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

JHON ALEXANDER ANGARITA CARRASCAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
SEMINARIO ESPECIALICADO EQUIPO ESTRATÉGICO EN CIBERSEGURIDAD:
RED TEAM & BLUE TEAM
OCAÑA, NORTE DE SANTANDER
2021

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

JHON ALEXANDER ANGARITA CARRASCAL

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

M.SC. JOHN FREDY QUINTERO
Director de curso.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
SEMINARIO ESPECIALICADO EQUIPO ESTRATÉGICO EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
OCAÑA, NORTE DE SANTANDER
2021

RESUMEN

WhiteHouse Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa, con lo que ha alcanzado la posición como la organización más sólida en el campo de la seguridad informática, por concerniente ha decidido que es el momento de conformar equipos de Red Team y Blue Team dentro de su estructura para aumentar los protocolos de seguridad al interior de esta.

En este informe se evidencia el desarrollo de las actividades propuestas para los diferentes escenarios, donde se analizó el carácter legal y ético de la normatividad vigente en Colombia referente a delitos cibernéticos, también se profundizaron conceptos de equipos Red Team y Blue Team, los cuales se aplicaron por medio de ataques y mitigación de los mismos en sistemas con alto riesgo de vulnerabilidad.

CONTENIDO

pág.

TABLA DE FIGURAS

GLOSARIO

ATAQUE INFORMÁTICO: intento de una persona o grupo organizado, mediante el cual se infringe daños o modifica un sistema o red por varias razones[1].

BLUE TEAM: grupo de personas que realizan evaluaciones de vulnerabilidad de la red operativa y proporcionan técnicas de mitigación a los clientes que necesitan una revisión técnica independiente de su postura de seguridad de la red. Blue Team identifica las amenazas y los riesgos de seguridad en el entorno operativo y, en cooperación con el cliente, analiza el entorno de la red y su estado actual de disponibilidad de seguridad. Con base en los hallazgos y la experiencia del Blue Team, brindan recomendaciones que se integran en una solución de seguridad comunitaria general para aumentar la postura de preparación de ciberseguridad del cliente. A menudo, Blue Team se emplea solo o antes de un empleo del equipo rojo para garantizar que las redes del cliente sean lo más seguras posible antes de que el equipo rojo pruebe los sistemas[2].

CIBERATAQUE: conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas[3].

CIBERSEGURIDAD: protección de los activos a través de una serie de estrategias, metodologías y tecnologías para protegernos de las amenazas actuales y es un nuevo punto de partida para lo que vendrá en el futuro[4].

CONTROL DE ACCESO: forma como se garantiza la seguridad a un espacio restringido.

FIREWALL: dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y permite o bloquea paquetes de datos según un conjunto de reglas de

[1] ALVEAR REINOSO, Francisco Xavier. (2019). Análisis y diseño de una propuesta para mitigar ataques cibernéticos a correos electrónicos utilizando técnicas de Hacking Ético. Recuperado de: https://dspace.ups.edu.ec/bitstream/123456789/17035/1/UPS-ST004012.pdf

[2] CSRC. Computer Security Resource Center. Recuperado de: https://csrc.nist.gov/glossary/term/red_team

[3] IBERDROLA. (2021). Ataques cibernéticos: ¿Cuáles son los principals y cómo protegerse de ellos? Recuperado de: https://www.iberdrola.com/innovacion/ciberataques

[4] CORLETTI ESTRADA, Alejandro. (2017). Ciberseguridad Una Estrategia Informático Militar. Recuperado de: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/Libro-Ciberseguridad_A.Corletti_nov2017.pd.pdf

seguridad. Su propósito es establecer una barrera entre su red interna y el tráfico entrante de fuentes externas (como Internet) para bloquear el tráfico malicioso como virus y piratas informáticos[5].

FIRMWARE: software que se utiliza para manipular el hardware.

IDS: sistema de detección de intrusos es utilizado para conocer por medio del análisis del tráfico en la red las actividades del mismo, con el fin de determinar los accesos no permitidos y de esta forma prevenir las intrusiones.

METASPLOIT: es una herramienta de prueba de penetración ampliamente utilizada que hace que la piratería sea mucho más fácil de lo que solía ser. Se ha convertido en una herramienta indispensable tanto para Red Team como para Blue Team[6].

PENTESTING: se puede determinar como una auditoria, se puede definir como un método aplicado mediante el cual se simula un ataque real a un sistema informático con el fin de detectar y dar solución a los problemas que pueda tener a nivel de seguridad de la información[7].

POLITICAS: lineamientos definidos por una entidad los cuales deben cumplir el personal para cumplir los objetivos o metas propuestas.

RED TEAM: grupo de personas autorizadas y organizadas para emular las capacidades de ataque o explotación de un adversario potencial contra la postura de seguridad de una empresa. El objetivo de Red Team es mejorar la ciberseguridad empresarial demostrando los impactos de los ataques exitosos y demostrando lo que funciona para los defensores (es decir, el Blue Team) en un entorno operativo. También conocido como Cyber Red Team[8].

---

[5] FORCEPOINT. (2021). CYBER EDU, What is a Firewall?. Recuperado de: https://www.forcepoint.com/es/cyber-edu/firewall

[6] PORUP, JM. (2019). What is Metasploit? And how to use this popular hacking tool. Recuperado de: https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html

[7] CATORIA, Fernando. (2013) Pruebas de Penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. Recuperado de https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetración-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

[8] CSRC. Computer Security Resource Center. Recuperado de: https://csrc.nist.gov/glossary/term/blue_team

RIESGOS: posibilidad que ocurra un evento inesperado y esto afecte los servicios que ofrece una entidad de forma negativa.

SIEM: gestión de eventos e información de seguridad (SIEM), es un software que mejora la conciencia de seguridad de un entorno de TI al combinar la gestión de la información de seguridad (SIM) y la gestión de eventos de seguridad (SEM). Las soluciones SIEM mejoran la detección de amenazas, el cumplimiento y la gestión de incidentes de seguridad mediante la recopilación y el análisis de datos y fuentes de eventos de seguridad históricos y en tiempo real[9].

VULNERABILIDAD: debilidad del sistema de red o equipos de cómputo en el cual un extraño puede atacar y comprometer la seguridad de la información.

[9] McAfee. (2021). What Is Security Information And Event Management (SIEM)?. Recuperado de: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-siem.html

INTRODUCCIÓN

Actualmente la información es un activo muy importante en las empresas, por lo cual se le debe dar un manejo altamente confidencial, al poseer la misma en formatos digitales se puede tener expuesta a riesgos informáticos, a este tipo de datos pueden acceder personas no autorizadas con el fin de manipularlos, pero ellos están protegidos en la actualidad por leyes o normas con el fin de garantizar o disminuir el acceso abusivo a los mismos. Para evitar este tipo de riesgos, es necesario crear controles o políticas de seguridad ante ataques externos a la infraestructura tecnológica de la organización, allí es donde actúan de manera organizada los equipos Redteam y Blueteam, quienes tratan de proteger en alto porcentaje la integridad y disponibilidad de la data en las organizaciones.

OBJETIVOS

GENERAL

Profundizar en cuanto a las leyes, decretos, herramientas de ciberseguridad, vulnerabilidades, Hardenización, SIEM y herramientas de contención de ataques informáticos para proteger la empresa Whitehouse Security de posibles ataques y vulnerabilidades.

ESPECÍFICOS

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

DESARROLLO DEL INFORME

1. LEYES Y DECRETOS QUE EXISTEN EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES

1.1 LEY 1273 DE 2009

La ley modifica el código penal para un nuevo bien jurídico denominado de la protección de la información y de los datos. También castiga a aquellas personas o entidades que atente contra la confidencialidad, integridad y disponibilidad de la información y datos.

La presente ley establece cuales son acciones consideradas delitos[10].

Acceso abusivo a un sistema informático*:* Se considera toda acción que un usuario acceda sin autorización a un sistema informático por medio de herramientas o técnicas que violen la seguridad establecida.

Obstaculización ilegitima de sistema informático red de telecomunicaciones: son aquellas acciones de usuarios que sin estar autorizados bloquee, niegan u obstaculicen un sistema informático o información allí contenida

Interceptación de datos informáticos: será juzgada toda actividad que incluya la interceptación de información sin autorización.

Daño informático: son consideradas como todas las actividades que dañe, borren, modifiquen, altere o suprima información que se encuentra asegurada o protegida,

Uso de software malicioso: se considera como toda actividad en la cual se negocie, cree o trasfiera cualquier tipo de software malicioso en el territorio nacional.

[10] Policía Nacional. (2021). Normatividad sobre delitos informáticos. Ley 1273 de 2009. Recuperado de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Violación de datos personales: son aquellas actividades en las cuales se utiliza los datos de personas extraídos ilegalmente para beneficio propio o de un tercero

Suplantación de sitios WEB para captura datos personales: se considera un delito todo aquel que suplante, diseñe, desarrolle, trafique o programe páginas web con el fin de beneficiarse a él o un tercero.

Hurtos por medios informáticos y semejantes: por el cual se establece como un delito todo aquel que hurte información de los sistemas operativos o una red por medio de herramientas y actividades prohibidas.

Trasferencia no consentida de activos: son todos aquellos actos que por medio de actividades o herramientas pueda generar manipular información considera confidencia a la cual se realiza trasferencia sin acuerdo de alguna de las partes.

Agravantes: se aumenta la pena si el acusado actuó sobre alguno de los siguientes puntos.

* Ataque a las redes de comunicación estatales, oficiales del sector financiero, nacionales o extranjeras
* Ser un servidor público
* Aprovecharse de la confianza depositada
* Revelar información considera confidencial
* Obteniendo provecho para sí o para un tercero
* Con fines terroristas o generando riesgos para la seguridad nacional
* Utilizando a un tercero en su buena fe

1.2 LEY ESTATUTARIA 1581 DE 2012

En la presente ley se dictan disposiciones generales para la protección de datos personales, esta ley complementa al derecho que tenemos como personas para autorizar que información propia es almacenada en sistemas de información digitales, así como actualización y rectificación de los mismos. Cabe resaltar que esta ley está vigente para información de personas naturales[11].

[11] IMSALUD. (2019). ABC Ley 1581 de 2012 Protección de Datos Personales. Recuperado de https://www.imsalud.gov.co/web/sin-categoria/abc-ley-1581-de-2012-proteccion-de-datos-personales/

2. ETAPAS DEL PENTESTING

El termino Pentesting también se puede determinar como una auditoria, se puede definir como un método aplicado mediante el cual se simula un ataque real a un sistema informático con el fin de detectar y dar solución a los problemas que pueda tener a nivel de seguridad de la información. Para realizar dicho test, se debe tener en cuenta las etapas o fases recomendadas para que el trabajo a realizar tenga un orden respectivamente, dichas etapas se pueden clasificar de la siguiente manera[12]:

Recopilación de Información. En este punto se busca la manera de obtener la mayor información precisa referente al sistema informático al cual se le aplicará el Pentesting, entre dicha información se puede obtener direcciones IP, puertos de comunicación, motores de base de datos. El software Nmap se podría mencionar como ejemplo útil de aplicación para obtener cierta información mencionada anteriormente.

Búsqueda de vulnerabilidades. En esta etapa se empieza a buscar las falencias que pueda tener el sistema que se quiere explotar, en esta búsqueda se pueden emplear ataques de fuerza bruta con Hydra Software o de denegación de servicio (DoS) con LOIC software, entre otras técnicas.

