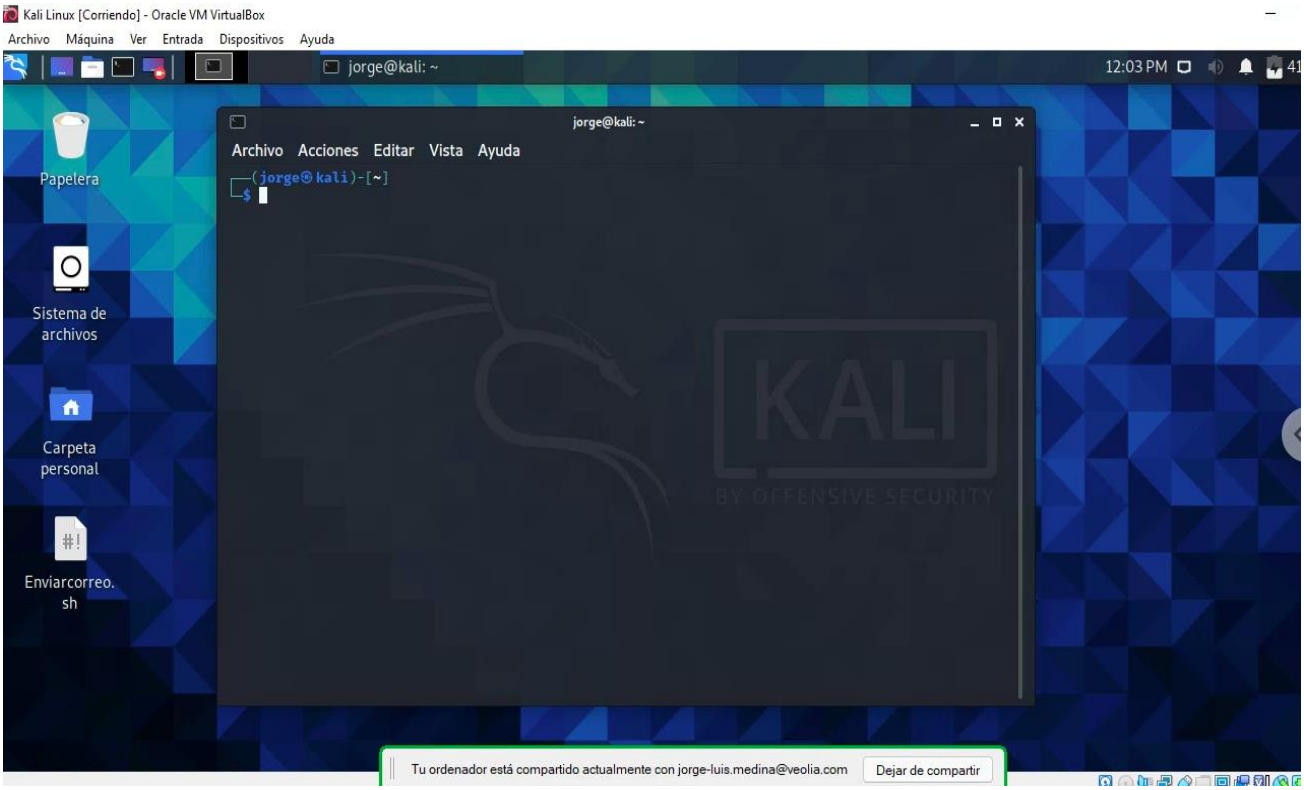
Paso B: Realizaremos el montaje de las máquinas en virtual Box creando una nueva máquina, asignando el nombre y el sistema operativo.

Imagen 5: Instalación de S.O en Virtual Box



Fuente: Propia

Imagen 6: Ejecución del sistema operativo Kali Linux



Fuente: Propia

2.2 ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL.

En esta etapa de tipo teórica y de análisis se hizo lectura de un problema para dar respuesta a una serie de preguntas, las cuales fueron:

2.2.1 ¿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.

De acuerdo con el anexo 2 podemos evidenciar que la compañía WhiteHouse Security, no lleva a cabo un análisis exhaustivo del personal que selecciona para trabajar en la organización, sino que por el contrario solo lleva a cabo recomendaciones mínimas dejando para su implementación un contrato que fue realizada por una persona que ya no labora en la organización descuidando con esto una labor fundamental como lo es el activo de información que allí se encuentra establecida. Esto desde mi punto de vista origina que la empresa pueda estar incurriendo sin preverlo en delitos informáticos al interior de su compañía, por el simple hecho de dejar una labor tan delicada como el conocimiento y validación de la información del personal contratado, ya que se está dejando vulnerable la información confidencial de otras personas.

Así mismo considero que es algo inapropiado el dejar el acceso libre a la información de una empresa en un proceso selección en donde no se tiene ningún vínculo laboral ya definido aún con quien va a realizar un proceso tan delicado como el del manejo de la información de terceros a nombre de la empresa WhiteHouse Security.

En cuanto al anexo 3 encontramos:

Clausula primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades

legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.

En esta cláusula evidenciamos claramente que la empresa no solo lleva a cabo procedimientos legales que requieran de confidencialidad, sino que también se realizan procesos ilegales que van en contra de su correcto funcionamiento y por ende obliga al receptor a no divulgar la información de estas irregularidades que se puedan presentar al interior de la organización de forma física o remota a compañeros de trabajo, autoridades, o algún tipo de asesor.

De acuerdo con lo anterior, si es la compañía Whitehouse Security quien realiza este tipo de procedimientos que van en contra de la normatividad estipulada al momento de los actos, esto incurre en un delito y falta de ética profesional, pues al identificar una conducta ilegal esta debe ser denunciada ante la autoridad competente.

Ahora bien y si por el contrario la empresa Whitehouse Security dentro de sus hallazgos realizados mediante procedimientos legalmente establecidos, se informa sobre procesos ilegales, se debe revisar con el superior quien tendrá la facultad de velar por el resguardo de la información clasificándola según los parámetros de la empresa Whitehouse Security.

Clausula segunda, Definición de información confidencial parágrafo 2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, 9 datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”

En este apartado de la cláusula es definida la información considerada confidencial por parte de la empresa Whitehouse Security, la cual debe ser cumplida y acatada por la parte receptora en caso de aceptar el acuerdo y por medio de la cual se realiza

descripción de datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos.

En esta cláusula es posible que dependiendo del volumen de información de todo tipo se capte no solo información legal, sino también de tipo ilegal pero que puede ser producto de la actividad misma de ciberseguridad y ciberdefensa.

Este tipo de acciones son reglamentadas y penalizadas por las leyes colombianas, además de ir en contravía de la ética profesional pues se debe buscar que la actividad profesional propende por el bien para todos y no debería ser perjuicio para otros.

Clausula cuarta, parágrafo 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

En esta cláusula encontramos que la parte receptora, se ve obligada a no divulgar información de actividades sospechosas al interior de la organización, sino también cualquier tipo de procesos ilegales que se pueda presentar al interior y que se lleven a cabo por parte de Whitehouse Security. Todo esto incurre en un delito ante la ley colombiana, además falta de ética profesional, pues al identificar una conducta ilegal esta debe ser denunciada ante la autoridad competente.

Clausula cuarta, parágrafo 4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

Esta cláusula obliga a que la parte receptora no realice ningún tipo de divulgación sobre la información no solo confidencial de Whitehouse Security, sino también cualquier tipo de procesos ilegales que se pueda presentar al interior y que se lleven 10 a cabo por parte de Whitehouse Security. Esto incurre en un delito y falta de ética profesional, pues debe ser denunciada ante la autoridad competente.

Clausula cuarta, parágrafo 8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

En caso de que el receptor acepte el cargo, se obliga automáticamente a responder por la información que tenga de Whitehouse Security y que se encuentre en su poder, en caso de que se realice una operación de allanamiento en contra de la parte receptora.

Clausula cuarta, parágrafo 9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security.

Esta cláusula establece que la parte receptora, en este caso el prospecto al cargo se obliga a no divulgar la información no solo confidencial de Whitehouse Security, sino también cualquier tipo de procesos ilegales que se pueda presentar al interior y que se lleven a cabo por parte de Whitehouse Security, de forma física o remota a compañeros de trabajo, autoridades, o algún tipo de asesor. Esto incurre en un delito y falta de ética profesional, pues al identificar una conducta ilegal esta debe ser denunciada ante la autoridad competente.

Clausula quinta, parágrafo 8. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora: Octava. Solución de controversias: Las partes (nombre estudiante– nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.

En caso de que no se logre aceptar la oferta, la parte receptora se obliga a responder por la información que tenga de la organización y que se encuentre en

su poder, en caso de que se realice una operación de allanamiento en contra de la parte receptora.

2.2.2 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.

De acuerdo con los acuerdos y cláusulas del anexo 3, si se evidencia de que dentro de este se presenten evidencias de posibles delitos informáticos tales como:

- Clausula primera y segunda, clausula cuarta, parágrafo 3. En el artículo 269A de la ley N.º 1273 se enuncia el acceso abusivo a un sistema informático, se tiene en cuenta para todo lo que tiene que ver con accesos no autorizados, incluyendo lo que se denomina como “chuzada”, procedimiento en el cual se utilizan diferentes herramientas.

- En el artículo 269B indica que no se debe generar indisponibilidad o perdida de acceso sistemas informáticos, a información o bases de datos y a redes de telecomunicaciones.

