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

JAIRO ORLANDO ACEVEDO JIMENEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

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

JAIRO ORLANDO ACEVEDO JIMENEZ

Tutor:
Jhon Freddy Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Ataque: Es el intento de acceder de forma abusiva e ilegal a un dispositivo informático usando recursos como virus, malware con el fin de alterar su funcionamiento.

Blue Team: Equipo de seguridad defensiva que defiende las empresas de ataques de una manera proactiva.

CVE: Una plataforma en línea muy conocida en el mundo de la ciberseguridad, ya que proporciona un listado casi ilimitado de vulnerabilidades que han sido detectadas por diferentes entidades y hackers éticos sin fines de lucro y que ponen en conocimiento público con el objetivo de prevenir que sean explotadas.

DMZ: La función de una DMZ es permitir las conexiones tanto desde la red interna como de la externa, mientras que las conexiones que parten de la DMZ solo puedan salir a la red interna; así, los equipos locales (hosts, en argot de redes) jamás podrían conectarse a la red interna.

ExploitDB: Es una base de datos web donde es almacenado un repositorio de exploits gratuitos para realizar prácticas de laboratorio o como pruebas de penetración sobre vulnerabilidades encontradas.

Hacker: Un hacker puede ser una persona que actúa con ética ya que se encarga de la búsqueda de vulnerabilidades en un ambiente informático para así tomar las debidas correcciones que minimicen estas fallas.

Metasploit: A través de esta herramienta que se conoce tanto a nivel de seguridad como de los criminales informáticos para detectar y auditar las vulnerabilidades de un sistema, todo a través de comandos cortos y de funciones ya grabadas.

Nmap: Es una herramienta open source y de código abierto que nos permite escanear y rastrear el estado de los puertos de una red entera o de una dirección IP especifica.

OpenVas: Esta herramienta open source y de software libre bajo la licencia GNU. Al igual que Nessus este se compone de herramientas que ayudan identificar vulnerabilidades por medio de escaneo de seguridad de red, contiene una interfaz gráfica de usuario e integra aplicaciones de seguridad.

Pirata Informático: Es muy generalizado ya que no solo abarca los datos e información, sino que afecta a varios sectores ya sea por el robo de propiedad intelectual e incluso puede darse en la usurpación de personal de una empresa.

Red Team: Emulan a un atacante real haciendo uso de herramientas reales o similares a la de un atacante para explotar vulnerabilidades usando seguridad ofensiva

Seguridad Defensiva: Es la encargada de proteger una organización de cualquier amenaza a nivel de ciberseguridad y los recursos informáticos.

Seguridad Ofensiva: Conjunto de herramientas o soluciones que permiten revisar el estado de vulnerabilidad de un recurso informático

Vulnerabilidad: Es la debilidad que presenta un sistema informático que puede poner en un posible riesgo de seguridad al sistema

INTRODUCCIÓN

En un mundo digital donde todos tenemos perfiles digitales que nos ayudan a interactuar con el mundo desde nuestro hogar, oficina, estudio, etc. Sin embargo, esta información es cada vez más apetecible para los delincuentes informáticos que cada día avanzan en la forma de cómo acceder a esta información para poder venderla al mejor postor o quien demuestre un interés en esta. Es por esto que es necesario conocer que es lo que los delincuentes buscan en sus víctimas para así establecer que protección se puede dar para reducir el riesgo de que podamos ser víctimas potenciales de este flagelo. Para poder reconocer estos factores, es necesario saber de casos que ha sucedido y que han sido mostrados en los medios nacionales para así lograr identificar qué es lo que estos delincuentes buscan al acceder ilícitamente a la información de las víctimas y así poder reconstruir un perfil criminal para poder reconocer factores de riesgo en caso de posibles ataques a nuestra información. Basándonos también en las leyes que tenemos al alcance para así reconocer como la misma ley puede protegernos y lograr judicializar a uno de estos delincuentes.