Explotación de Vulnerabilidades. En esta fase posterior a la detección de vulnerabilidades, se obtiene acceso al sistema por medio de diferentes métodos aplicados para la explotación, un ejemplo que podría mencionarse podría la inyección de código SQL mediante herramientas como SQLmap o Metasploit.

Entrega de reporte. En entornos reales se realizan los respectivos informes a los interesados donde se indican las vulnerabilidades o falencias detectadas y como se han explotado las mismas. Cabe resaltar que se podría entregar dos informes, el técnico y ejecutivo (el cual será entregado en lenguaje comprensible a personas que no conocen los términos técnicos respectivos al trabajo realizado).

[12] CATORIA, Fernando. (2013) Pruebas de Penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. Recuperado de https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetración-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

3. HERRAMIENTAS DE CIBERSEGURIDAD

3.1 HERRAMIENTAS

Metasploit: Es una herramienta de software para realizar auditorías a sistemas informáticos, está basada en la colaboración de la comunidad de código abierto, por lo cual permite que sea de mayor acceso a la misma. Es de gran utilidad para los equipos de seguridad de las empresas ya que permite verificar vulnerabilidades a las que se está expuesto y así mejorar la conciencia en seguridad de los equipos de seguridad de la información[13].

Nmap: Es una herramienta de software gratuita de código abierto para la detección de vulnerabilidades y redes. Los administradores de red usan Nmap para establecer qué dispositivos se están ejecutando en sus sistemas, descubrir los hosts activos y los servicios que están vigentes o activos, encontrar puertos abiertos y detectar problemas de seguridad[14].

OpenVAS: es un Open source Vulnerability scanner muy práctico y eficiente que permite detectar problemas de seguridad e información específica de vulnerabilidades que pueden ser explotadas y de esta atentar contra la confidencialidad, disponibilidad e integridad de los datos almacenados y procesados en nuestros sistemas informáticos[15].

3.2 SERVICIOS EN LÍNEA

ExploitDB o Database: Es una página o directorio web donde hackers y equipos de blue team dan a conocer información referente a vulnerabilidades en aplicaciones, servicios, etc. Exponiendo datos importantes sobre cómo aprovechar falencias con instrucciones dadas para vulnerar las mismas. Dicha página es un arma de doble filo, ya que se puede hacer mal uso de la información con fines diferentes a salvaguardar la estabilidad de los sistemas expuestos[16].

---

[13] RAPID 7 METASPLOIT. El marco de pruebas de penetración más utilizado del mundo. Recuperado de https://www.metasploit.com/

[14] NMAP.ORG. Nat Security Scanner. Recuperado de https://nmap.org/

[15] OPENVAS BY GREENBONE. Open Vulnerability Assessment Scanner. Recuperado de https://www.openvas.org/

[16] OFFEBSIVE SECURITY. (2021). Explotar la Base de Datos por seguridad ofensiva. Recuperado de https://www.exploit-db.com/

CVE (Common Vulnerabilities and Exposures, siglas CVE): Las Vulnerabilidades y exposiciones comunes forman una gran lista de fallas de seguridad en sistemas informáticos que se encuentran disponibles públicamente por medio de su directorio o sitio web. Los CVE permiten que los especialistas le den importancia o prioridad a la solución en seguridad de los puntos vulnerables que se mencionan allí, con el fin de asegurar y garantizar la estabilidad de su infraestructura tecnológica[17].

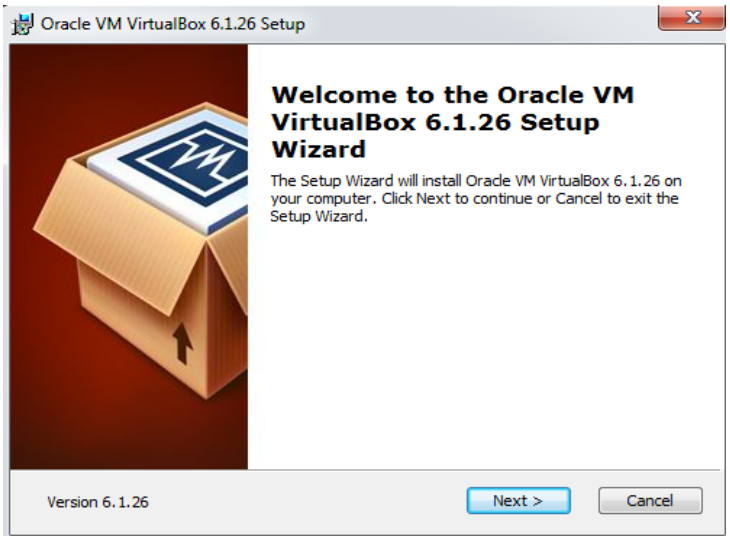
[17] CVE. (2021). Catalogar las Vulnerabilidad de Seguridad. Recuperado de https://cve.mitre.org/

4. BANCO DE TRABAJO

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

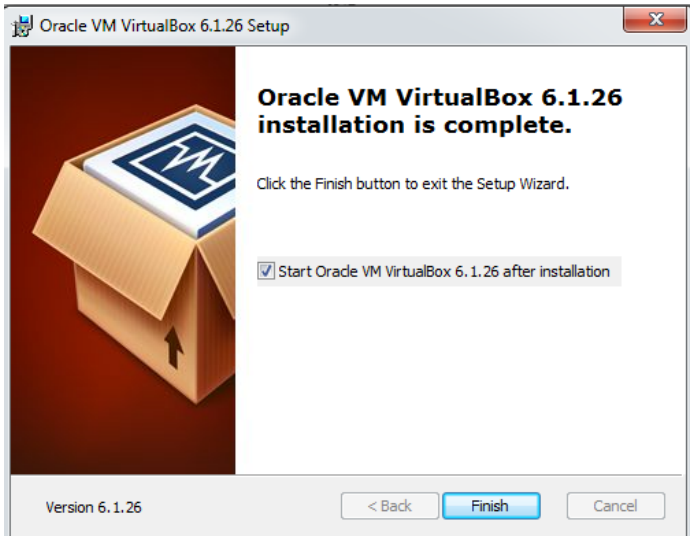
Se inicia la instalación de VirtualBox 6.1.26 y la respectiva ejecución de la aplicación.

Figura 1**.** Instalación de VirtualBox



Fuente: Elaboración propia

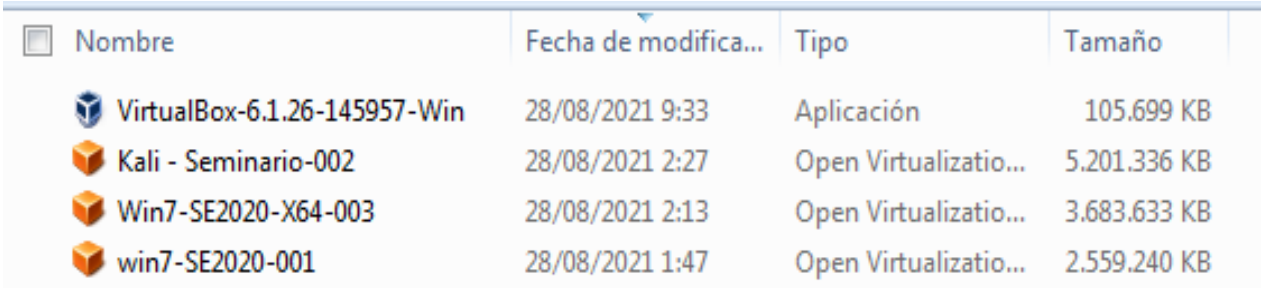
Figura 2. Finalización de la instalación de VirtualBox



Fuente: Elaboración propia

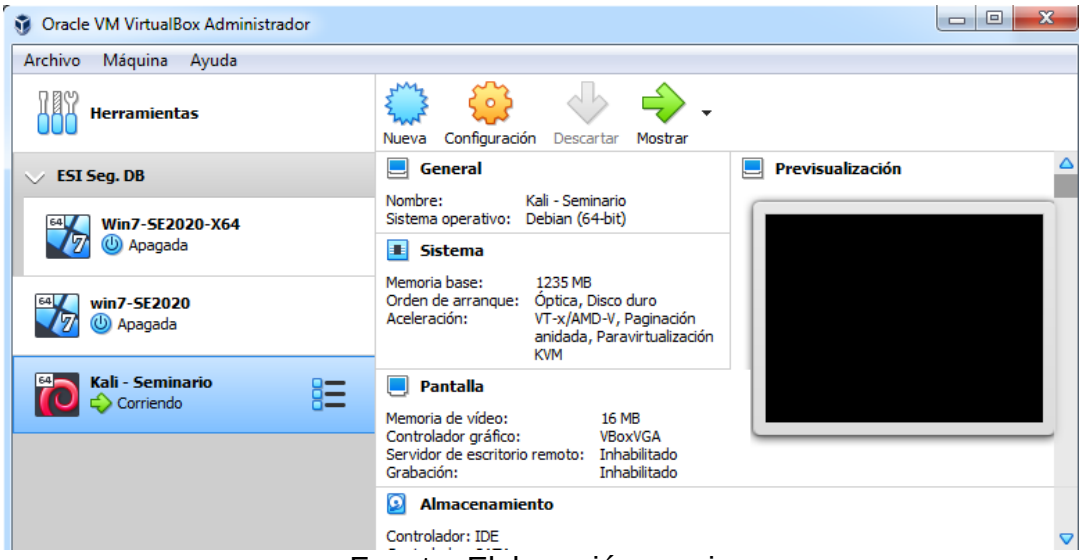
Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

Figura 3. Descarga archivos para el montaje del banco de trabajo



Fuente: Elaboración propia

Figura 4. Inclusión archivos . OVA en virtualbox



Fuente: Elaboración propia

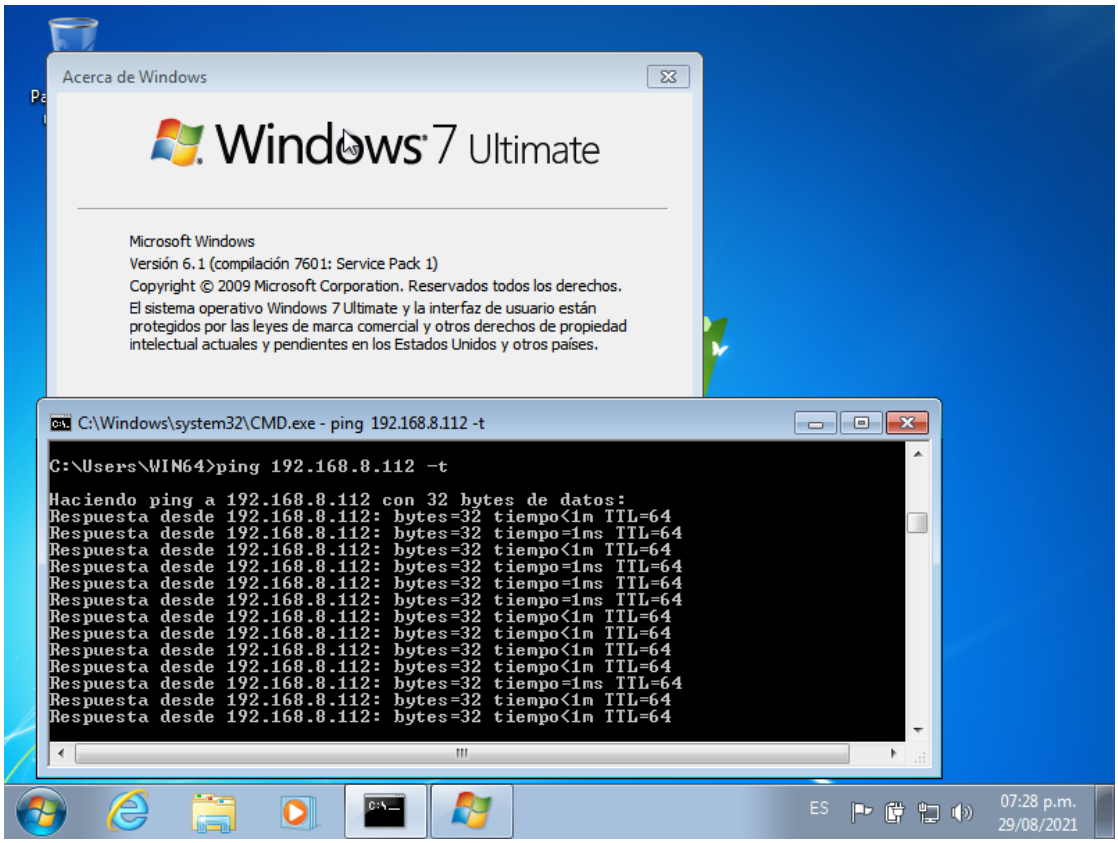
Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Los archivos VDO compartido por google drive presentaron problemas de compatibilidad, por ende, no pude trabajar sobre los mismos, de igual manera informarle mi computador no funcionó con sistema a 32 bits.