- En la Clausula segunda se viola el Artículo 269C el cual Habla de la no legalidad de interceptación de datos informáticos, en ningún punto ya sea origen o destino, además que contempla la no interceptación de ondas electromagnéticas.

- El Articulo 269D indica que es ilegal cualquier tipo de daño a nivel de software y hardware, sea memoria o funcionamiento, para tener en cuenta ante ataques.

- El Articulo 269F contempla la protección de datos personales contenidos e

- La suplantación de sitios Web con el fin de obtener datos personales este enunciado en el artículo 269G, atiende a personas que clonen paginas legales o realicen desvió de información para beneficio propio.

- En los artículos 269 I y J se contempla el hurto por medios informáticos y la transferencia no consentida de activos.

2.2.3 Existiendo procesos poco confiables en el anexo 3 - Acuerdo usted como experto en ciberseguridad aplicaría a este trabajo en WhiteHouse 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.

Teniendo en cuenta que la empresa está contratando especialistas en seguridad informática inicialmente como aspirante al cargo solicitaría revisión del acuerdo entre las partes y de esta manera verificar si se presentan anomalías irregulares. En caso de que se presenten, las recomendaría e informaría a la empresa los términos y cláusulas que pueden estar en contra de la legalidad, si luego de que las anomalías del contrato hayan sido revisadas y no sufren ningún tipo de modificación, no aceptaría la posibilidad de aplicar a un cargo de esta magnitud, ya que se puedan llevar a cabo actividades delictivas, criminales o que vayan en contra de la ley y no solo eso, también me considero un profesional integro que valora y respeta su conocimiento, como lo indica el código de ética el cual se apoya en la ley 842 de 2003: “busca que los ingenieros, profesionales afines y auxiliares, actúen con compromiso y honestidad en aras de brindar a la ciudadanía un ejercicio ético de su profesión”.

Además, no aceptaría un empleo en el cual pueda verme implicado en acciones ilícitas cometidas sin conocimiento, ya sea de mi parte o de compañeros de

trabajo, pues al realizarlas con el fin de cumplir las razones laborales no me exonera de la culpa.

En el Código emitido por el COPNIA el cual se indica como el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31. Esta el parágrafo que indica “Son deberes generales de los profesionales los siguientes”:

f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda 13 la información y pruebas que tuviere en su poder;

Si en caso de que estas acciones sean llevadas a cabo con pleno conocimiento, estaré incurriendo en un delito implicando no solo mi persona, sino la profesión y mi círculo familiar, social, académico, laboral.

De nuevo en el Código emitido por el COPNIA, Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 34. Esta el parágrafo indica, “Son prohibiciones especiales a los profesionales respecto de la sociedad”:

a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación.

En el caso de que un profesional incurra en participar de cualquier clase de delito en el desarrollo de sus funciones va en contra del código de ética, y en detrimento de su profesión, además en caso de un delito está obligado legalmente a revelar información.

En el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES Y

OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 39. Esta el parágrafo indica, “Son deberes de los profesionales para con sus clientes y el público en general:”:

a) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo;

Por último, se dejan en claro las faltas graves que un profesional de la ingeniería en este caso un especialista en seguridad informática debe evitar.

En el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, se contemplan las faltas gravísimas contempladas en el artículo 53 de la ley 842 de 2003.

e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares;

f) Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente ley.

2.2.4 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.

La operación militar que se llevó a cabo con el nombre de “Andromeda” y que dio cuenta de todo un escándalo por sus implicaciones sociales y políticas, fue un entramado creado por la inteligencia militar como una operación legitima, y que

tenía como finalidad utilizar las habilidades informáticas de civiles en la búsqueda de información por medios abusivos.

Fue así como de esta manera se creó un lugar de acogida informal al aprecer en el barrio Galerías en Bogotá el cual tenía como nombre Buggly, donde confluían elementos atrayentes para los jóvenes como tatuajes, comida, paintball y por supuesto salas con computadores y una mezcla de civiles y personal militar.

Andromeda Buggly fue una operación legitima y encubierta en la cual el ejercito mediante mentiras atraía a personal civil para que realizara actos ilegales, el tema se desbordo porque no se contaba con una ética clara para el actuar tanto de civiles como de militares.

El caso tomo aún más revuelo por estar involucrado el llamado hacker Carlos Andrés Sepúlveda, quien al parecer compraba y obtenía información valiosa de Buggly y que además servía a la campaña del entonces candidato presidencial por el centro democrático Oscar Iván Zuluaga, quien había contratado sus servicios, de una manera indirecta.

En toda la historia de la humanidad se ha dado gran relevancia a la información y al uso que de esta se puede hacer, ya sea para beneficio o en detrimento de personas, entidades, pueblos, pero hoy en día que la información es almacenada en medios electrónicos y viaja a través de redes de computadores es de suma importancia no solo conocer su acertado manejo sino también su resguardo, porque habrá personas inescrupulosas que harán lo que sea para obtenerla.

En el caso del ejercito es un actuar fuera de la ética, el usar a civiles mientras bien pudieran emplear los mismos fondos de operaciones de engaño a capacitar a funcionarios militares, es aún más falto de ética atraer y engañar con el fin de obtener datos e información de manera claramente abusiva, poniendo en evidencia a civiles que estaban cometiendo delitos informáticos como son la interceptación y robo de datos, crímenes que ya estaban legislados en su momento bajo la ley 1273 de 2009.

A nivel legal “Andromeda” al no tener control dejo que conocedores de la información se hiciesen con ella al mejor precio, personas que obviamente sabían qué hacer con la información que se obtenía en la operación y que pudiese ser destinada a cualquier clase de ilícito, incluso a ganar unas elecciones o sabotear al candidato opositor.

Al manejar la seguridad nacional y la seguridad de la información pública se debe contar con altos estándares en la ética profesional ya que pueden presentarse oportunidades de usufructuar la información que se maneja, así mismo se debe de tener conocimiento del marco legal en Colombia que define, reglamenta y penaliza los delitos informáticos para no pecar por omisión, y cometer un crimen por ignorancia o falta de conocimiento.

2.3 ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN.

Para la realización de esta etapa se procedió con la instalación del banco de trabajo para poder realizar las pruebas de intrusión las cuales posterior a ello conllevarían a dar respuesta a unos interrogantes. Estos fueron:

2.3.1 Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Red Team. 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 el desarrollo de este punto se hizo uso de las siguientes herramientas software:

- Nmap: es una herramienta utilizada para la exploración de redes, puertos y vulnerabilidades de servicios que pueden servir como punto de entrada a los sistemas. Es utilizada comúnmente en auditorías de seguridad y monitoreo de redes.

- Nessus: es una herramienta de seguridad web que realiza escaneo de vulnerabilidades en diversos sistemas operativos. Previene ataques a la red mediante la identificación de vulnerabilidades y problemas de configuración que los piratas informáticos utilizan para penetrar una red.

- Mestaspolit: es una herramienta que permite ejecutar exploits contra una máquina remota, permite realizar auditorías de seguridad, probar y desarrollar sus propios exploits.

2.3.2 A continuación, liste y 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.

- Los equipos sospechosos cuentan con Windows 7 X86 y X64.

- Se tenía una evidencia relacionada con la fuga de información que se presentaba al interior de la organización en uno de los equipos de cómputo.

- La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada Rejetto v. 2.3 bajo un Windows 7 con arquitectura X64.

- Se hace investigación sobre aplicación Rejetto v. 2.3 la cual es una HTTP file server, un servidor web para compartir archivos libre de malware y pensada para ser útil, pero que presenta una vulnerabilidad.

- La aplicación presenta múltiples vulnerabilidades, las cuales se pueden asociar a diferentes exploits que pueden terminar entre otros en una Shell reversa y una sesión abierta de Meterpreter.

- En un escenario típico de acceso al sistema remoto, el usuario es el cliente y la máquina de destino es el servidor. El usuario inicia una conexión de Shell remota y el sistema de destino escucha dichas conexiones.

- Existe la posibilidad de invertir este proceso donde es la máquina de destino la que inicia la conexión con el usuario y la computadora del usuario escucha las conexiones entrantes en un puerto específico.

- La razón principal por la que los atacantes suelen utilizar Shells inversos es la forma en que se configuran la mayoría de los firewalls. Los servidores atacados generalmente permiten conexiones solo en puertos específicos. Por ejemplo, un servidor web dedicado solo aceptará conexiones en los puertos 80 y 443. Esto significa que no hay posibilidad de establecer un escucha de Shell en el servidor atacado. Tener los puertos abiertos o en modo escucha es una mala práctica ya que los sistemas operativos y aplicaciones como correo, almacenamiento de información, navegadores, bases de datos, almacenamiento de contraseñas y usuarios quedan completamente expuestos a rastreo o escaneo de puertos por medio de herramientas como Metasploit, Nessus, Nmap.

- La mala gestión en las políticas y controles de los puertos genera una gran cantidad de vulnerabilidades y posibles amenazas a la seguridad de la información.

- El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

Procedimientos implementados para llevar a cabo el anexo 4 – escenario 3 enfocado a Red Team.

- **Fase de recolección y levantamiento de la información:**

Como primera medida tenemos el requerimiento por medio del cual se informa sobre lo sucedido en la organización y el cual será el punto de partida para proceder con el análisis de la información.

Se tiene la evidencia sobre la fuga de información que se presenta al interior de la organización en uno de los equipos de cómputo.