Lo que se busca con este informe es demostrar la importancia de tener una protección de datos de amenazas externas potenciales aplicando técnicas de ethical hacking como lo es el uso de equipos de seguridad basados en el esquema de Red Team y Blue Team. Para eso se plantean unos escenarios en los cuales se debe analizar el método de funcionamiento que tienen estos equipos que, de forma separada, pero con el mismo objetivo el de hallar, identificar, mitigar y fortalecer los puntos débiles que en materia de ciberseguridad, seguridad de la información y seguridad informática pueda tener una empresa. Es por eso que en este informe se muestra la importancia que ha tomado actualmente el plantear estas estrategias en las empresas para proteger y salvaguardar la información y los datos en todos sus formatos tanto físicos como digitales que cada vez, es más utilizado en el mundo moderno.

1 PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Las empresas de hoy en día están volcando sus servicios al uso de la tecnología. Sin embargo, la importancia que se le da a la seguridad de estos recursos en algunos casos es muy poca o ninguna.

Para lograr identificar cada riesgo, amenaza y/o vulnerabilidad, las empresas deben tener un modelo de administración segura que vaya enfocado a los lineamientos culturales y objetivos del negocio de acuerdo con su modelo de negocio. Y que a la vez se apoye con la parte técnica que permita ver que amenazas se concentran sobre esos activos informáticos que cada vez toman mucha más importancia en los negocios de ahora. Es por esto que en este informe se pretende plasmar como en cada uno de los escenarios propuestos, utilizando técnicas de ethical hacking apoyados por herramientas de uso libre conocidas como opensource se va dando solución a los problemas planteados en dichos escenarios actuando sobre los marcos legales y éticos que un especialista de seguridad informática debe tener para ejercer esta labor de gran importancia y de mucha complejidad que va cambiando y evolucionado cada día ya que los criminales cada vez encuentran nuevas formas de intentar acceder de forma abusiva e ilegal a la información privada de las personas y las empresas.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo aspirante al puesto que ofrece WhiteHouse, tendré las capacidades técnicas, éticas y legales que WhiteHouse está buscando?

1.3 DESCRIPCIÓN

WhiteHouse requiere conocer por medio de unos escenarios propuestos basados en experiencias que han tenido con su información, lograr identificar las capacidades de los aspirantes para el cargo vacante, teniendo en cuenta las capacidades técnicas y éticas de cada uno en la resolución de cada escenario a través de preguntas y ejercicios prácticos con ambientes reales de ataques y vulnerabilidades que se encuentran en una empresa que quiere diagnosticar, identificar y mitigar o eliminar cualquier amenaza que se cierne sobre su información.

2 JUSTIFICACIÓN

Al igual que las personas que realizan estos ataques con fines delictivos, también hay personas que lo hacen con el fin de proveer a las empresas las soluciones que permitan mitigar el riesgo de ser víctimas de estos ataques. Cada día sale a la luz vulnerabilidades que pueden afectar a los sistemas de una empresa o en general a cualquier sistema, por lo cual se hace necesario entender que los riesgos que desencadenen deben ser mitigados en el menor tiempo posible y elevar el nivel de seguridad como en el caso que se plantea en este informe.

El análisis de vulnerabilidades se justifica en la constante amenaza que se cierne en torno a estos recursos informáticos a nivel de empresas. La información siempre estará expuesta a cualquier tipo de ataque por lo cual siempre habrá un mayor riesgo de seguridad en esta y nunca habrá los controles de seguridad suficientes, y en algunos casos los controles de seguridad no son aplicados por las empresas de la mejor manera. Esto es aprovechado por personas externas o en ocasiones internas a la empresa para poder atentar en contra de las políticas de seguridad tanto a nivel físico como a nivel lógico de la misma. De ahí la necesidad de que una empresa cuente con los recursos necesarios para responder a estos ataques y establecer métodos de seguridad que mitiguen las fallas de seguridad y se fortalezca la seguridad.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar los escenarios propuestos desarrollando habilidades como especialista en Pentesting y aplicarlas bajo la estrategia de Red Team y Blue Team.