Por medio de la siguiente captura de pantalla se muestra la evidencia del proceso ejecutado con el fin de validar la comunicación entre las máquinas virtuales.

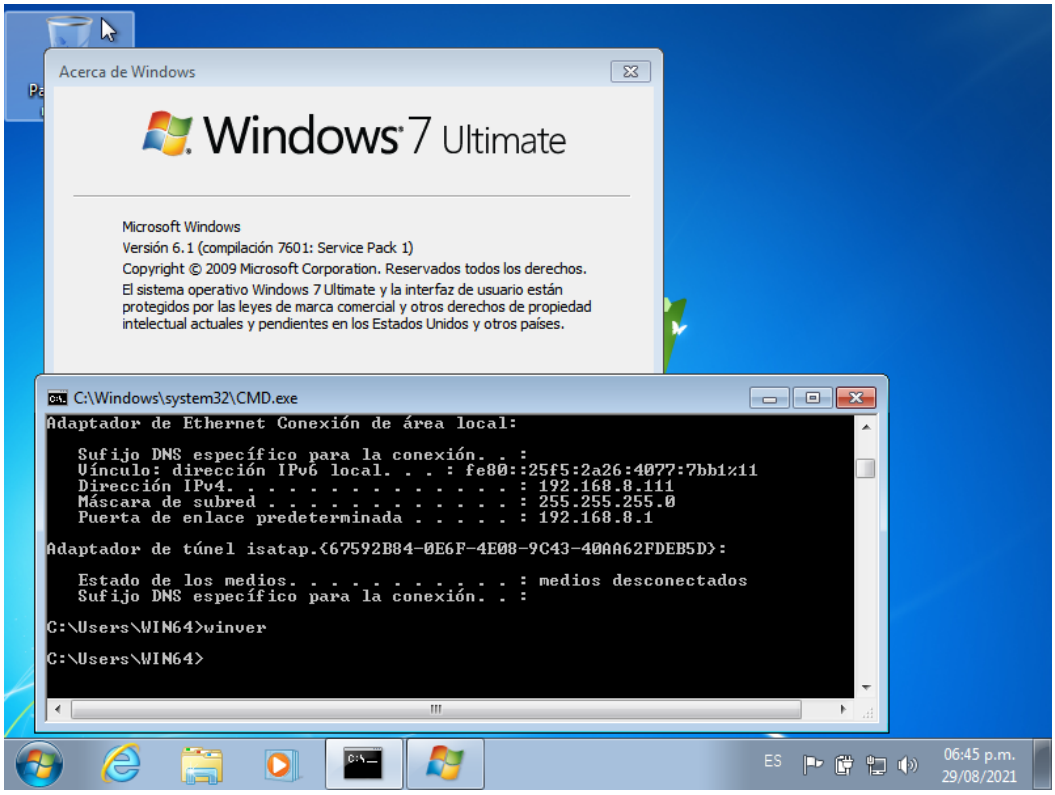
Se aplica el comando ping **192.168.8.112 -t** desde la maquina Windows con el fin de recibir respuesta desde Kali Linux, siendo este satisfactorio.

Figura 5. Prueba de conexión entre los hosts Kali Linux y Windows 7 x64



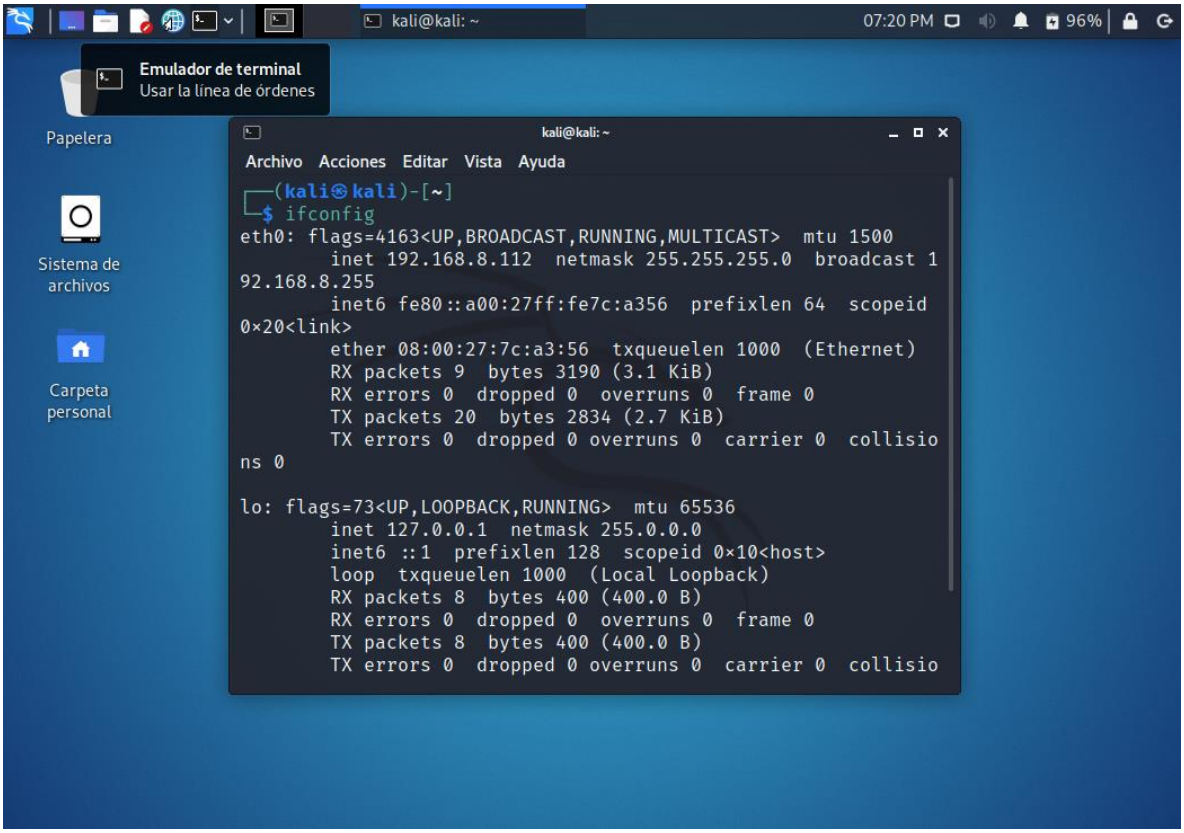
Fuente: Elaboración propia

Figura 6. Máquina virtual Windows 7 x64 con IP 192.168.8.111



Fuente: Elaboración propia

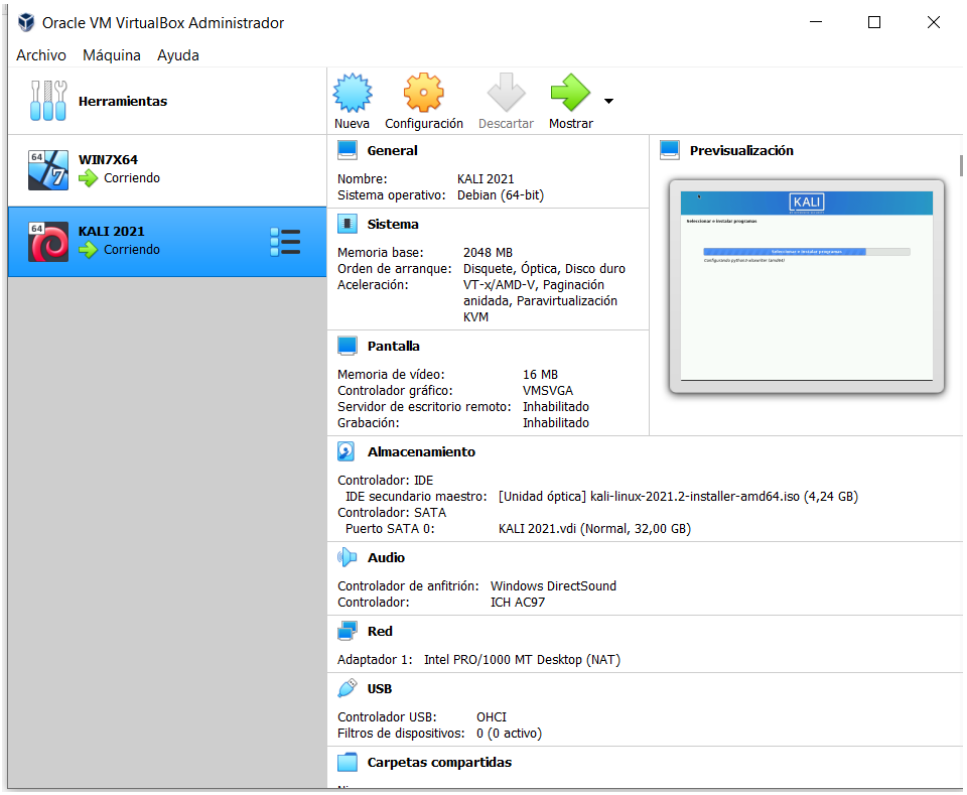
Figura 7. Máquina virtual Kali Linux 2021 con IP 192.168.8.112