La información inicial que existe es que el equipo donde se está generando la fuga de información tiene instalada una aplicación llamada Rejetto v. 2.3 bajo un sistema operativo Windows 7 con arquitectura X64.

El sistema operativo Windows 7 actualmente instalado en el equipo de cómputo, no cuenta con actualizaciones de seguridad ya que estas dejaron de ser emitidas por Microsoft desde enero de 2020, al considerar que este sistema operativo había cumplido con su vida útil y para que de alguna forma se forzara y diera paso al sistema operativo Windows 10.

El empleo de este sistema operativo es cada vez más riesgoso, ya que se aumentan los casos de nuevas vulnerabilidades encontradas que son aprovechadas para minar los pilares de la información, teniendo en cuenta que aun muchos usuarios y empresas no han realizado la actualización de sus sistemas operativos.

- **Fase de Búsqueda de vulnerabilidades.**

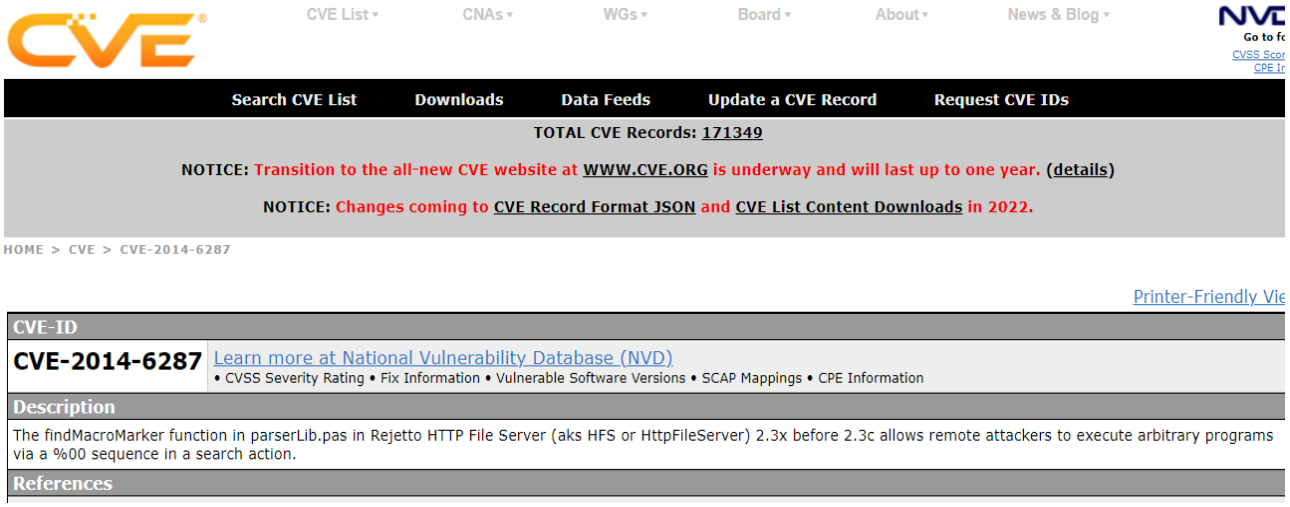
Dentro de la información que fue entregada por la organización se hace estudio de las vulnerabilidades que se presentan. Se hace investigación sobre la aplicación Rejetto v. 2.3 la cual es una HTTP file server, un servidor web que permite compartir archivos, es decir, una aplicación libre de malware y pensada para ser útil, pero presenta una vulnerabilidad.

Se hace revisión y estudio de casos similares e investigación en bases de datos de vulnerabilidades donde se encuentran dos vulnerabilidades para esta aplicación. Dentro de las fuentes confiable se evidencian alertas sobre la vulnerabilidad presente en la aplicación Rejetto v. 2.3 y anteriores:

Imagen 7: Vulnerabilidad 2014-6287 para aplicación Rejetto v. 2.3 y anteriores

Fuente: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

Imagen 8: Vulnerabilidad 2014-6287 para aplicación Rejetto v. 2.3 y anteriores

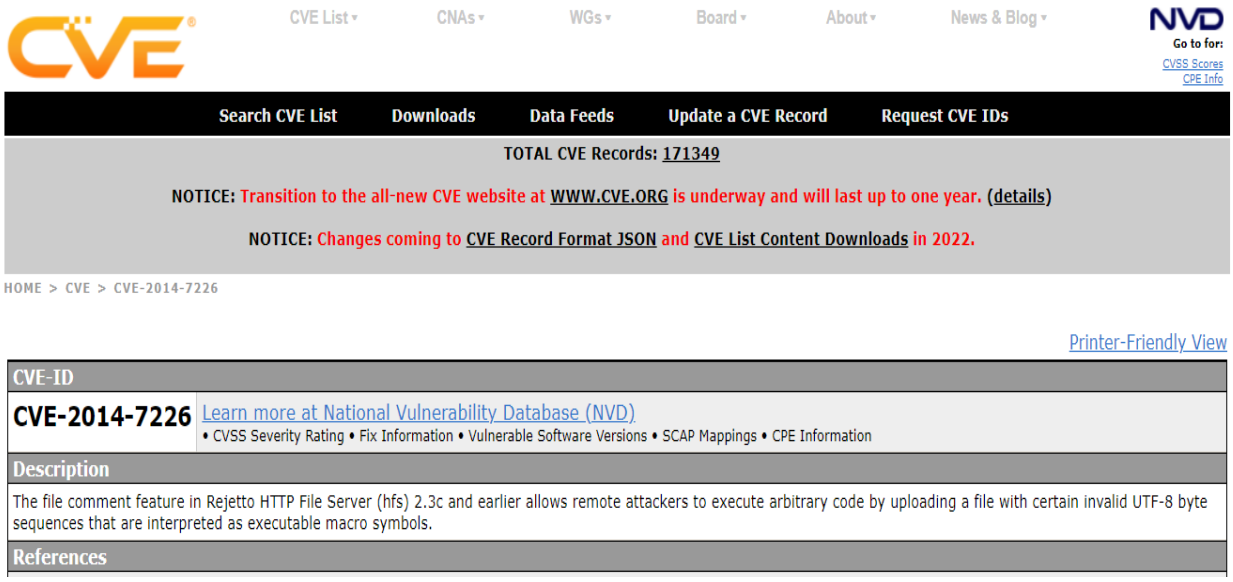


Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

La función findMacroMarker en parserLib.pas en Rejetto 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.

Esta aplicación tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de Meterpreter. Además, la aplicación Rejetto v. 2.3 y anteriores presenta dos vulnerabilidades más documentadas:

Imagen 9: Vulnerabilidad 2014-7226 para aplicación Rejetto v. 2.3 y anteriores

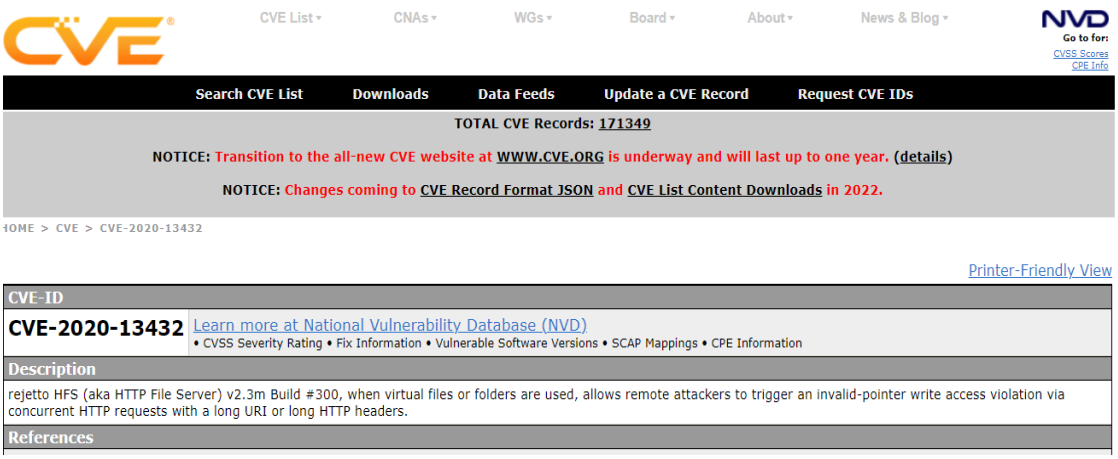


Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7226

La función de comentario de archivo en Rejetto HTTP File Server (hfs) 2.3c y versiones anteriores permite a los atacantes remotos ejecutar código arbitrario cargando un archivo con ciertas secuencias de bytes UTF-8 no válidas que se interpretan como macro símbolos ejecutables.