3.2 OBJETIVOS ESPECIFICOS

- Analizar las herramientas Opensource que existen para encontrar vulnerabilidades y así poder realizar un pentesting
- Conocer el manejo de los delitos informáticos en la legislación colombiana
- Diferenciar entre un Blue Team, un CSIRT y un Red Team
- Entender las implicaciones éticas y legales sobre un caso de la vida real

4 MARCO TEÓRICO

4.1 SEGURIDAD INFORMATICA

La vida actual ha llevado que cada vez dependamos de la tecnología para múltiples cosas de la vida, tanto para comunicarnos con otras personas a largas distancias o para realizar nuestras labores más rápido. Esto sin contar el tiempo que pasamos conectados a la gran red que es internet, tanto correos electrónicos como transacciones en línea se ha vuelto muy cotidiano para todos en las últimas décadas. Las organizaciones cada vez más han delegado actividades de vital importancia para el negocio a los sistemas y redes informáticas como lo pueden ser los servicios financieros, controles de la producción etc. Sin embargo, esta expansión digital ha dejado que su información sensible se vea cada vez más amenazada por el hecho de estar visibles en la red mundial, de ahí la importancia de que esta información este lo más segura posible en caso de algún intento de sustraerla. La seguridad de la información se basa en impedir que se ejecuten operaciones no autorizadas dentro del sistema, que pueden llegar a comprometer la información de una organización tanto en su confidencialidad, su integridad y su autenticidad.[1]

La seguridad de la información la define la norma ISO 17799 como la actividad de preservar los pilares de la información que son confidencialidad, la integridad y/o la disponibilidad. De la información que maneje la organización dependerá el nivel de seguridad que se implemente al sistema el cual garantice que los pilares de la información se cumplan.[2]

La seguridad informática por su parte es la encargada de encontrar los mecanismos de control y las medidas que aseguren que los sistemas de información de una organización tendrán confidencialidad, integridad y estará siempre disponible, tanto para el hardware, software y toda información que almacenen, procesan y comunican.

En este punto una organización debe comprender que la seguridad de la información depende de muchos factores entre los que se destacan:

- La parte directiva deberá tomar conciencia de que esta función es importante y por lo cual se debe destinar recursos considerables a esta razón.

[1] GÓMEZ, VIEITES. Álvaro. Seguridad en equipos informáticos. España: RA-MA, 2000. 165p.
[2] Ibid., p. 16.

- Los responsables de los sistemas informáticos deben ser personal capacitado, con conocimientos y dominio de la tecnología que se maneje, además de conocer de las posibles amenazas y ataques que pueden recibir.

- La capacitación de todos los usuarios, sus responsabilidades y el rol que desempeñan en la seguridad de la información.

- La instalación, configuración y mantenimiento de los equipos sea de la manera correcta.

- Todo lo concerniente al soporte de los fabricantes de hardware y software, estar pendiente de actualizar sus productos para así corregir las fallas en seguridad.

- Contemplar que las amenazas no solo pueden venir de afuera de la organización, sino que también de adentro, aplicando el principio de Defensa en Profundidad.

- Adaptar los objetivos de la seguridad con los objetivos y necesidades de la organización.

Se puede concluir que la seguridad de la información ha tomado mucha importancia, al principio las empresas tomaban esta actividad como algo de poca importancia y en algunos casos hasta creían que era un lujo innecesario, sin embargo en los últimos años ha sido transformada en una necesidad para la gestión corporativa, siendo una responsabilidad de la Alta gerencia el destinar recursos y los medios que se necesiten para la implementación de un Sistema de Gestión de la seguridad de la Información.

La seguridad de la información tiene unas funciones que son fundamentales en un proceso de gestión de la seguridad informática.

- Confidencialidad: Debe garantizar que el contenido de un mensaje ya sea almacenado o transmitido a través de un sistema de información solo podrá ser visto por el receptor y el destinatario. Es decir, esta función debe garantizar la confidencialidad de la información que reside en una organización tanto a nivel de equipos, servidores, sistemas de Backup y en la transmisión de datos por la red de comunicación.