Fuente: Elaboración propia

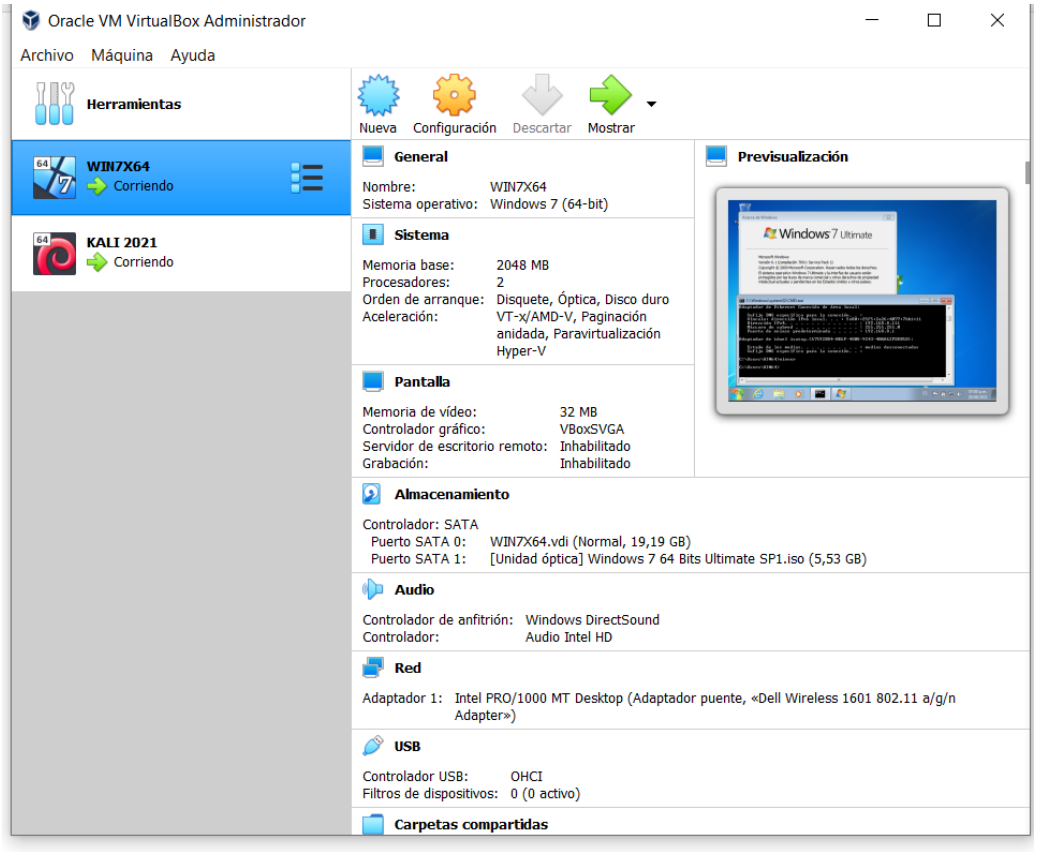
Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Figura 8. Montaje del banco de trabajo y características de hardware para Kali Linux



Fuente: Elaboración propia

Figura 9. Montaje del banco de trabajo y características de hardware para Windows 7 x64



Fuente: Elaboración propia

5. EVIDENCIAS DEL PROCESO ILEGAL Y NO ÉTICO QUE SE ESTÉ ESTIPULADO

Luego de analizar el anexo 3 – Acuerdo, se logra evidenciar diferentes anomalías de carácter legal y ético, las cuales violan la ley y políticas de privacidad o tratamiento de datos vigente, además deja mucho que pensar de la empresa WhiteHouse Security quien inicia un proceso "irresponsable" de selección de personal sin revisar previamente los puntos del contrato (acuerdo) elaborado por su ex abogado, quien fue despedido por la organización al hallar procesos ilícitos de su parte.

Después de estudiar la situación queda un gran interrogante en este momento:
¿Es la organización quien aprovecha la redacción del acuerdo para librar responsabilidad con el nuevo personal contratado o es negligencia de la misma proceder sin verificar el vacío legal donde finalmente se desconoce quién será perjudicado?

A continuación, se señalan los fragmentos ilegales del anexo acuerdo y se mencionan donde se ubican:

- ✓ **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.

- ✓ **Clausula Segunda.**

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

  2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas,

interceptación de información, accesos abusivos a sistemas informáticos". **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

- ✓ Clausula Tercera.

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

- ✓ Clausula Cuarta.

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

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

7. Responder por el mal uso que le den sus representantes a la **información confidencial.**

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**.**

- ✓ Clausula Octava.

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.** <u>En caso 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.</u>

6. ARTÍCULOS DE LA LEY 1273 QUE SE PUEDEN VULNERAR EN EL ACUERDO

Al descubrir procesos ilegales en el anexo 3 – Acuerdo, se aclara porque infringe los artículos de la ley 1273 de 2009[18] en los siguientes puntos:

- ✓ Clausula Segunda.

  En esta cláusula se vulnera el artículo 269A y 269C porque se pide guardar la confidencialidad de procesos en los cuales se obtuvo información de manera ilícita, entre estos podemos mencionar chuzadas, acceso abusivo a sistema informático e interceptación de datos sin consentimiento del propietario.

- ✓ Clausula tercera y cuarta.

  En esta cláusula se vulnera el artículo 269F ya que independiente de la fuente o soporte y sin que se informe sobre el carácter confidencial de la información, se hace uso de esta sin estar facultados, llegando a realizar una violación de datos personales.

- ✓ Clausula Octava.

  En esta cláusula se vulnera el artículo 269H debido a su circunstancia de agravación punitiva por quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información.

[18] Policía Nacional. (2021). Normatividad sobre delitos informáticos. Ley 1273 de 2009. Recuperado de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

7. ARGUMENTACIÓN DEL TRABAJO EN THE WHITEHOUSE, DONDE LA ORGANIZACIÓN DISPONE DE UN SUELDO DE $15.000.000 DE PESOS COLOMBIANOS MENSUALES Y CONTRATO VITACLICIO

Mi respuesta seria negativa ante esta opción laboral, a pesar del sueldo tentador y que colocaría a más de uno a dudar, preferiría desistir de esta oportunidad ya que viola mi conducta como ingeniero, quedando expuesto a sanciones fuertes por parte de quien terminaría definiendo mi futuro profesional basada en los hechos que se demuestren, para este caso en particular seria COPNIA quien se basaría en la argumentación que se dispone en su código de ética para ingenieros.

A continuación, se mencionan algunos de los argumentos dispuestos en el Código de Ética para el ejercicio de la Ingeniería de COPNIA[19] y que podría vulnerar al aceptar el cargo:

Título IV. Capitulo II
ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES.

b) Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados.

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

ARTÍCULO 32. PROHIBICIONES GENERALES A LOS PROFESIONALES. Son prohibiciones generales a los profesionales:

b) Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley

[19] COPNIA. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Recuperado de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

g) Causar, intencional o culposamente, daño o pérdida de bienes, elementos, equipos, herramientas o documentos que hayan llegado a su poder por razón del ejercicio de su profesión

8. PUNTO DE VISTA DEL CASO OPERACIÓN ANDROMEDA BUGGLY

De acuerdo a la información consultada referente a la noticia mencionada, aparentemente se logra evidenciar que en el actuar de Buggly Ethical Hacking quien era la fachada de la operación Andrómeda 2021 de la Central de Inteligencia Técnica del Ejército Nacional, se vulneraron de cierta manera las leyes de protección de datos personales y de sistemas informáticos, es decir la ley 1273 de 2009 y 1581 de 2012.

A continuación, se menciona de qué forma se violaron ciertos artículos de la ley 1273 con el actuar de la operación Andrómeda:

- Artículo 269A y 269G: *Acceso abusivo a un sistema informático* y s*uplantación de sitios web para capturar datos personales*.

  Se obtuvo información confidencial por medio de diferentes métodos o técnicas de ethical hacking en los cuales se evidencia la infracción pertinente.

- Artículo 269E: *Uso de software malicioso*.

  Mencionan que se empleó software malicioso para acceder a información de personas, lo que equivale a interceptación de comunicaciones, el cual enviaba información hacia donde estaba alojado el sitio web de Buggly. El malware tomaba capturas de pantalla del escritorio, enviaba una copia de lo que entraba y salía a través de sus redes y registraba lo que tecleaban, según reportes de medios de comunicación.

- Artículo 269F y 269J: *Violación de datos personales y transferencia no consentida de activos*.

  Algunos de los involucrados fueron acusados de vender bases de datos de los desmovilizados de las Farc, entre otros tipos de información de suma reserva publica, la cual habrían obtenido de carácter ilegal de las redes internas del ejército sin consentimiento alguno de sus superiores.

Es evidente como este tipo de leyes siguen siendo violadas de manera recurrente, ya que es difícil la identificación de los sucesos y el rastreo de las personas que están detrás de las vulneraciones a sistemas informáticos día a día, por esto es preciso recalcar la importancia de la seguridad informática por parte de los profesionales del área, donde deben ayudar a proteger o salvaguardar la confidencialidad y disponibilidad de la información en los diferentes escenarios que se aplique.

9. HERRAMIENTAS SOFTWARE UTILIZADAS - EVIDENCIAS DE LOS COMANDOS UTILIZADOS Y RESULTADOS QUE ARROJÓ CADA HERRAMIENTA

Herramientas Software utilizadas para la solución del problema propuesto:

- ✓ VirtualBox 6.1.
- ✓ Kali Linux 2.5.3.
- ✓ Windows 7 X64.
- ✓ Nmap.
- ✓ Metasploit Framework Data Base.

Evidencias de los pasos de un Pentesting aplicados a la actividad Unidad 2 – Etapa 3

- **Recopilación de información**

Esta etapa inicial tiene como objetivo hallar datos importantes sobre la aplicación o proceso activo Rejetto 2.3, donde según la información brindada en Anexo 4 – Escenario 3 desde una máquina que tiene Windows 7 con arquitectura X64 se está presentando una fuga de información sensible.

Sobre la aplicación mencionada se logra consultar la siguiente información importante, la cual puede ayudar a comprender el entorno de estudio actual:

Descripción[20]

La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (también conocido como HFS o HttpFileServer) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.

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

Impacto

Vector de acceso: A través de red.

Complejidad de Acceso: Baja.

Autenticación: No requerida para explotarla.

Tipo de impacto:

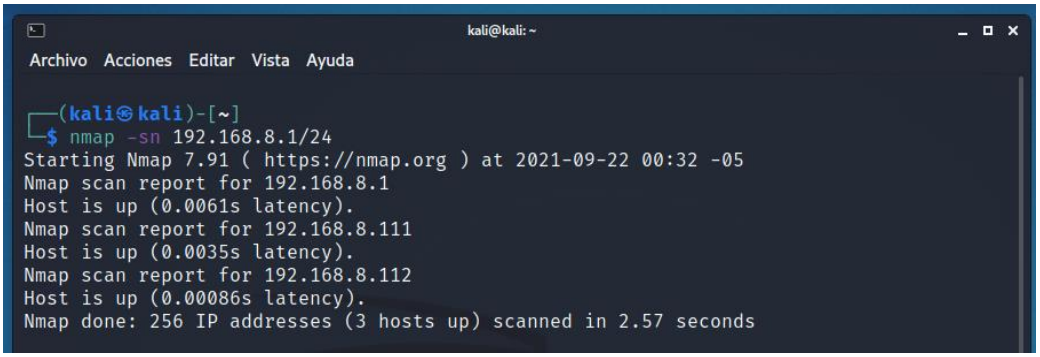
- ✓ Compromiso total de la integridad del sistema.
- ✓ Compromiso total de la confidencialidad del sistema.
- ✓ Compromiso total de la disponibilidad del sistema.

Herramienta para explotar vulnerabilidad

- ✓ Exploit a través de Metasploit framework.