Por último, aparece una vulnerabilidad documentada para aplicación Rejetto v. 2.3 y anteriores:

Imagen 10: Vulnerabilidad 2020-13432 para aplicación Rejetto v. 2.3 y anteriores CVE-2020-13432



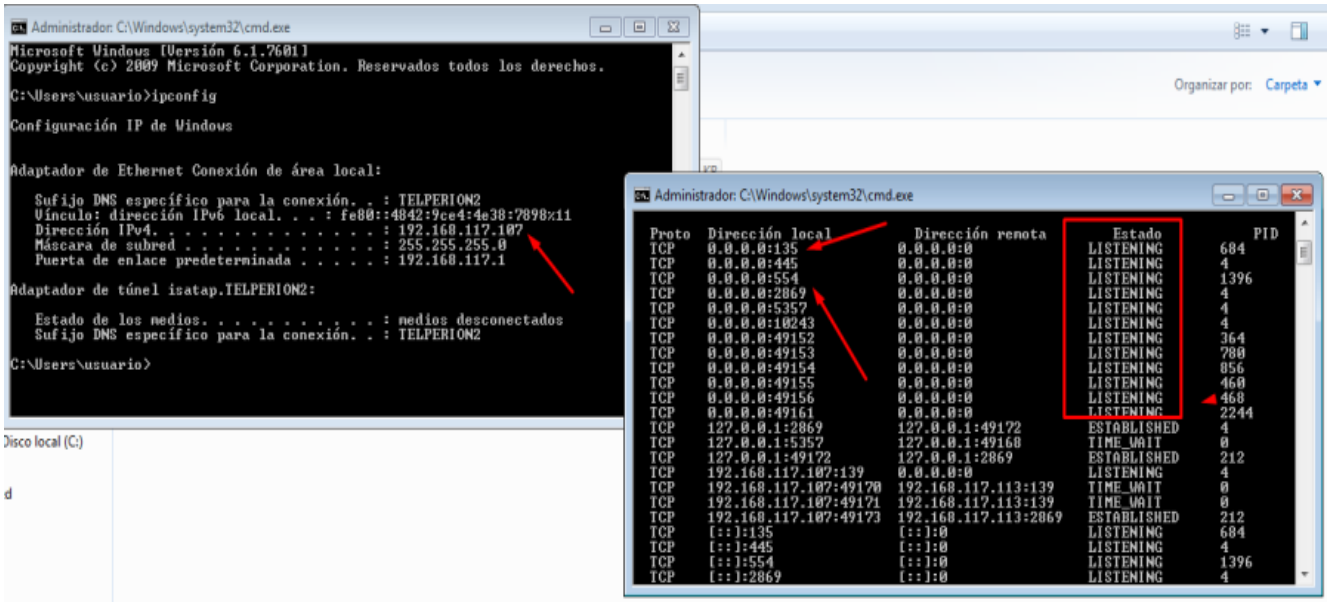
Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13432

Rejetto v. 2.3 y anteriores, cuando se utilizan archivos o carpetas virtuales, permite a los atacantes remotos desencadenar una infracción de acceso de escritura de puntero no válido a través de solicitudes HTTP simultáneas con un URI largo o encabezados HTTP largos

2.3.3 ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 7"? ¿Qué puerto abre la aplicación específica en el anexo?

Nuestra máquina con sistema operativo Windows 7, tiene servicios ejecutándose como servicio y el cual acepta conexiones entrantes, dado que se detecta que su firewall no las bloquea.

Imagen 11: Resultado comando ipconfig - Windows 7.

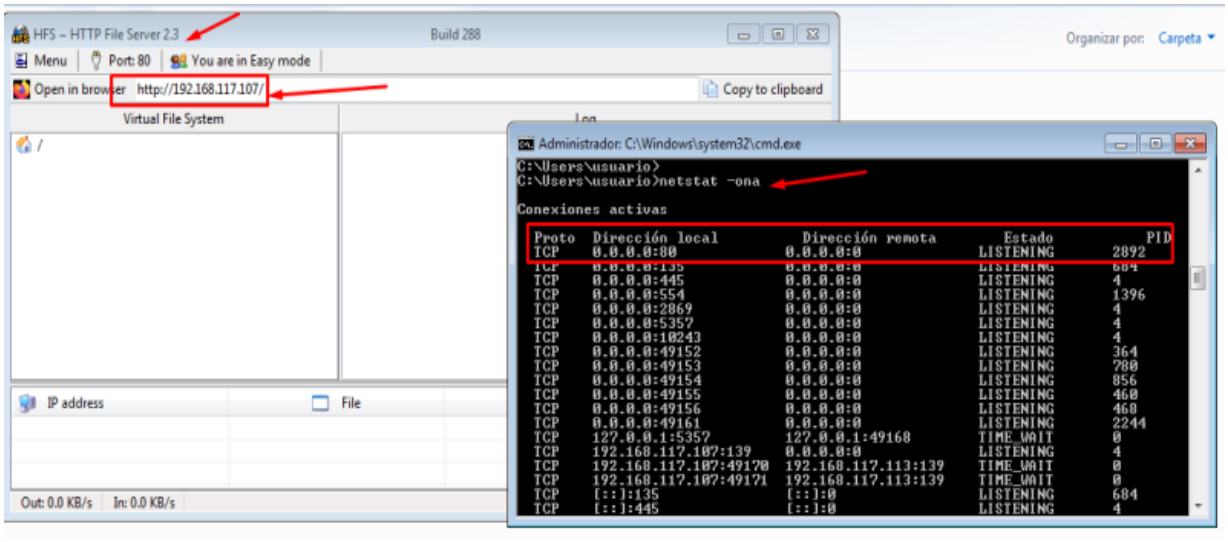


Fuente: propia

Por medio de la herramienta ipconfig, podemos observar que tiene configurada la ip: 192.168.117.107, con la herramienta de comandos netstat se observa los puertos que están abiertos y que están en estado LISTENING como se observa en la imagen derecha arriba.

El aplicativo que se ejecuta en el host corre una aplicación que tiene una vulnerabilidad conocida, al activarla se abre un nuevo puerto en el equipo, el cual es detectado con la herramienta netstat. En este caso la aplicación abre el puerto 80, como se observa a continuación.

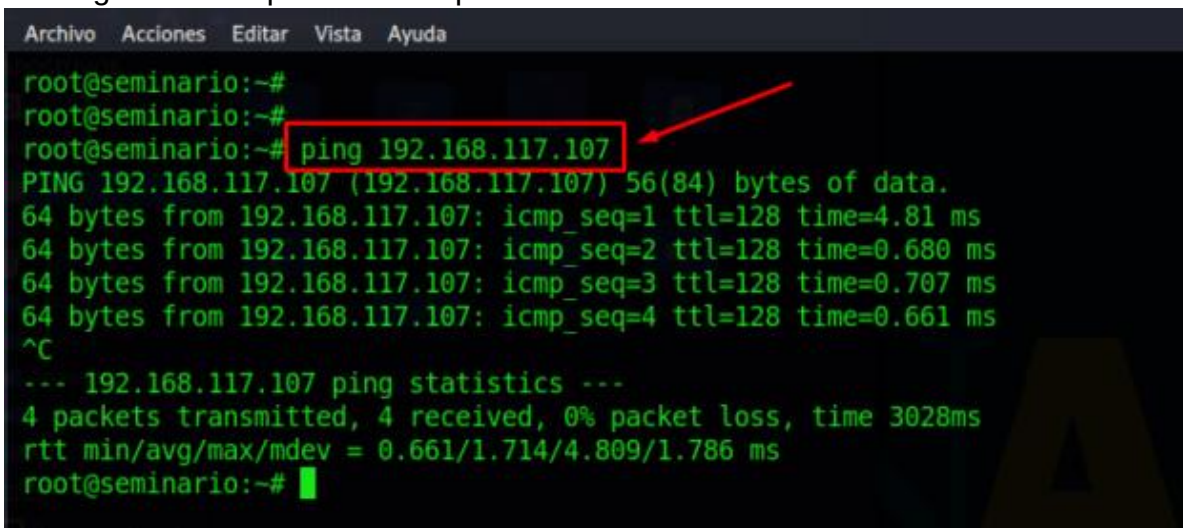
Imagen 12: Puerto 80 en modo listening - Rejetto v. 2.3



Fuente: propia

En este caso un atacante haciendo uso de un sistema operativo de pentesting (Kali) puede alcanzar dicha maquina dado que están en red, como lo muestra la siguiente imagen:

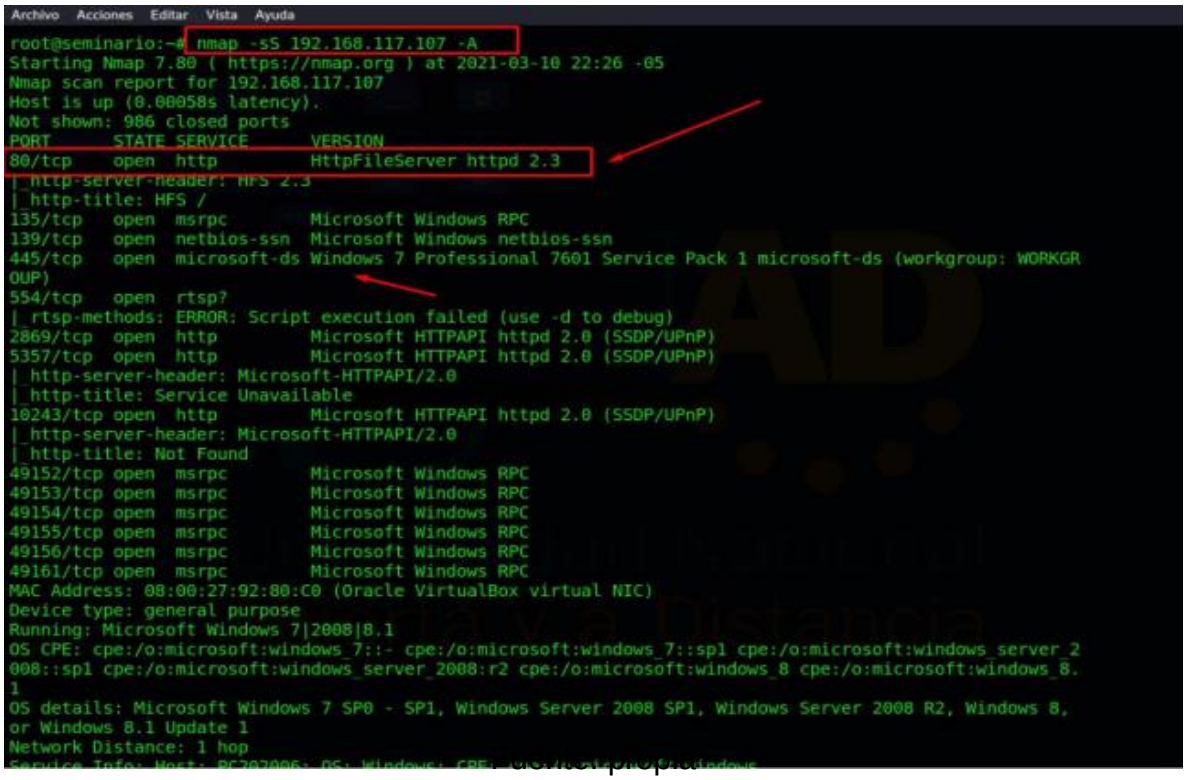
Imagen 13: Ataque sistema operativo



Fuente: propia

Con la herramienta Nmap, un atacante puede detectar los puertos abiertos que tiene el equipo y el servicio que los tiene corriendo (ejecutando en background)

Imagen 14: Uso de Nmap - Puerto 80 open - Rejetto v. 2.3

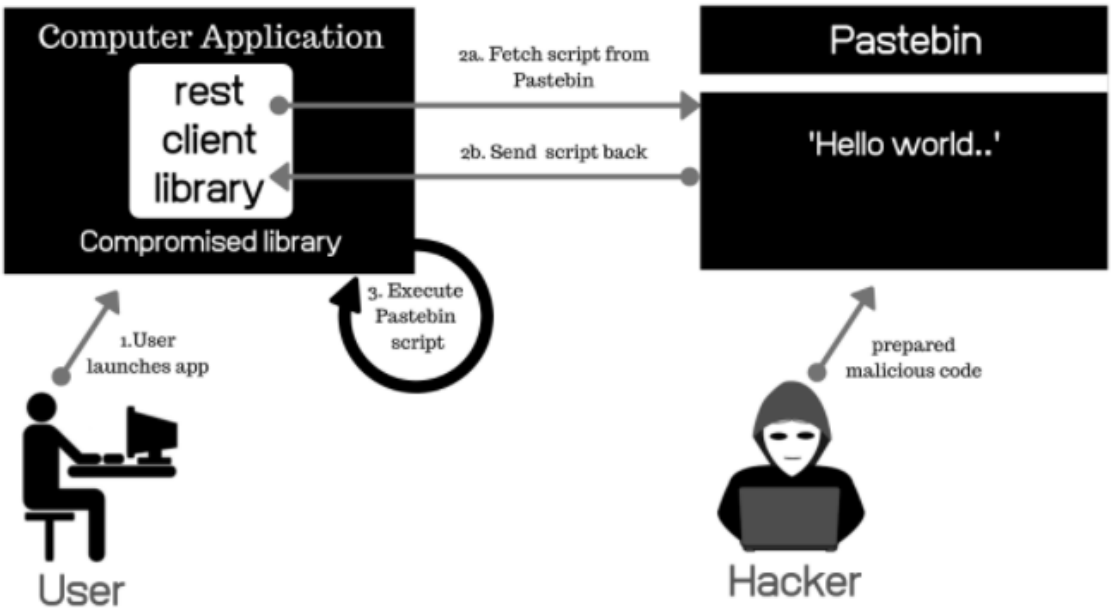


2.3.4 Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.

Un atacante puede saber de acuerdo con la versión de software que se corre en el host remoto que vulnerabilidades conocidas tiene la aplicación y si no se han parchado se corre el riesgo de que sean explotadas. Como se hará en este PoC, se aprovecha el bug conocido que permite a un atacante remoto ejecutar código arbitrario en el servidor (host) que hospeda la aplicación.

La función de comentario de archivo en Rejetto HTTP File Server (hfs) 2.3c y versiones anteriores permite a los atacantes remotos ejecutar código arbitrario cargando un archivo con ciertas secuencias de bytes UTF-8 no válidas que se interpretan como macro símbolos ejecutables, como se explica gráficamente en la siguiente Imagen:

Imagen 15: Estructura del ataque

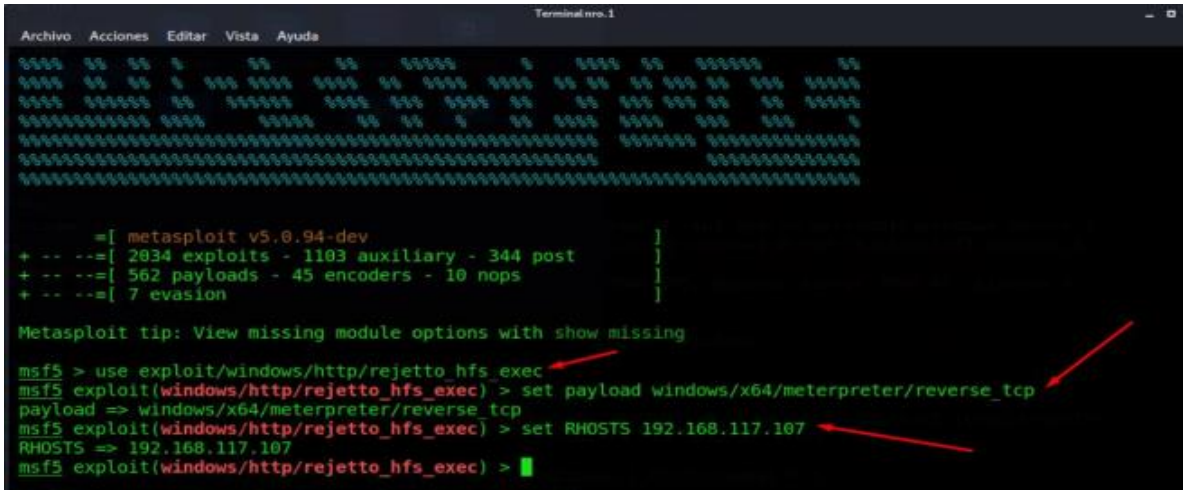


Fuente: https://blog.meterian.com/2019/08/27/vulnerability-focus-remote-code-execution-rce-attacks/

2.3.5 Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Se conocer que el servidor tiene una aplicación vulnerable y escuchando en el puerto 80, en este sentido se requiere demostrar cómo se puede ganar acceso a una Shell (cmd), de forma remota para poder controlar el servidor.

Imagen 16: Vista Metasploit con IP de Windows 7



Fuente: propia

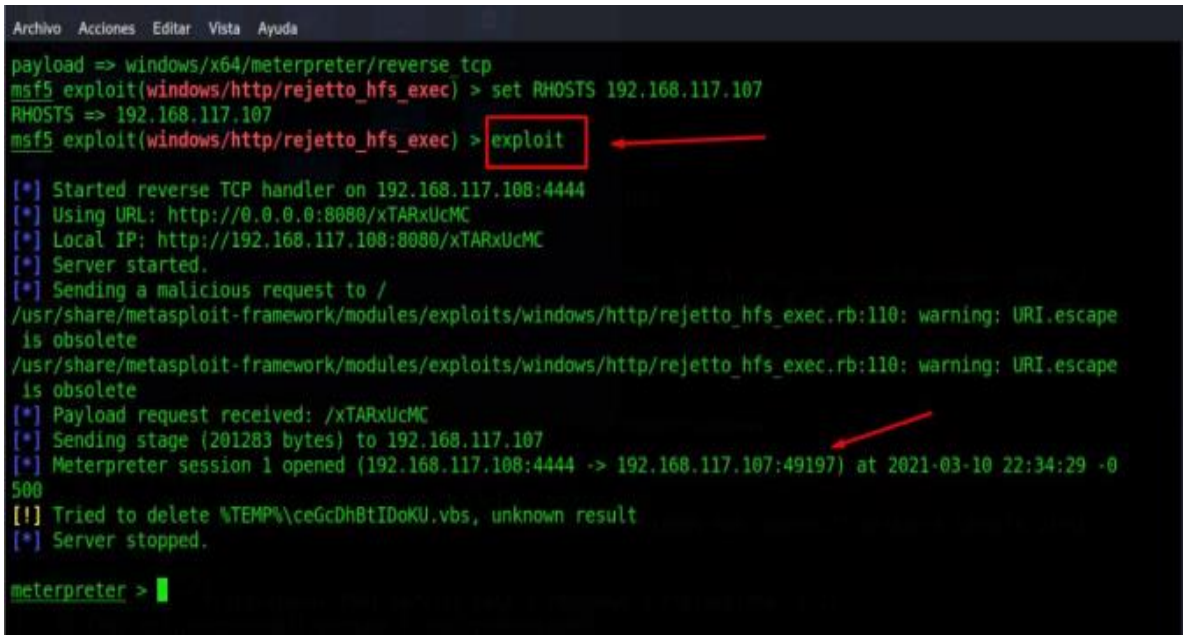
1. Luego se procede a ingresar a la base de datos que contiene los exploits de las vulnerabilidades ya conocidas

2. Se carga un payload para que luego de que sea explotada la vulnerabilidad el equipo servidor haga una conexión reversa al equipo del atacante, en este caso el SO Kali Linux 3.