- Autenticidad: Garantiza que en la creación de un mensaje la identidad del creador sea legitima dando la seguridad al destinatario de que la información que recibe es legítima. Esta función también autentica los equipos en la red para entrar en un determinado servicio, este tipo de autenticación puede ser unilateral que es cuando solo se conecta a la red o mutua donde se intenta conectar a un servidor y este solicita se autentique para validar sus permisos y permitir ingresar.

- Integridad: Encargada en que el contenido de un mensaje enviado al destinatario no se haya visto modificado en el proceso desde su creación y su transmisión. Y en caso de que esto ocurra, detectar que el mensaje fue modificado.

- No Repudio: Permite probar la autoría y envió de un determinado mensaje, mediante un mecanismo probatorio tanto el creador del mensaje como el destinatario no podrán negar que crearon y enviaron el mensaje ni negar haberlo recibido.

- Disponibilidad: Esta función es muy importante ya que se encargará de que el sistema esté siempre a disposición de los usuarios, este sistema debe ser lo suficientemente completo para que pueda resistir ataques e interferencias y aun así funcionar correctamente. Además, debe contar con un sistema de recuperación en caso de algún incidente de seguridad, al igual que a factores inesperados como desastres naturales o ataques malintencionados.[3]

Para una organización el implantar un sistema de seguridad para la información requiere una inversión considerable, para esto se debe analizar previamente las posibilidades de pérdida para la organización y evaluar los riesgos. El objetivo para una organización deberá ser que en caso de un ataque a los recursos o a la información sensible de la organización no tenga mayor costo para la misma, sino que al contrario sea más costoso para el atacante. Las organizaciones deben de tener la idea que esto es una inversión que a largo plazo es menor en comparación a los bienes y recursos que están protegiendo, esto después de analizar el costo beneficio dará una respuesta clara a que se debe invertir lo que sea necesario para proteger estos recursos. Las organizaciones deben analizar muy bien que expectativas debe cumplir esta seguridad ya que si no está enfocada en las necesidades y la misión de la organización está muy posiblemente no será suficiente para evitar que la información o los recursos de la organización se vean

[3] Ibid., p. 20, 21.

expuestos en un ataque, y que al final representará un costo muy elevado ya que se deberá reponer y resarcir el daño causado.

La seguridad de la información se deberá implementarse de una manera ordenada y a través de un proceso formal que deberá estar bien documentado y en este se definirán las responsabilidades a partir de unas políticas y procedimientos. A este proceso se le conoce como un Sistema de Gestión de la Seguridad de la información (SGSI), este es un estándar completo de procesos que van encaminados a establecer, implementar, mantener y mejorar de una manera continua la seguridad de la información tomando como referencia los riesgos a los que está expuesta la organización. Este sistema cuenta con múltiples procesos en los que se destacan dos:

- Procesos de Gestión: se encargan de controlar todo el sistema y su mejora continua.

- Procesos de Seguridad: se encargan de gestionar los procesos de seguridad de la información.[4]

4.2 AMENAZAS A UNA RED CORPORATIVA

Los ataques informáticos a las empresas siempre están motivados por el factor económico, aunque para algunos casos y en muchos ataques la motivación del atacante es simplemente el reto de acceder a un sistema. Existen muchas formas de ataques que se pueden hacer a la red de una empresa, aunque la más común es la de ataques por virus, ataques de denegación de servicios (DoS) etc.

- Ataques de repetición

Su vector de ataque se centra en la utilización de componentes que hacen la captura de contraseñas que han sido utilizadas anteriormente para acceder a aplicaciones de red. Para mitigar esto se recomienda aplicar software que identifique la reutilización de contraseñas y no permita el ingreso.

- Ataques de diccionario

Se basa en la utilización de un listado de contraseñas encriptadas, aprovechando que los sistemas de autenticación trabajan de forma unidireccional en el uso de contraseñas para computarlas de forma fácil pero descifrada complicado, para esto se usa este listado para comparar las contraseñas guardadas en este de la misma forma y así encontrar una contraseña que se repita.

[4] Ibid., p. 30, 31.