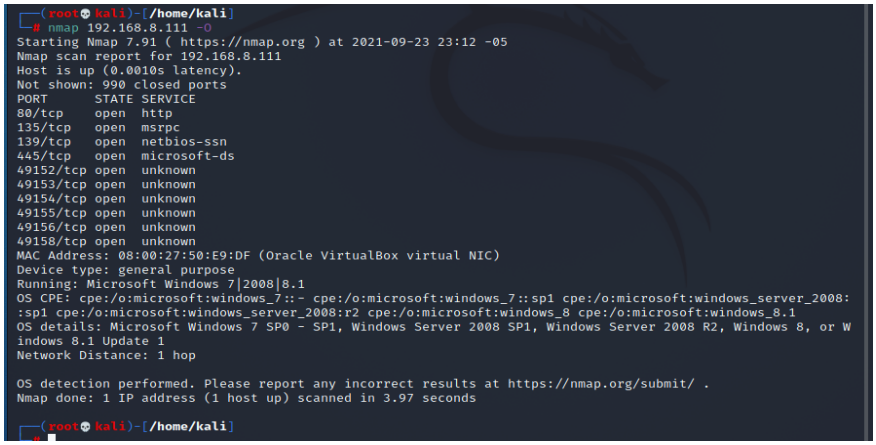
Adicionalmente se realiza un análisis con la herramienta Nmap sobre el segmento de red, donde se identifican los equipos que se encuentran activos en la misma y que sistema operativo ejecutan, esto a fin de conocer cual posee Windows 7 X64.

Figura 10. Ejecución de Nmap para buscar equipos activos en red



Fuente: Elaboración propia

Figura 11. Ejecución de Nmap para la identificación de información adicional como sistema operativo



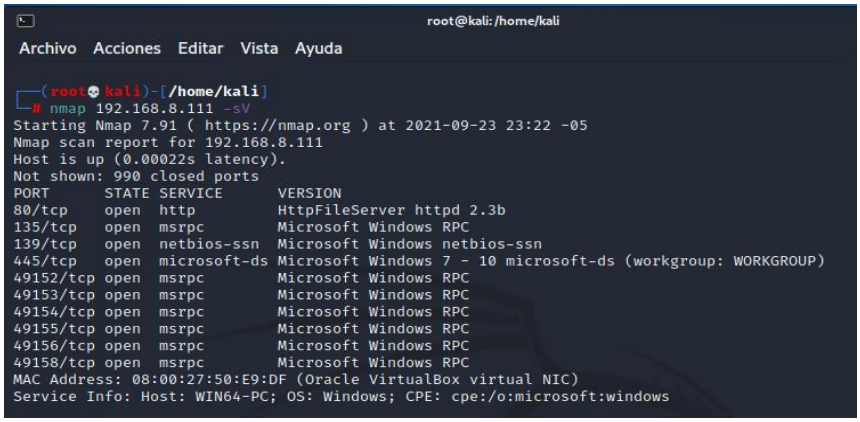
Fuente: Elaboración propia

- **Búsqueda de vulnerabilidades**.

En esta etapa se inicia con la búsqueda de las falencias que pueda tener el sistema que se quiere explotar, en esta búsqueda se pueden emplear ataques de fuerza bruta, denegación de servicio (DoS), entre otras técnicas.

Posteriormente se ejecuta un scaneo a fin de identificar vulnerabilidades que posee el equipo donde se reporta el fallo, específicamente en este caso se identifica el puerto 80 abierto con un HFS activo.

Figura 12. Ejecución de Nmap para identificar el estado de puertos y posibles vulnerabilidades



Fuente: Elaboración propia

Al identificar el HFS activo con puerto abierto, se realiza una búsqueda de las posibles herramientas de explotación a fin de proceder a la etapa de explotación de la vulnerabilidad.

Figura 13. Búsqueda de Exploit para HFS en Metasploit framework

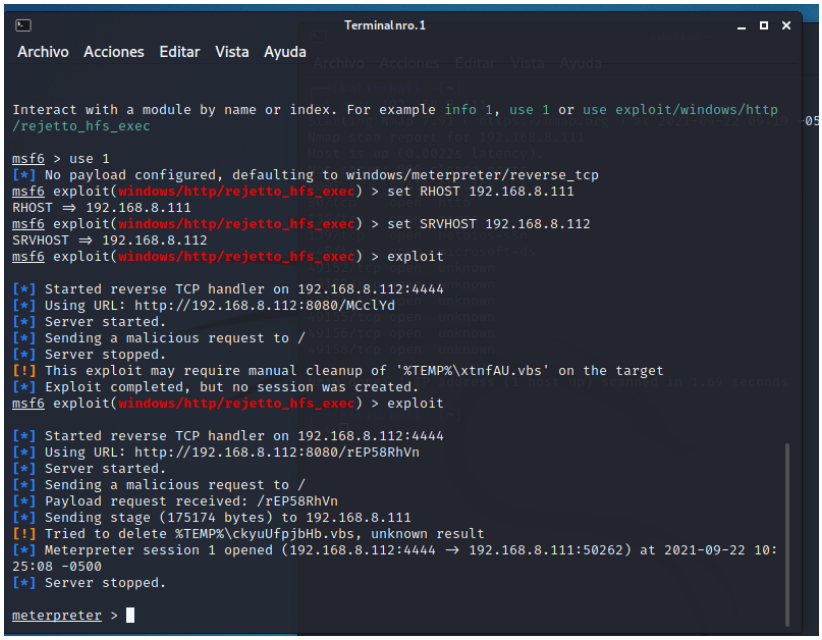
Fuente: Elaboración propia

- **Explotación de Vulnerabilidades**

En esta fase posterior a la detección de vulnerabilidades, se obtiene acceso al sistema por medio de diferentes métodos aplicados para la explotación, un ejemplo que podría mencionarse es la inyección de código SQL mediante herramientas como SQLmap o Metasploit, entre otras técnicas según sea el caso necesario para aplicar.

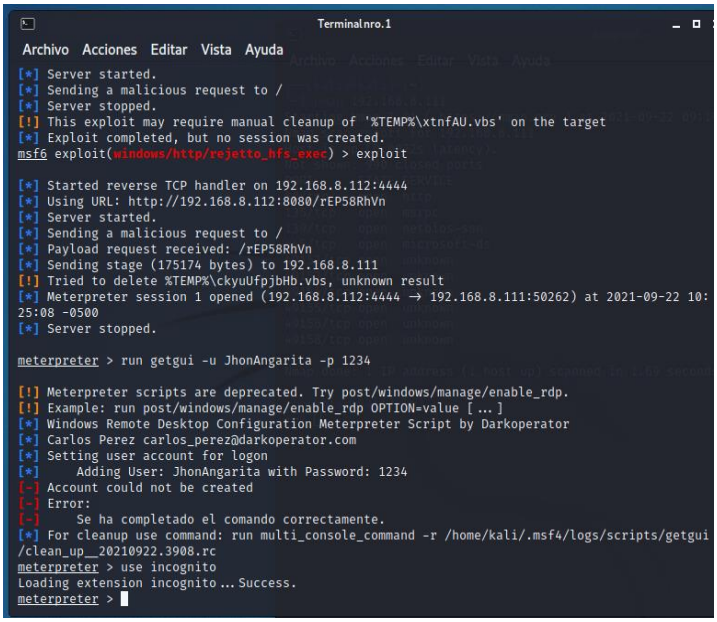
Para este caso particular se ejecuta el exploit rejetto_hfs_exec el cual logra explotar la vulnerabilidad, generando una shell reversa y una sesión abierta de meterpreter dando acceso al equipo remoto con Windows 7 x64, facilitando las acciones que se evidencian en las siguientes figuras adjuntas.

Figura 14. Carga del exploit reverse_tcp con IP destino y servidor con sesión meterpreter ejecutada



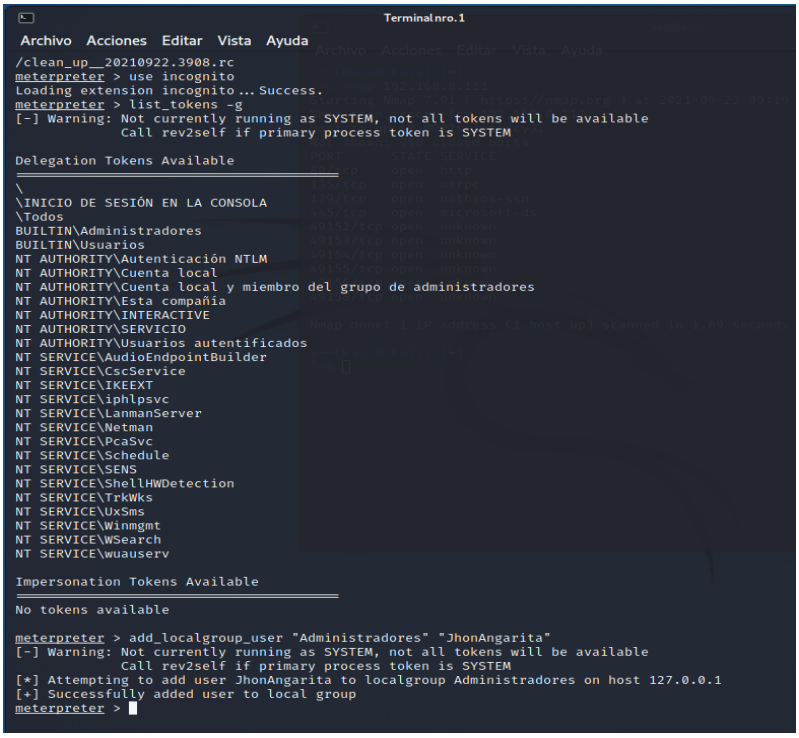
Fuente: Elaboración propia

Figura 15. Creación de usuario JhonAngarita en la sesión remota e inicio de la inclusión en el grupo de usuario administrador



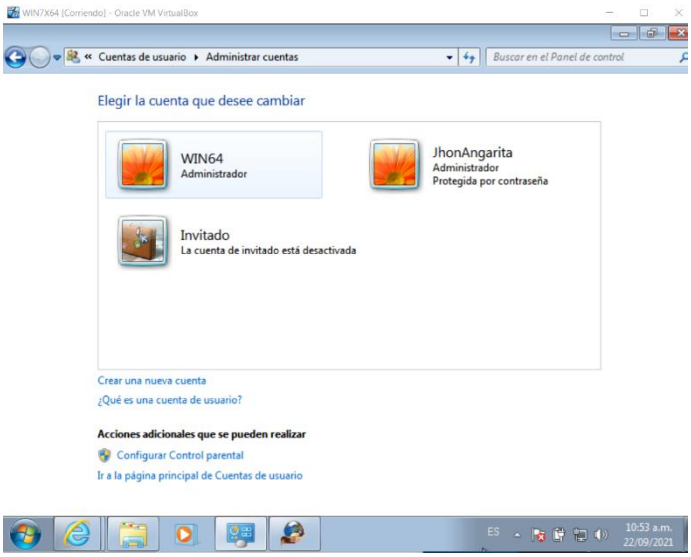
Fuente: Elaboración propia

Figura 16. Escalamiento de privilegios como usuario administrador



Fuente: Elaboración propia

Figura 17. Validación de usuario JhonAngarita como administrador en Windows 7



Fuente: Elaboración propia

10. DATOS E INFORMACIÓN QUE AYUDARON A IDENTIFICAR EL FALLO DE SEGURIDAD QUE ATACA LA MAQUINA WINDOWS 7 X64

Los datos importantes que se brindan en este anexo como ayuda a la identificación del fallo de seguridad fueron los siguientes:

- ✓ **Nombre de la aplicación o proceso activo**.

  Rejetto 2.3.

- ✓ **Sistema operativo y arquitectura de la máquina donde se ejecuta.**

  Windows 7 con arquitectura X64 Bits.

- ✓ **Tipo de herramienta maliciosa utilizada**.

  Exploit.

- ✓ **Vector de Acceso.**

  A través de recursos de Red.

- ✓ **Escalamiento de privilegios.**

  Tipo administrador del sistema.