3. Se especifica el target (RHOST), que será el host remoto, en este caso el servidor que se ataca.

Una vez se definen los parámetros, se explota la vulnerabilidad:

Imagen 17: Análisis de la vulnerabilidad explotada

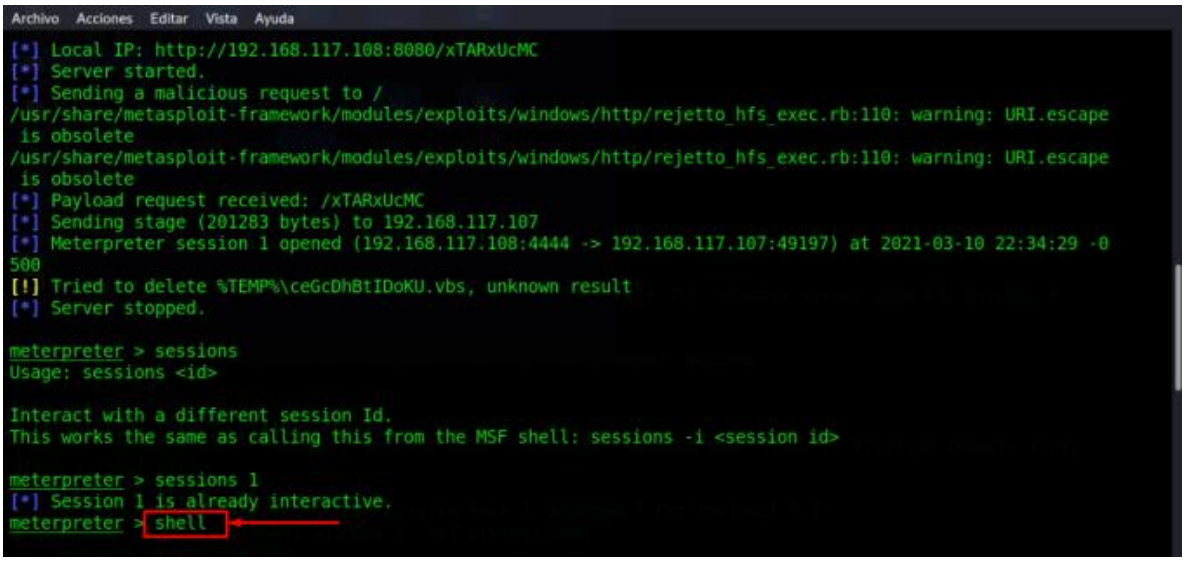


Fuente: propia

Como se observa en la imagen anterior, el equipo Kali Linux establece una sesión con la víctima en este caso el servidor 192.168.117.107.

En la siguiente imagen se muestra como la vulnerabilidad permite ejecutar código en el servidor, dado esto, se puede obtener acceso a la Shell de Windows, en este caso el programa (cmd.exe) que permite ejecutar código como si se estuviera localmente en el servidor:

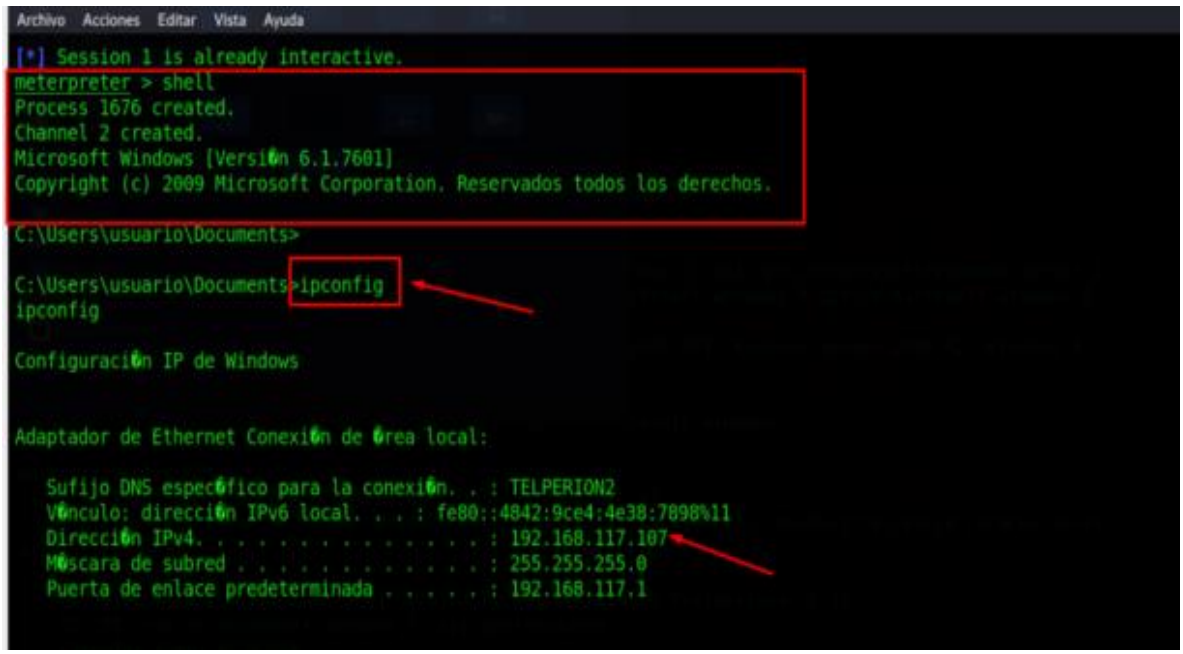
Imagen 18: Ejecución de código



Fuente: propia

Una vez se tenga acceso al equipo atacado, se recolecta información que permita verificar que efectivamente estamos al interior del equipo deseado, se utiliza comando ipconfig:

Imagen 19: Sesión en Windows 7 – ataque exitoso – revisión IP

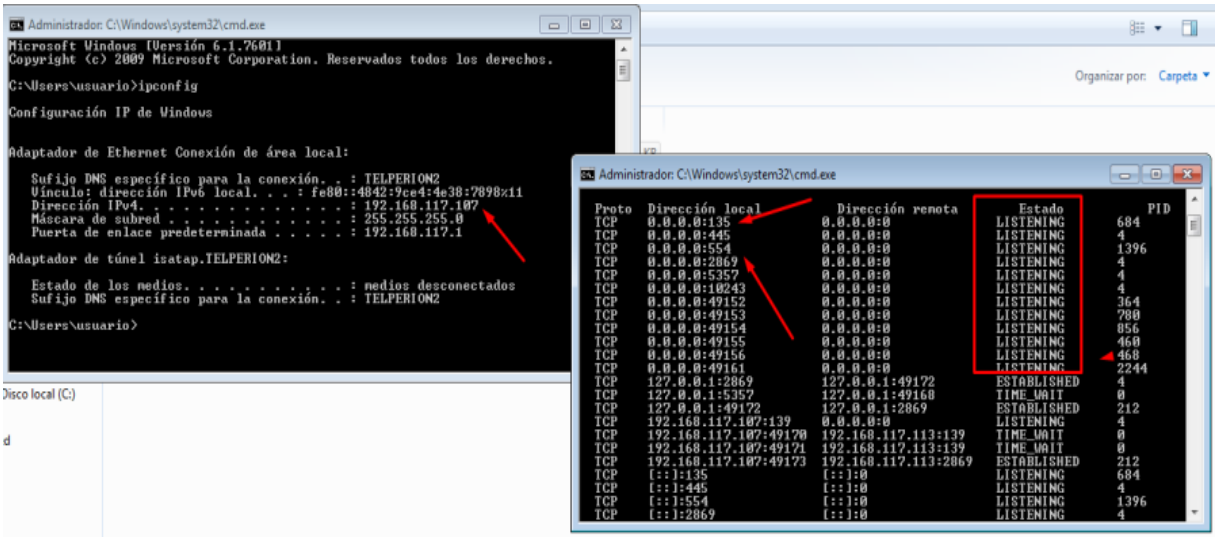


Fuente: propia

Como se pudo evidenciar en la imagen anterior, el atacante obtiene acceso a la Shell de Windows y en este caso se ejecuta el comando ipconfig que muestra la dirección ip del servidor (host remoto), lo que indica que el equipo ahora está bajo control del atacante.

Para confirmar la IP del equipo atacado, se ingresa y se recolecta la información de direccionamiento, con el comando ipconfig, pero esta vez desde Windows 7.

Imagen 20: Confirmación IP atacado



Fuente: propia

Evidenciamos entonces como por medio de la vulnerabilidad presente en una aplicación instalada en un sistema operativo se puede tener un fallo en la seguridad y una fuga en la información, en este caso se evidencia que gracias a Rejetto v. 2.3, se deja abierto el puerto 80 por el cual se puede realizar un ataque exitoso.

2.4 ETAPA 4: CONTENCIÓN DE ATAQUES INFORMÁTICOS.

Para la realización de esta etapa se realizó lectura de una situación problema y de acuerdo con el banco de trabajo realizado en la etapa anterior se dio respuesta a una serie de preguntas. Estas fueron:

2.4.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Sea lo primero aclarar que la mayoría de los ataques que son detectados por lo general se presentan cuando ya han surgido algún tipo de efecto o por el contrario cuando ya llevan mucho tiempo propagándose sobre el sistema logrando su objetivo. No obstante, hay que tener en cuenta que los escenarios y circunstancias donde se presentan pueden variar, por tal motivo es responsabilidad nuestra estar a la vanguardia de estos. Como profesional lo principal que haría ante un ataque en tiempo real sería cortar la red, ya sea desde el equipo o el medio por el cual el ataque se estaba realizando con el fin de garantizar que lo que se estaba realizando no tenga comunicación con el autor intelectual.