- Alteración y destrucción

En esta categoría se encuentran los virus, DoS, correos Phishing, Spam, etc. Los ataques DoS saturan los recursos del sistema hasta el punto del colapso del sistema para bloquear las aplicaciones. Hay varias formas de realizar ataques DoS donde se destacan él envió de tráfico basura como paquetes flooding o envió de solicitudes de conexión con direcciones IP ficticias.[5]

- Troyano

También conocidos como caballos de Troya debido a su método de infección en los sistemas de información que evoca al caballo de Troya de la mitología griega, ya que se encuentra escondido dentro de software que simula ser para cumplir un fin determinado y que el usuario necesita, pero que tiene instrucciones las cuales buscan degradar la seguridad y el sistema como tal sin que el usuario lo sepa y camuflarse dentro de este como un software inofensivo. Normalmente se usan con el fin de esconder al usuario atacante y a su vez prolongar la infección creando BackDoors en el caso de que este sea descubierto.[6]

- MITM (Man In The Middle)

Consiste en la interceptación de información desde un equipo cliente hacia un servidor sin que estos se percaten de este proceso. Todo esto ocurre cuando el equipo que realiza el ataque se infiltra en la red LAN y con técnicas de ARP Spoofing hace creer al equipo victima que está realizando una conexión con la puerta de enlace con la MAC del equipo atacante.

Un ataque de tipo MITM es fácilmente ejecutado a través de un conjunto de técnicas que permiten recibir la información de ambos extremos entre las cuales están:

- Usar un certificado invalido y hacer que el equipo cliente lo acepte a través del navegador.

- Usar un certificado valido en un dominio registrado por el atacante y el cliente confundirlo con un dominio legítimo.

- No usar un certificado y hacer un ataque en tiempo real.

---

[5] ARIAS SÁNCHEZ, Pablo. *Diseño de una red LAN/WAN segura para el Tribunal Constitucional aplicando la metodología de 3 capas de CISCO*. Quito. 2011. Tesis de Licenciatura. Pontificia Universidad Católica del Ecuador. Facultad de ingeniería

[6]HUERTA, Antonio. Seguridad en Unix y redes. 2002, vol. 1, p. 81.

Hay otro tipo de ataque de tipo MITM el cual consiste en la cual obliga que la conexión entre las partes se haga de manera forzada con el protocolo HTTP y evitar que la información se cifre con el protocolo HTTPS. Para esto el equipo atacante se sitúa entre el cliente y el servidor a través de distintas técnicas que incluyen suplantación ARP, modificación del proxy en el navegador o una red Wi-Fi de acceso abierto. Aquí cuando se logra que el atacante intercepte el tráfico entre las dos partes, busca el momento de que la comunicación cambie de HTTP a HTTPS, para así enviar un tráfico falso a la víctima para que no se complete el proceso de redireccionamiento y después si se haga la conexión con el servidor por HTTPS para así tanto la víctima como el atacante tengan acceso al sitio aunque la víctima no lo hace cifrando la información sino que la envía a través del protocolo HTTP y así el atacante podrá recibir la información que la víctima envié en un archivo de texto plano.

- Validación incorrecta de certificados

    - Certificados Autofirmados: estos certificados son parecidos a los certificados firmados por una entidad certificadora no fiable, pero en estos ellos no tiene otra entidad certificadora que el mismo certificado. Como estos certificados son fáciles de crear y no se pueden verificar por ninguna entidad, estos certificados no deben ser válidos, de por si los navegadores son capaces de detectarlos y envían advertencias al usuario al querer ejecutar alguno.

    - Certificados Expirados: para realizar la validación de los certificados es necesario hacerlo a través de X.509 donde se verifican las fechas de expedición y expiración, lo cual implica que la fecha de verificación debe estar dentro de este rango.

    - Aceptación de CA desconocidas:

- Revisión de revocación de certificados

Cada vez que un certificado se valida por razones diferentes que no cumplen con las políticas de X.509 (seguridad del certificado no segura, la llave privada o la CA hayan sido comprometidas, el propietario ya no califica), estos certificados deben revocarse y reportarse a la Lista de Revocación de Certificados (CRLs) y al Protocolo de Status de Certificados en Línea (OCSP).