11. HERRAMIENTA UTILIZADA PARA IDENTIFICAR LOS FALLOS DE SEGURIDAD Y PUERTO QUE ABRE LA APLICACIÓN

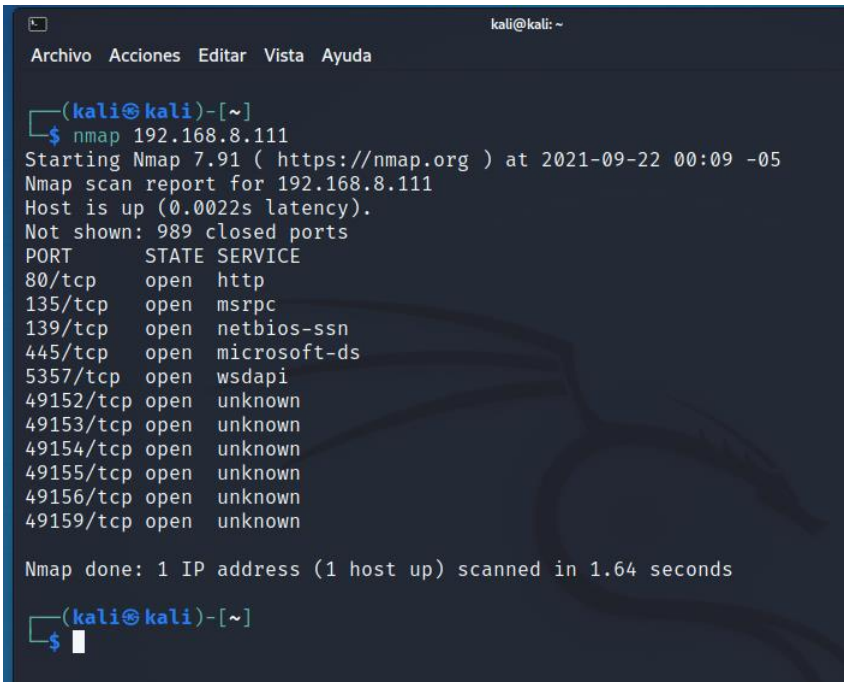
¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 7"?

La aplicación utilizada para la identificación es Nmap por medio del comando **nmap 192.168.8.111**, este se ejecuta sobre Kali Linux permitiendo realizar escaneo de redes y puertos, a fin de identificar servicios activos en los hosts, servidores, router, etc.

¿Qué puerto abre la aplicación específica en el anexo?

El puerto que se abre por medio de Rejetto 2.3 es el TCP 80 por tipo de servicio Http.

Figura 18. Ejecución de Nmap a host con Windows 7 en Kali Linux



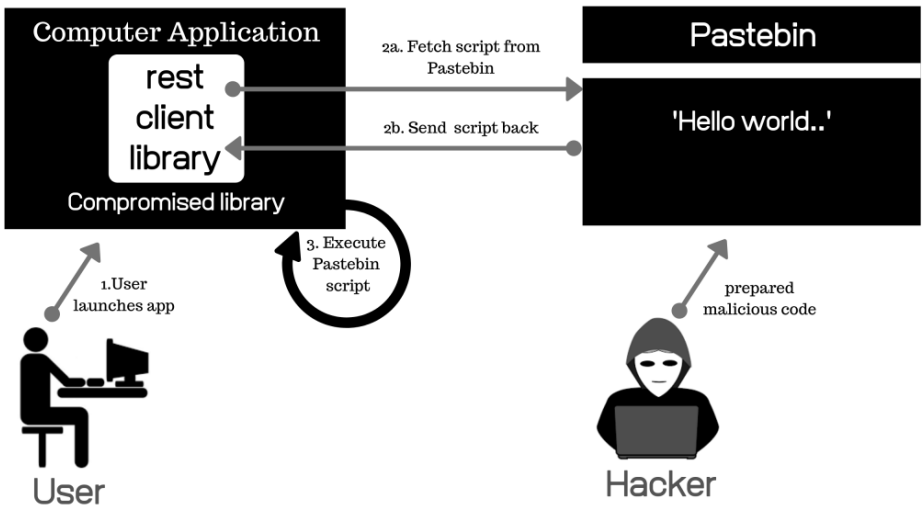
Fuente: Elaboración propia

12. CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64)

El ataque realizado hace provecho de la vulnerabilidad existente en Rejetto HTTP File Server 2.x, esta aprovecha una función llamada findMacroMarker de la biblioteca parserLib.pas de Windows, repercutiendo de manera directa en la toma de control de la maquina a través de una Shell remota dando como resultado la escala de privilegios como usuario administrador.

Este tipo de procedimiento usa como vector de ataque servicios de red, comprometiendo en alto porcentaje la integridad, confidencialidad y disponibilidad total del sistema.

Figura 19. Grafica de ejecución de ataque



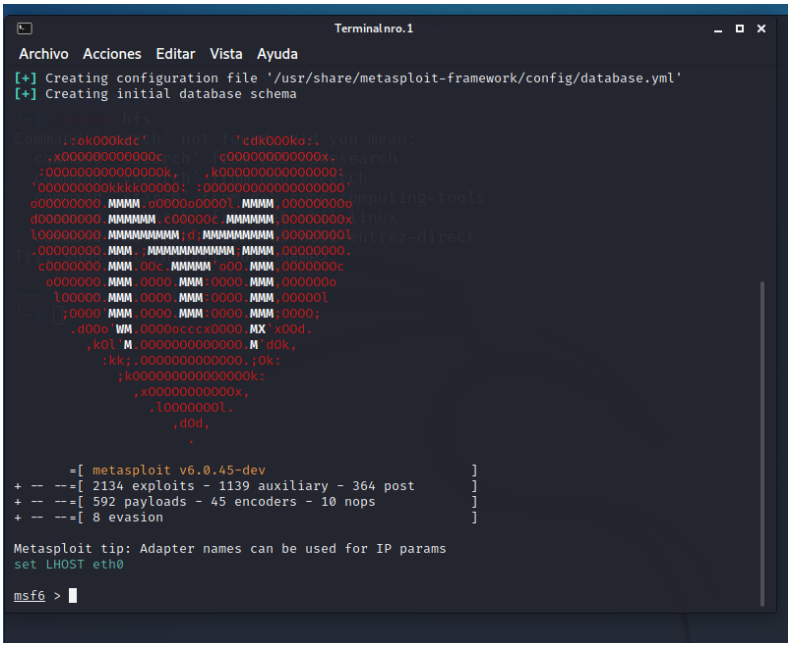
Fuente: Victoria[21]

[21] VICTORIA, C. (2019) Enfoque de vulnerabilidad: ataques de ejecución remota de código (RCE). Recuperado de https://blog.meterian.com/2019/08/27/vulnerability-focus-remote-code-execution-rce-attacks/

13. DOCUMENTACIÓN PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS 7

Como se tiene información inicial sobre un exploit que está explotando la vulnerabilidad, se remite a la herramienta de explotación de Metasploit framework.

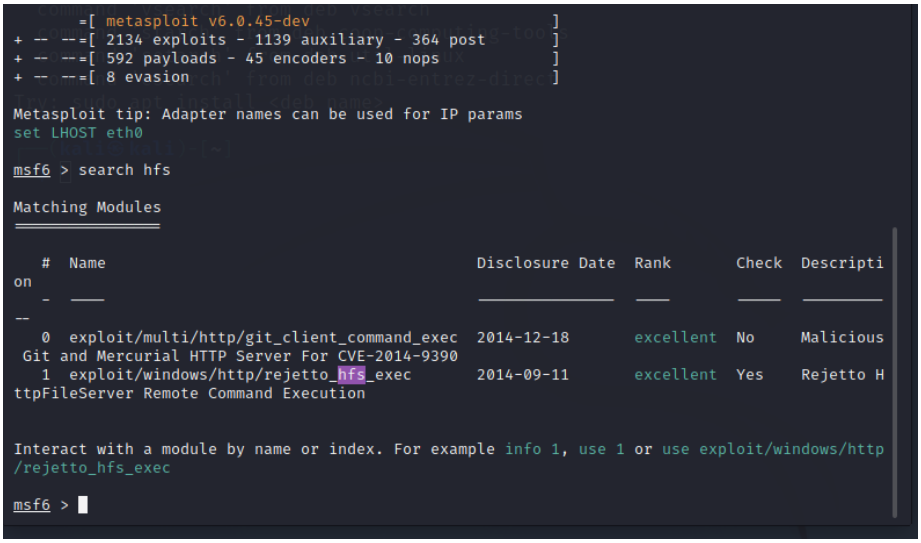
Figura 20. Ejecución Metasploit framework en herramientas de explotación



Fuente: Elaboración propia

De manera adicional se genera la búsqueda de exploits que tenga relación con hfs o rejetto, para posteriormente iniciar la ejecución del mismo.

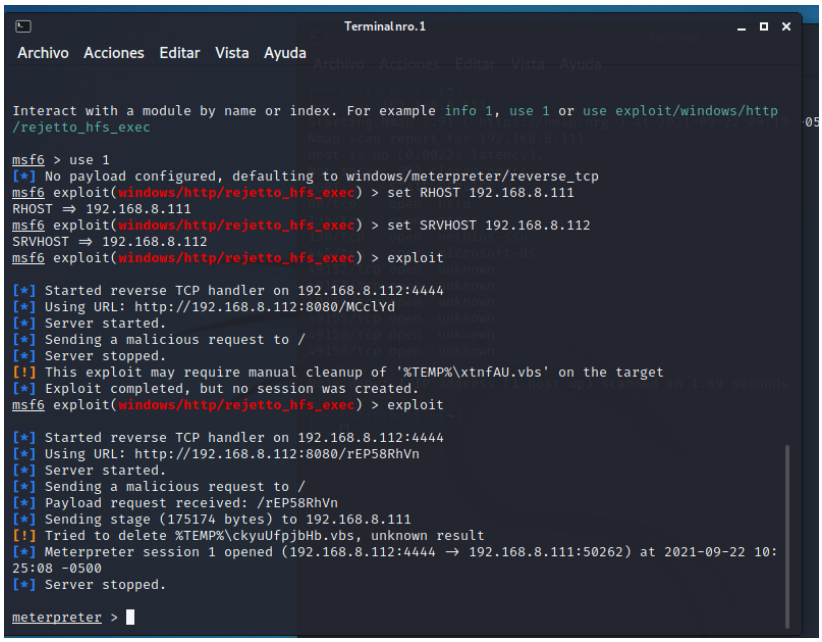
Figura 21. Búsqueda de Exploit para Hfs



Fuente: Elaboración propia

Posteriormente se ejecuta el exploit rejetto_hfs_exec, el cual realiza la explotación de manera efectiva y abre una sesión para poder realizar el escalamiento vía shell.

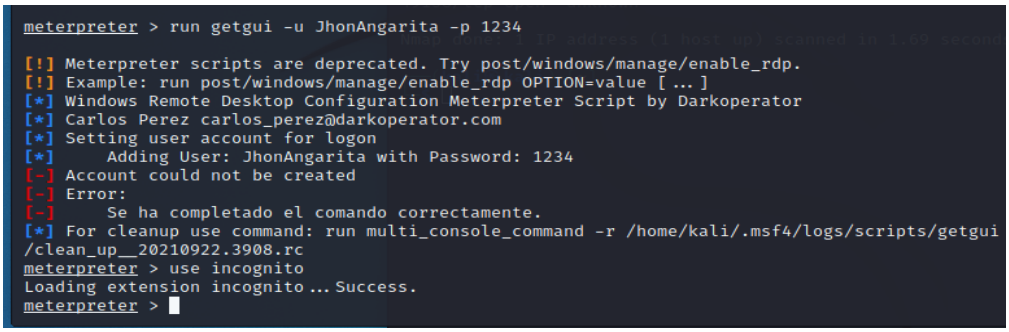
Figura 22. Carga del exploit reverse_tcp con IP destino y servidor con sesión meterpreter ejecutada



Fuente: Elaboración propia

Se procede a la creación del respectivo usuario a fin de generar el escalamiento de privilegios en el sistema.