Los ataques en tiempo real pueden generar mucho cuestionamiento, ya que siempre suelen surgir interrogantes tales como; ¿Qué tanto afectó al sistema?, ¿Cuál era el ataque exactamente?, ¿Por qué se presentó el ataque?, ¿Cuáles son los objetivos?, ¿Cuáles son sus consecuencias?, etc. Por eso es importante darle un orden a cada acción o pasos a realizar. Ahora bien, una vez interrumpida dicha comunicación la organización o empresa debe ejecutar el plan de contingencia que tiene previamente elaborado, establecido y socializado para este tipo de situaciones, igualmente esa contingencia depende siempre del tipo de ataque que se esté presentando. Por ejemplo, cuándo el ataque es por medio de un ordenador este tiene un centro y es un equipo, pero si el ataque es realizado a través de una

red, entonces las acciones van a ser más extensas y los pasos van a ser diferentes. Hay ataques que pueden ocasionar que los servicios se detengan por un tiempo considerado, esto debe estar controlado, ya que el impacto puede ser muy grave ocasionando pérdidas financieras.

También se pueden realizar acciones como apagar el equipo, finalizar procesos, interrumpir transferencias, etc. Luego de haber identificado la fuente del ataque y de que este suceso se haya interrumpido, el siguiente paso es el proceso de análisis, informe, respuestas, recuperación, solución y toda la documentación que esto conlleva, ya que es necesario realizar la debida denuncia antes las autoridades y esta debe ser explícita y clara en cuánto a lo que sucedió, lo que hizo, lo que afectó y las consecuencias posibles que se originaron.

En la mayoría de los ataques la información o es alterada o es hurtada, por ende, deben restablecerse las copias de seguridad o configuraciones necesarias para restablecer el sistema y los servicios. En otras ocasiones el ataque también genera desconfiguración del sistema y/o daños al sistema operativo, siendo necesario un formateo y reinstalación.

2.4.2 ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team qué medidas de hardenización propondría para que el ataque no se repita?

Las medidas de hardenización que propondría serían las siguientes:

- Mantener actualizado los sistemas operativos.
- Activar las actualizaciones automáticas del sistema y confirmar la instalación de dichas actualizaciones.
- Asignar contraseñas alfanuméricas que no sean vulnerables ante posibles ataques que se puedan presentar y que permitan además el bloqueo ante

intentos fallidos de inserción tanto en acceso al sistema como a los sistemas de archivos de datos.

- Deshabilitar aquellos usuarios genéricos del sistema y eliminar las cuentas locales que no se estén utilizando, limitando los privilegios de las cuentas que queden activas.
- Activar el Firewall de Windows.
- Instalar y activar un Antivirus que proteja y escanee el sistema en tiempo real.
- Implementar las restricciones de software no funcional, implementando listas de software permitido y no permitido, listas blancas y listas negras, para generar cultura de uso en los usuarios.
- Recomendar el uso de red en NAT y para que se limiten los servicios de TCP/IP en lo posible, ya que aquí se habilitan muchas vulnerabilidades de seguridad.
- Se deshabilitará el acceso remoto a los equipos que no lo requieran y si es específicamente necesario, propondrá el uso de canales de comunicación cifrados como SSH, así como el acceso limitado a usuarios específicos.
- En cuanto al respaldo de la información, propondría los respaldos en unidades físicas que no estén ligadas por red del equipo que genera la información.
- Activar las copias de seguridad del equipo.
- Realizar la debida documentación y análisis de los programas que debe tener el equipo con la previa verificación de seguridad.
- Cerrar los puertos que no van a ser utilizados por los procesos del usuario para evitar dejar puertas de acceso a cualquier atacante.
- Cambiar periódicamente la contraseña de usuario del sistema.

2.4.3 ¿Describa con sus palabras las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos?

Un equipo Blue Team es aquel equipo externo de seguridad que se contrata para defender a las organizaciones y empresas de posibles ataques de una manera proactiva. Su función es analizar sistemas, vulnerabilidades, mitigar riesgos, establecer estrategias, hacer seguimiento a los comportamientos del sistema y evaluar amenazas mientras que un equipo de respuesta a incidentes informáticos provee servicios y da soporte para prevenir, gestionar y responder ante los incidentes de seguridad de la información. Son los encargados de solucionar desde el incidente hasta la recuperación de la información que se vio afectada en el ataque. En conclusión, el equipo Blue Team se encarga de establecer una defensa con un seguimiento dedicado a todo lo que concierne al sistema en cuanto a seguridad informática y un equipo de respuesta a incidentes informáticos son conformados básicamente por personal de la compañía que está sufriendo los incidentes y se encargan de enfrentar y dar solución a un ataque ya realizado frente a un sistema.

2.4.4 ¿Si dentro de un equipo Blue Team le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

Inicialmente lo utilizaría para aprender y educar a los empleados de la organización sobre las prioridades que tiene la seguridad de un sistema, las buenas prácticas que se deben implementar, esto con el fin de que las personas puedan entender todo lo bueno y malo que existen en las redes y sistemas informáticos.
Posteriormente lo utilizaría para poder establecer un análisis de vulnerabilidades basados en una biblioteca de casos aportados y de medidas de seguridad previamente establecidas, de experiencias compartidas, de esta forma estaría analizando e implementando a medida que realizo las pruebas en el sistema de la

organización las defensas adecuadas para evitar cualquier tipo de ataques. También puedo implementar buenas prácticas en cuanto a seguridad informática, estableciendo una documentación completa y basada en lo que corresponde únicamente a la organización. Toda esta documentación, aunque no solo resalta aspectos como: activos, redes, aplicaciones, herramientas, privilegios, archivos y transferencias también ayuda a establecer configuraciones necesarias que permitan fortalecer la seguridad y el rendimiento de estos en el sistema, estableciendo a medida monitoreo, estadísticas, análisis, resultados, protección y mantenimiento.

También ayuda a mantener una estructura organizada en cuanto a control de las acciones y los procesos del sistema de una organización. Con esta implementación se ven beneficiados no solo los procesos sistemáticos de la empresa, sino que también afecta positivamente a los procesos de auditorías, certificaciones, rendición de cuentas, balances generales, resultados y decisiones que ayuden a la alta gerencia.

2.4.5 Explique y redacte las funciones y características principales de lo que es un SIEM.

SIEM (Security Information and Event Management), es una solución dedicada y capaz de detectar, responder y neutralizar las amenazas informáticas potenciales que pueden afectar la seguridad de un sistema, ayudando así a tomar las mejores decisiones para proteger el sistema. Su objetivo principal es proporcionar una visión global de la seguridad de las tecnologías de la información.

Esta solución permite además tener control absoluto sobre la seguridad informática de la organización, al tener información y administración total sobre todos los

eventos que suceden segundo a segundo, resultando más fácil detectar tendencias y centrarse en patrones fuera de lo común.

Por medio de SIEM se pueden establecer informes detallados que conlleven a la generación de estrategias por parte de los profesionales de seguridad informática para que el ataque no se lleve a cabo y de esta forma poder dar una respuesta oportuna antes de que se materialice.

Se basa en el principio de buscar patrones y encontrar situaciones fuera de lo común del funcionamiento y al hacer esto se enfoca los recursos de seguridad en lo anormal.

SIEM no solo aporta en la detección de amenazas sino en la verificación de que las normas básicas de seguridad de un sistema se estén cumpliendo, ayudando así a mantener o establecer una infraestructura legal y adecuada. De esta forma los procesos de auditorías futuras se verán beneficiadas, manejando procesos actualizados y acordes a lo establecido por las normas.

Son Funciones principales de un programa SIEM: la recopilación de registros y datos de contexto, la clasificación y normalización, la correlación, las alertas y notificaciones, los establecimiento de prioridades, las visitas en tiempo real y los flujos de trabajo con seguridad.

2.4.6 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.

- **Servidor Proxy:** es una red informática que "hace de intermediario" entre las peticiones que realiza un cliente a otro servidor. Se puede controlar todo lo que viaja por un navegador web, desde el acceso a una página hasta el cifrado de la información y 38 comunicación entre los canales. Por medio de este se puede garantizar la navegación a los sitios seguros, autorizados y confiables.

- **Snort:** Es un programa de monitoreo y detección de intrusiones por red que utiliza bases de datos y patrones de ciberataque conocidos. Está basado en la creación de reglas que conforman patrones de monitoreo de red. El programa funciona bien con reglas y filtros que se configuran desde la instalación inicial para adaptar el proceso de monitoreo a lo que requerimos. Tiene la ventaja de funcionar como un sniffer, es decir, que se puede observar el tráfico en paquetes desde consola o como un IDS (sistema de detección de intrusos) en modo automático o semiautomático.

- **VPN (Virtual Private Network) Red Virtual Privada:** se pueden establecer por medio de este software privacidad en la navegación entre red empresarial, cifrado de datos y ocultamiento de ubicación, direcciones IP, datos de sistema, transferencias y archivos que viajen por la red, ya que la VPN se encarga de crear canales seguros y de acceso controlado, donde se necesita de una autenticación y una sesión autorizada para poder entrar en este canal. De este modo no solo se garantiza lo que se trabaja en la red, sino que se evitan fugas e infiltraciones. Todo se maneja con un cifrado que solo el remitente y el receptor podrán entender.