- Basic Constraints

En 2002, Moxiw Marlinspike demostró como validar una CA no segura de nivel intermedio, todo a través del valor del parámetro Basic Constraints que está en el

certificado. Si este valor se encuentra en “false”, el certificado no es válido por ninguna CA intermedia. Pero hay navegadores y proxies de interceptación que pueden no validar correctamente este valor, y permitir que se lleven a cabo ataques por medio de certificados válidos y actuar como una CA intermedia y firmar otros certificados.

Para poder contrarrestar estas amenazas es necesario usar algunas medidas de seguridad.

- Nuevos Protocolos: Fuzzy Secure Socket Layer (FSSL)
- Validación de certificados en el navegador
- HTTP Strict Transport Security (HSTS): obliga el uso de HTTPS en la navegación
- The Public Key Pinning Extension for HTTP (HPKP): cada sitio especifica su clave pública con cabecera HTTP y rechaza el sitio que no sea conocida
- TLS Origin-Bound Certificate (TLS-OBC): Autentica al cliente por TLS, los navegadores generan un certificado autofirmados para cliente bajo demanda, sin configuraciones de usuario[7]

- Auditoría en Seguridad Informática

Es un documento donde analiza detalladamente un sistema de información, permitiendo ver, descubrir, identificar y corregir las vulnerabilidades en todo lo que compone un sistema de información ya sea Hardware, Software, infraestructura y recurso humano y en la labor que desempeña. Al final de esta se centra en que se cumplan los procedimientos de seguridad y se cumplan las políticas de seguridad, dando un vistazo actual a la seguridad que tiene la organización.

Dentro del documento que entrega el encargado o equipo encargado de la auditoria resalta que vulnerabilidades se identificaron durante el análisis y además donde contiene:

- Descripción y Características de los activos y procesos analizados

- Análisis de las relaciones y dependencias entre activos o en el proceso de la información

- Relación y evaluación de las vulnerabilidades detectadas en cada activo o subconjunto de activos y procesos

- Verificación del cumplimiento de la normativa en el ámbito de la seguridad

[7] ANGULO CASTRO, Diana. Análisis de herramientas de interceptación para el control de ataques reales de suplantación con certificados SSL. 2018.

- Propuestas de medidas preventivas y de corrección.[8]

4.3 DELITO INFORMATICO

Es todo aquel delito que atente en contra de cualquier sistema informático, ya sea sobre algún programa o información sensible o de mucha relevancia, o mediante la manipulación de alguna de las tecnologías de la información siendo típico (es decir que esté en contra del código penal), antijurídico (alguna norma existente configurada) y culpable (se le imputa el delito).

4.3.1 TIPOS DE DELITO INFORMATICO

- HACKING: Se le conoce como el acto de ingresar a un sistema de información sin autorización del propietario o el encargado de administrar dicho sistema, este proceso lo realiza vulnerando los sistemas de protección para tener acceso a información sensible con diferentes fines (ver, copiar o destruir).

- CRACKING: el objetivo del cracking es muy similar al del hacking el cual ingresa de la misma forma, pero su objetivo es destruir este sistema de alguna forma, ya sea cambiando contenidos que generen que el sistema colapse.

- PHREAKING: es usada para obtener acceso gratuito a los servicios de telefonía ya sea esta digital o análoga, celular o fija.

- CARDING: forma de fraude que se utiliza con tarjetas de crédito u otras tarjetas que usen números de identificación o sean recargables. Todo con el fin de realizar compras por distintos métodos, estos números pueden ser robados o creados a través de procedimientos digitales.[9]

4.4 PENTESTING

Existen varios conceptos de pentesting según la metodología que se vaya a implementar en un análisis de vulnerabilidades. En términos generales se conoce como pentesting al método donde el investigador forense o hacker ético intenta generar un tipo de ataque de forma segura para tener acceso o control de un sistema informático llámese red, equipos de cómputo etc. Para de esta manera descubrir y así lograr mitigar o corregir las vulnerabilidades encontradas y que pueden afectar a la organización basándose en un conjunto de técnicas y

[8] AGUILERA LÓPEZ, Purificación. Seguridad informática. (2010). Editex. 240p.