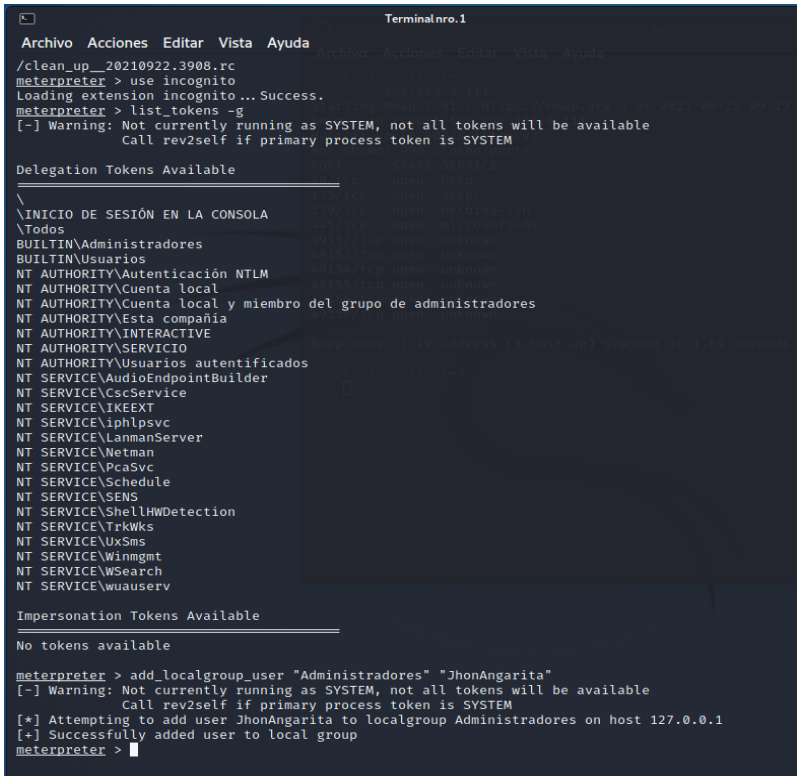
Figura 23. Creación del usuario JhonAngarita en la sesión remota e inicio de la inclusión en el grupo de usuario administrador



Fuente: Elaboración propia

Se incluye el usuario “JhonAngarita” en la escala o grupo de administradores del sistema.

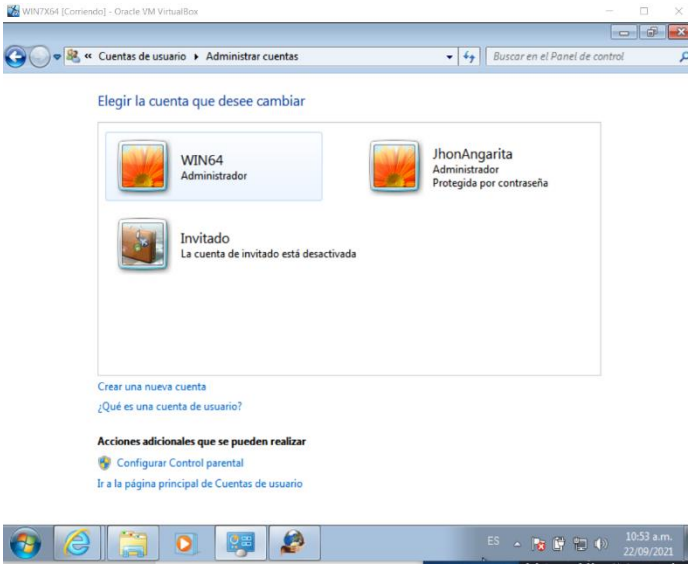
Figura 24. Se realiza escalamiento de privilegios como usuario administrador



Fuente: Elaboración propia

Se realiza la validación del ataque en la máquina virtual que tiene el sistema operativo windows 7 x 64, constatando que el ataque ha sido satisfactorio al validar que el usuario se encuentra creado y posee privilegios de administrador.

Figura 25. Se realiza validación de usuario JhonAngarita como administrador en Windows 7



Fuente: Elaboración propia

14. QUE HACER SI LLEGARA A ENCONTRAR UN ATAQUE EN TIEMPO REAL

Al enfrentar un ataque informático se debe tener una base de conocimientos sólida como profesionales, ya que de esto depende la pronta contingencia que se le dé al caso y ante todo la pronta solución al mismo.

Cabe resaltar que es vital actuar con prontitud, ya que al pasar el tiempo se puede ampliar el daño informático ocasionado, afectando la integridad, confidencialidad y disponibilidad del sistema atacado.

Ante estas circunstancias y lo planteado en el anexo, se podría entrar a indagar lo que se menciona a continuación:

- Analizar de donde proviene el ataque, es decir, si es desde la LAN o WAN, ya que con eso se puede tomar decisiones a lo que se va a realizar para contenerlo.

- Identificar la dirección IP interna o externa desde donde se está realizando e incluirla en las reglas de denegación de conexión del firewall, esto con el fin de evidenciar si persiste el ataque desde otra ubicación.

- Recurrir a herramientas de análisis de trafico de red para visualizar con claridad la información o paquetes que transitan por la misma.

- Desconectar el equipo de la red e indagar si está haciendo bots autónomos o automáticos.

- Activar el firewall de Windows o del antivirus que se esté usando para proteger el equipo o la red atacada y validar si se presentan anomalías.

- Si se posee infraestructura TI robusta contraatacar la dirección IP de origen por métodos que ayuden a colapsar esta ruta de datos.

- Actualizar o parchar el equipo atacado a nivel de seguridad del sistema operativo para ver si se detiene el mismo.

- Aplicar políticas de autenticación con umbrales de seguridad, entre estos se puede encontrar umbral de bloqueo de cuenta, tiempo de reactivación. Como también directivas de seguridad para el uso de contraseñas robustas, aumentando así el nivel de seguridad.

- Luego de controlar el ataque realizar la implementación de IDS, IPS, SIEM o cualquier tipo de mecanismo de defensa para aumentar los niveles de seguridad y tratar de mitigar en alto porcentaje el riesgo actual.

15. MEDIDAS DE HARDENIZACIÓN PROPUESTAS PARA QUE NO SE REPITA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM

Actualmente es de vital importancia mantener altos los niveles de seguridad de los equipos de cómputo que se tienen en las empresas, ya que de esto depende en alto porcentaje el flujo de producción de los negocios.

Teniendo en cuenta lo aplicado desde el ejercicio de Redteam se puede proponer o reforzar las siguientes medidas de seguridad (hardening) que se mencionan a continuación:

- Actualizar el sistema operativo con las versiones más recientes a nivel de seguridad.

- Activar el firewall con políticas de preferencia por parte del personal TI, para proteger las conexiones que se envían o reciben sobre la red en la cual se está operando.

- Asignar controles de usuarios por medio de directivas de seguridad local.

- Activar cuentas diferentes a la del administrador, de esta manera se restringen las modificaciones directas al sistema operativo.

- Monitorear la red por medio de herramientas que sean aliadas para los administradores de infraestructura, en las que se puede encontrar (PRTG, Pandora FMS, etc.).

- Utilizar listas de control de acceso (ACL) en los dispositivos activos, para evitar la intrusión de dispositivos no autorizados en la red.

- Crear Vlan en la red de la compañía, esto con el fin de aislar o dividir las dependencias y así evitar que al atacar un equipo se tenga acceso a la red por completo.

- Usar directorios activos con el fin de asignar permisos escalables o con restricciones, esto con el ánimo de controlar el acceso a recursos de red, entre otros.

- Implementar el cifrado de información en los sistemas operativos como barrera de protección ante el robo de información confidencial.

- Sugerir el uso de VPN para las conexiones de equipos fuera de la LAN de la compañía.

- Establecer contraseñas robustas, que tengan caducidad en el tiempo y con umbrales de inicio de sesión.

- Gestionar el uso de certificados de seguridad en las comunicaciones como HTTP, SMTP, POP, entre otros.

- Escanear las direcciones IP de forma automatizada constantemente, esto con el fin de estar alerta ante alteraciones no autorizadas en los equipos de cómputo de la organización.

- Restringir o inhabilitar el uso de servicios innecesarios sobre los cuales no se vayan a ejecutar procesos, evitando backdoor en los equipos o sistemas operativos en producción

16. DESCRIPCIÓN DE LAS DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

Un equipo Blue Team es aquel que tiene como misión principal realizar la defensa de manera proactiva en la compañía ante ataques informáticos, brindando soluciones ante los eventos que se puedan presentar, entre las funciones esenciales de un Blue Team se pueden mencionar algunas de mayor relevancia como lo son:

- Monitoreo constante de patrones o actos que se encuentren fuera del uso tradicional del sistema o aplicaciones.
- Análisis de los sistemas y aplicativos pertenecientes a la infraestructura de tecnología de la organización.
- Identificación de fallos o vulnerabilidades con el fin de verificar la eficiencia de las medidas de seguridad aplicadas.
- Recomendación de planes para actuar en la mitigación de los riesgos.
- Establecimiento de medidas para futuros caso as detectar[22].

Mientras que el equipo de respuesta frente a Incidencias de Seguridad **Informática** (CSIRT) es quien está atento a hechos reales o sospechosos que puedan terminar siendo una vulnerabilidad, dentro de sus funciones se puede mencionar:

- Detección de alteraciones no autorizadas de software y hardware.
- Ejecución de tiempos de respuesta eficientes para disminuir daños o afectaciones.
- Identificación y clasificación de los tipos de ataques.
- Desarrollo de planes de continuidad, prevención y recuperación ante desastres.

Según lo que se menciona anteriormente, queda claro que ambos hacen parte o cumplen con un rol importante en la mitigación de riesgos informáticos, ofreciendo mejores niveles de seguridad y garantizando en alto porcentaje la disponibilidad de la infraestructura tecnológica de las empresas[23].

[22] UNIR. (2020). Red Team, Blue y Purple Team, ¿cuáles son sus funciones y diferencias?. Recuperado de: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[23] CESICAT. Equipo de Respuesta a Incidentes. Recuperado de: https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf

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

Actualmente usaría CIS (center for internet security) para aplicar el conjunto de controles que tiene incluidos y así se puedan orientar a la seguridad critica de la organización. Estos por su parte, serian de gran ayuda en el mejoramiento de las políticas de seguridad.

Adicionalmente se podría optar por ejecutar o aplicar según se necesite la clasificación de los controles que se mencionan a continuación:

- Controles de CIS básicos: Estos son controles de seguridad de uso general que cada organización debe implementar para garantizar la disponibilidad de una defensa informática esencial.

- Controles de CIS fundamentales: Estos son controles que las organizaciones deben implementar para contrarrestar amenazas técnicas más específicas.

- Controles de CIS organizacionales: Estos controles están menos enfocados en aspectos técnicos y más enfocados en las personas y los procesos involucrados con la seguridad informática. La organización debe implementar estas prácticas clave internamente para garantizar la madurez de la seguridad a largo plazo.