- **Firewalls o Cortafuegos:** Sistemas operativos como Windows cuentan con un Firewall instalado y preconfigurado cuando este se instala en un computador. Este cortafuegos se puede configurar y hacer más robusto, pero hay cortafuegos dedicados a servidores, los cuales abarcan muchos más puertos y están diseñados para mantener el acceso controlado al sistema. Cerrando y controlando esos puertos, las puertas de acceso a un sistema sin autorizaciones con cada vez menos y elevan la dificultad de acceso a algún presunto atacante.

3. CONCLUSIONES

Con el informe realizado se resaltan los aspectos más relevantes e importantes de cada una de las etapas vistas a lo largo del seminario especializado en equipos estratégicos en Ciberseguridad Red Team & Blue Team, exponiendo al detalle cada una de las falencias encontradas y las pruebas de cómo se realizan los ataques desde su auditoría, vulnerabilidad y posterior explotación. Todo este proceso documentado para tener en cuenta ante un ataque similar.

Además, se conoció y aprendió también sobre las cláusulas de confidencialidad, legislación y normativa que se les aplica a todas aquellas personas que violen las normas de seguridad. Se hizo análisis en un escenario de aquellos procesos ilegales que se encontraron y que no correspondían a un acuerdo legal y ético de una organización y que desde el rol profesional se debió visualizar todas esas falencias y argumentarlas de manera idónea y eficaz.

Por otra parte, se abarcó un caso de estudio real de ciberseguridad y cómo desde una percepción minuciosa poder identificar las implicaciones que se pudieron generar en esta a través de ciertos análisis de herramientas y procedimiento, también se aprendió a evidenciar estos fallos e identificarlos para conocer por donde se estaba filtrando la información, esto con el fin de tener una base para prevenir estos ataques y entender que con solo tener un puerto abierto es suficiente para afectar un sistema.

De igual manera aprendimos de una manera proactiva como contener un ataque en tiempo real y proteger una organizacional al igual que las herramientas que nos ayudarán a contener los ataques informáticos.

Finalmente, con la realización de todas estas etapas se pudo ampliar aún más el conocimiento que se tenía al respecto sobre los equipos estratégicos Blue Team &

Red Team y los controles, descripción y herramientas que nos ayudará a ampliar nuestro conocimiento y como explotarlo en un evento relacionado.

4. RECOMENDACIONES

Se debe siempre tener en cuenta una serie de deberes y responsabilidades como lo es administrar, coordinar el proceso de seguridad en las organizaciones, proponer, coordinar riesgos, mantener organizado la seguridad, promover nuevos proyectos, mantener el sistema estable y alejado de vulnerabilidades internas y externas.

Es necesario implementar barreras físicas y procedimientos de control, como medidas de mitigación y prevención ante amenazas a los recursos e información confidencial, lo que quiere decir, todo lo concerniente a implementar las medidas necesarias para contrarrestar alteraciones de la ciberseguridad.

Se debe estar a la vanguardia de las actualizaciones de seguridad, comprobación de la integridad del Kernel de Linux según sea el caso, sistema de ficheros y configuraciones, modificaciones no autorizadas de las reglas del firewall o búsqueda de software potencialmente.

Por otra parte, es necesario e importante que se destinen gastos para la inversión en la seguridad informática de las organizaciones, ya que existen unos pilares fundamentales que hacen que esta pueda funcionar de una manera segura y que mientras estos pilares se mantengan en la empresa no se va a ver afectada la seguridad de la información ante posibles ataques.

5. VÍDEO

https://www.youtube.com/watch?v=xQMeSY6xsFA&t=1s

6. BIBLIOGRAFIA

- Congreso De La República de Colombia. Ley 1273 de 2009. [27 febrero 2022]. En: Diario Oficial. Enero de 2009 Nro. 47.223. p.p. 14-25.

- Leyes desde 1992. Vigencia expresa y control de constitucionalidad: Ley 1581 2012. [En línea]. [28 febrero de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley15812012.html

- Congreso de la República de Colombia. Ley 1341 de 2009. [27 febrero 2022]. En: Diario Oficial. Julio, 2009. Nro. 47.426.

- Departamento Nacional de Planeación. Consejo Nacional de Política Económica y Social Conpes 3701. [1 de marzo de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

- Policía Nacional de Colombia. Normatividad sobre delitos informáticos. [27 febrero 2022] [En línea]. Disponible en: https://www.policia.gov.co/denunciavirtual/normatividad-delitos-informaticos.

- LEACOCK, S. Introducción al escaneo de red y vulnerabilidad con Nmap. [12 de mayo de 2019]. [En línea]. [28 febrero de 2022]. Disponible en: https://backtrackacademy.com/articulo/introduccion-al-escaneo-de-red-y-vulnerabilidades-con-nmap#:~:text=Nmap%20es%20una%20herramienta%20opensource,seguridad%20y%20monitoreo%20de%20redes.

- JAGREY. ¿Qué es metasploit y como se usa bien? [27 febrero 2022]. [En línea]. Disponible en: https://www.funinformatique.com/es/curso/que-es-metasploit-y-

como-usarlo-bien/

- ARAYA, J. Guía de instalación de OpenVas en Kali Linux. [28 febrero de 2022]. [en línea [. Disponible en: https://www.spainclouds.com/blog/guia-de-instalacion-de-openvas-en-kali-linux

- Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. Ley 1273 de 2009. [En línea]. [24 de febrero 2022]. Disponible en: https://www.enticconfio.gov.co/ley-1273-del-2009

- COPNIA. Código de ética. [En línea]. [25 de febrero 2022]. Disponible en: https://www.copnia.gov.co/tribunaldeetica/codigo-de-etica

- COPNIA. Ley 842 de 2003. [en línea]. [24 de febrero 2022]. Disponible en: https://www.copnia.gov.co/nuestraentidad/normatividad/ley-842-de-2003

- EL TIEMPO. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [En línea]. [24 de febrero 2022]. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-15141236

- EL ESPECTADOR. Caso Andrómeda y sus interrogantes. [En línea]. [24 de febrero 2022]. Disponible en: https://www.elespectador.com/noticias/judicial/casoandromeda-y-sus-interrogantes/

- EL ESPECTADOR. Los detalles de Andrómeda, según la Procuraduría. [En línea]. [24 de febrero 2022]. Disponible en: https://www.elespectador.com/noticias/judicial/losdetalles-de-andromeda-segun-laprocuraduria/

- JAGREY. ¿Qué es metasploit y como se usa bien? [27 febrero 2022]. [En línea]. Disponible en: https://www.funinformatique.com/es/curso/que-es-metasploit-y-como-usarlo-bien/#:~:text=Metsploit%20es%20un%20herramienta%20para,reescrito%20en%20el%20lenguaje%20Ruby

- INCIBE-CERT. Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014- 6287). [En línea]. [27 de febrero de 2022]. Disponible en:. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

- EXPLOIT DATABASE. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). CVE-2014- 6287CVE-111386. [En línea]. [03 de marzo de 2022]. Disponible en: https://www.exploit-db.com/exploits/34852

- Software Engineering Institute. Rejetto HFS versions 2.3, 2.3a, and 2.3b are vulnerable to remote command execution. [online] [27 february 2022]. Available is: https://www.kb.cert.org/vuls/id/251276

- CVE DETAILS. Security vulnerabilities of Rejetto Http File Server: List of all related CVE security vulnerabilities. [Oline]. [03 de marzo de 2022]. Available is: https://www.cvedetails.com/vulnerability-list/vendor_id-14180/product_id-29196/RejettoHttp-File-Server.html

- ASTUDILLO, K. Analizador de Vulnerabilidades Nessus: “Hacking Ético Video Series #6”. [en línea]. [28 febrero 2022]. Disponible en: Internet: https://www.youtube.com/watch?v=7qJ1wNRkEt4&feature=youtu.be

- PENTESTING. “Kali Linux - Metasploit VM”. [En línea]. [3 marzo 2022]. Disponible en: https://www.youtube.com/watch?v=r7wJfOGsIr4&feature=youtu.be

- INFOLAFT. Anticorrupción, fraude y LA/FT. ¿Qué hacer antes, durante y después de un ataque informático? [en línea]. [13 de marzo 2022]. Disponible en: https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

- FERNANDEZ. Begoña. Pasos a seguir ante un ataque informático. En: Deloitte. [en línea]. [13 de marzo 2022]. Disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

- GRUPO SMARTEKH. ¿Qué es hardening? [en línea]. [14 de marzo 2022]. Disponible en: https://blog.smartekh.com/que-es-hardening

- SOFECOM. SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran. [en línea]. [13 de marzo 2022]. Disponible en: https://sofecom.com/que-es-un-siem/

- PETTERS. Jeff. What is SIEM? A Beginner's Guide. En: Varonis. [online]. [13 de marzo 2022]. Disponible en: https://www.varonis.com/blog/what-is-siem/

- «CIS Controls Spanish Translation», s. f. «Código de ética para ingenieros». [en línea]. [14 de marzo 2022]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

- Red Team, Blue Team y Purple Team: funciones y diferencias». [en línea]. [14 de marzo 2022]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purpleteam-ciberseguridad/