Estas herramientas podrían ser muy importantes, ya que contribuyen a:

- Prevenir los ataques de alto impacto o de mayor alcance.

- Desarrollar un gran escudo de seguridad cibernética enfocado al hardening en los activos de la organización.

- Seguir un enfoque validado de gestión de riesgos, basándose en la aplicación de los mismo al mundo real.

- Aplicar el conjunto de técnicas más efectivas que estén disponibles con la intensión especifica de mejorar la protección de los activos de la empresa[24].

[24] CIS. (2021). Controles CIS versión 8. Recuperado de: https://www.cisecurity.org/controls/v8/

18. FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM

Los sistemas SIEM han logrado escalar como una de las mejores opciones para que las organizaciones puedan enfrentar de forma inmediata cualquier incidente o amenaza para la seguridad de sus sistemas informáticos.

Se define como SIEM (gestor de información y eventos de seguridad) al conjunto de software que ofrece datos detallados e importantes a las organizaciones o administradores de infraestructura informática, con la intensión de identificar vulnerabilidades a las que pueden estar expuestos actualmente.

Funciones Principales.

- Detectar fallos generales de seguridad.
- Rastrear amenazas de seguridad.
- Identificar ataques o vulnerabilidades activas en tiempo real.

Características Principales.

- Usar un sistema de datos estandarizado para enfrentar los riesgos informáticos.
- Ayudar a mejorar la seguridad de las compañías.
- Dar a conocer una perspectiva general de la protección actual de las empresas.
- Generar informes basados en la recopilación de datos inicial.
- Reconocer patrones de ataque informático por medio de repositorios con el fin de mitigar con efectividad las amenazas presentes.
- Notificar en tiempo real lo que está sucediendo en los activos tecnológicos.
- Establecer patrones de conducta para evitar accesos futuros.
- Disminuir el trabajo del personal de IT.
- Responder con rapidez y eficacia a soluciones que se necesiten con urgencia.

- Documentar todo el proceso de detección, actuación y resolución de incidentes[25].

[25] PEDROZA, J. (2016). Implementación de un Gestor de Seguridad de la Información y Gestión de Eventos (SIEM). Recuperado de: http://bibliotecadigital.usb.edu.co/bitstream/10819/3944/1/Implementacion_Gestor_Seguridad_Pedroza_2016.pdf

19. HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS "HARDWARE O SOFTWARE"

Para la contención de ataques de manera eficiente y autónoma se hace uso de herramientas basadas en hardware y software, estas ayudan en la ejecución rápida ante contingencias que se puedan enfrentar en ataques a nivel de red o físicas. A continuación, se mencionan algunos importantes en el sector de seguridad de la información.

- Los Firewall de FortiGate inspeccionan el tráfico a hiperescala a medida que entra y sale de la red. Estas inspecciones ocurren a una velocidad, escala y rendimiento incomparables para garantizar que solo se permita el tráfico legítimo, todo esto sin degradar la experiencia del usuario ni crear tiempos de inactividad costosos[26].

- IBM QRadar SIEM ayuda a los equipos de seguridad a detectar amenazas con precisión y darle prioridad a las mismas. Este puede correlacionar diferentes datos y agregar eventos relacionados en una sola alarma para un rápido análisis y prevención de incidentes. También puede generar alertas de prioridad junto con el progreso del ataque en la cadena de eliminación. Esta solución está disponible en la nube (entornos IaaS y SaaS) y en entorno local.

- McAfee Enterprise Security Manager es una herramienta SIEM de la prestigiosa empresa de seguridad McAfee permite monitorizar los sistemas para poder recopilar, analizar y comparar incidentes de seguridad con una gran base de datos de registros, y así poder detectar amenazas de forma inteligente[27].

[26] FORTINET. (2020). Next-Generation Firewall de FortiGate. Recuperado de: https://www.fortinet.com/lat/products/next-generation-firewall

[27] AMBIT. (2021). ¿Qué significa SIEM y cómo funciona?. Recuperado de: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

CONCLUSIONES

Por medio de la ley 1273 de 2009 y la 1581 de 2012 se le da vital importancia a la confidencialidad de la información, castigando con penas ejemplares a quien abuse accediendo a sistemas informáticos o divulgando datos de terceros sin previo consentimiento de parte de quien tiene derechos por norma sobre los mismos.

Se analiza la importancia del código de ética para profesionales de ingeniería, los cuales dan una pauta clara sobre las responsabilidades y recomendaciones a tener en cuenta en el desarrollo de la vida profesional o laboral.

Se presenta un reporte de ejecución de pentesting para dar a conocer las falencias y vulnerabilidades que pueda poseer Red Team de igual forma se da a conocer las herramientas para realizar los ataques informáticos más comunes y a su vez información de sitios web donde se centralizan los errores comunes a nivel de seguridad de sistemas informáticos.

Al encontrar la vulnerabilidad y explotarla respectivamente, se logra evidenciar las falencias que pueden aprovechar los equipos Red Team, comprometiendo así la confidencialidad, integridad y disponibilidad de la información en las organizaciones que no poseen buenas prácticas al proteger su infraestructura tecnológica.

Al presentarse un ataque en tiempo real se debe realizar acciones de inmediato como el análisis del ataque, identificación de la IP, analizar el tráfico, activar el firewall, aplicar las políticas de autenticación con umbrales de seguridad, parchar el equipo atacado para controlar el ataque y poder implementar IDS, IPS, SIEM o cualquier tipo de mecanismo de defensa que impida que se realice el ataque nuevamente.

Las empresas deben mantener niveles altos de seguridad en cuanto a contar con el sistema operativo actualizado, activar el firewall, asignar controles de usuarios con permisos escalables, monitorear la red, utilizar ACL, VPN y VLAN, implementar cifrado de la información, utilizar contraseñas robustas y certificados de seguridad en las comunicaciones y restringir los servicios innecesarios.

RECOMENDACIONES

Según la información profundizada mediante el desarrollo de las actividades incluidas en los anexos, se evidencian fallas a nivel general, es decir, en el aspecto legal, ético, de ataque y mitigación de factores de riesgo informático, teniendo en cuenta lo anterior y con el objetivo de mejorar los procesos se realizan las siguientes recomendaciones:

- Mejorar los procesos de contratación basados en la efectiva aplicación de las leyes o normas actuales vigentes, aclarando los términos y condiciones de quienes se postulen a nuevos cargos en la organización.

- Incentivar a los empleados de la entidad para que apliquen de manera correcta su ética profesional, del comportamiento de estos depende en gran medida el desarrollo adecuado de los procesos que se ejecutan, evitando así posibles conflictos a nivel legal según su comportamiento aplicado.

- Capacitar a los integrantes de la empresa en la ejecución de buenas prácticas de seguridad informática, ya que estos son un eslabón fundamental para ayudar a proteger los activos informáticos de la misma.

- Fortalecer los niveles de seguridad que se tienen actualmente, ya que han desencadenado en problemas de confidencialidad para la información de la empresa. Por medio de estos se puede lograr la conservación de su integridad y disponibilidad.

- Invertir en la implementación de dispositivos de hardware o software que logre hacer robusta la infraestructura tecnológica, entre los que se pueden mencionar FIREWALL, IDS, IPS, SIEM, entre otros.

- Implementar la ejecución de herramientas para el monitoreo en tiempo real de las actividades que ocurren en los sistemas informáticos de la empresa, con esta práctica se puede lograr la mitigación de problemas de ciberseguridad.

BIBLIOGRAFÍA

AMBIT. (2021). ¿Qué significa SIEM y cómo funciona?. Recuperado de: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

ALVEAR REINOSO, Francisco Xavier. (2019). Análisis y diseño de una propuesta para mitigar ataques cibernéticos a correos electrónicos utilizando técnicas de Hacking Ético. Recuperado de: https://dspace.ups.edu.ec/bitstream/123456789/17035/1/UPS-ST004012.pdf

CATORIA, Fernando. (2013) Pruebas de Penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. Recuperado de https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetración-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

CESICAT. Equipo de Respuesta a Incidentes. Recuperado de: https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf

CIS. (2021). Controles CIS versión 8. Recuperado de: https://www.cisecurity.org/controls/v8/

COPNIA. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Recuperado de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

CORLETTI ESTRADA, Alejandro. (2017). Ciberseguridad Una Estrategia Informático Militar. Recuperado de: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/Libro-Ciberseguridad_A.Corletti_nov2017.pd.pdf

CSRC. Computer Security Resource Center. Recuperado de: https://csrc.nist.gov/glossary/term/blue_team

CSRC. Computer Security Resource Center. Recuperado de: https://csrc.nist.gov/glossary/term/red_team
CVE. (2021). Catalogar las Vulnerabilidad de Seguridad. Recuperado de https://cve.mitre.org/

El TIEMPO. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. Enero 23 de 2015. (Recuperado el 7 de septiembre de 2021) Disponible en https://www.eltiempo.com/archivo/documento/CMS-15141236

FORCEPOINT. (2021). CYBER EDU, What is a Firewall?. Recuperado de: https://www.forcepoint.com/es/cyber-edu/firewall

FORTINET. (2020). Next-Generation Firewall de FortiGate. Recuperado de: https://www.fortinet.com/lat/products/next-generation-firewall

IBERDROLA. (2021). Ataques cibernéticos: ¿Cuáles son los principals y cómo protegerse de ellos? Recuperado de: https://www.iberdrola.com/innovacion/ciberataques

IMSALUD. (2019). ABC Ley 1581 de 2012 Protección de Datos Personales. Recuperado de https://www.imsalud.gov.co/web/sin-categoria/abc-ley-1581-de-2012-proteccion-de-datos-personales/

INCIBE-CERT. (2014) Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287). Recuperado de https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

McAfee. (2021). What Is Security Information And Event Management (SIEM)?. Recuperado de: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-siem.html

NMAP.ORG. Nat Security Scanner. Recuperado de https://nmap.org/

OFFEBSIVE SECURITY. (2021). Explotar la Base de Datos por seguridad ofensiva. Recuperado de https://www.exploit-db.com/

OPENVAS BY GREENBONE. Open Vulnerability Assessment Scanner. Recuperado de https://www.openvas.org/

PEDROZA, J. (2016). Implementación de un Gestor de Seguridad de la Información y Gestión de Eventos (SIEM). Recuperado de: http://bibliotecadigital.usb.edu.co/bitstream/10819/3944/1/Implementacion_Gestor_Seguridad_Pedroza_2016.pdf

PEÑARREDONDA, José Luis. Detrás de Buggly: la historia de la fachada Andrómeda. Diciembre 9 de 2015. Revista Enter.co. (Recuperado el 8 de septiembre de 2021). Disponible en https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

POLICÍA NACIONAL. (2021). Normatividad sobre delitos informáticos. Ley 1273 de 2009. Recuperado de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

PORUP, JM. (2019). What is Metasploit? And how to use this popular hacking tool. Recuperado de: https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html

RAPID 7 METASPLOIT. El marco de pruebas de penetración más utilizado del mundo. Recuperado de https://www.metasploit.com/

UNIR. (2020). Red Team, Blue y Purple Team, ¿cuáles son sus funciones y diferencias?. Recuperado de: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

VICTORIA, C. (2019) Enfoque de vulnerabilidad: ataques de ejecución remota de código (RCE). Recuperado de https://blog.meterian.com/2019/08/27/vulnerability-focus-remote-code-execution-rce-attacks/

VIDEO PRESENTACIÓN INFORME TÉCNICO FINAL

https://youtu.be/mUHcR2MZfi4