[9] CABRERA MEZA, Harold. Introducción Informática Forense. (2013).

procedimientos utilizados en muchas ocasiones por los mismos atacantes reales.

El pentesting sirve como medio de evaluación para medir el compromiso que tiene la organización con la seguridad informática y si sus políticas de seguridad informática han llegado al punto de que sus procesos de seguridad deben estar en constante evolución y que ningún mecanismo o metodología será suficiente para proteger completamente la información ante los ataques. La mejor forma de que las empresas estén seguras ante los ataques es que estén conscientes que la mejor forma es prevenir y detectar cualquier vulnerabilidad que se tenga y tener presente que siempre habrá vulnerabilidades y así estar preparado con contingencias que minimicen el impacto del ataque.

4.4.1 PASOS PARA HACER UN PENTESTING

Para poder ejecutar un pentesting es importante definir desde el principio la metodología que logre cubrir las necesidades de la organización a auditar, sin embargo, estas metodologías pueden ser estándar o se puede seguir un esquema propio siempre y cuando cumpla con los objetivos de realizar el pentesting. Para esto hay metodologías muy conocidas en el campo del pentesting, una de ellas es la OSSTMM (Open Source Security Testing Methodology Manual) del Instituto para la Seguridad y las Metodologías Abiertas (ISECOM). Existe también la OWASP (Open Web Application Security Project) enfocada en auditoria a páginas y aplicaciones web y por último esta ISSAF (Information Systems Security Assessment Framework).

Como se mencionó anteriormente, la metodología influye en el proceso de pentesting, cada metodología usa sus propios pasos para realizar un pentesting donde algunos ejecutan más procesos que otras o hay más fases. Por eso se toman algunos de los pasos fundamentales para un pentesting que la mayoría de las metodologías comparten y se describen a continuación:

- Fase de Recolección de Información

En esta se empieza con la recolección de toda la información, es muy importante ya que de esa información se comenzará un proceso que dispondrá en su totalidad de esta información. Estos datos van desde la razón de la empresa, su core o núcleo de negocios y hasta la conformación de la empresa. Todo esto a través de una recolección pasiva de información para que no haya interacción directa con los activos tecnológicos que se auditan, todo esto a través de consultas públicas en internet sobre el objetivo.

- Fase de Enumeración

Similar a la fase de recolección con la diferencia que ya se puede hacer contacto con los activos tecnológicos, haciendo pruebas de intrusión con herramientas que sean para pentesting. Aquí quedaran identificados los objetivos a través de múltiples pruebas dependiendo del área a auditar (escaneo de puertos, identificación de servicios, sistemas operativos, etc.).

- Fase de análisis

Existe ya una interacción con los activos tecnológicos donde por medio de algunos ataques se busque explotar una vulnerabilidad comprometiendo activamente al servicio, equipo, o dispositivo. Para esto es necesario que el analista cuente con los permisos por parte de la empresa para hacer estos ataques para realizar este análisis. Esto se logra usando la información recolectada en las fases anteriores para así poder ejecutar los escáneres de vulnerabilidades que permitirán evidenciar los puntos débiles de los medios analizados.

- Fase de Explotación

Como su nombre lo indica, en este punto los ataques ya son intrusivos y directos y van a un objetivo específico, para esto es necesario en algunos casos el uso de exploits ejecutados desde frameworks. Aquí se ejecutan ataques comunes como son fuerza bruta, cracking passwords, captura de paquetes de red, ingeniería social, ejecución de exploits conocidos, ataques DoS, pivoting, escalada de privilegios, etc.

- Fase de Documentación

Es la culminación después de ejecutadas las demás fases, obteniendo los resultados de los análisis y plasmándolos en un documento detallando los procesos realizados durante el pentest. En este documento es importante el plasmar las medidas de prevención que se sugieren para evitar que la empresa sea víctima de algún tipo de ataque reales a los que se ve expuesta.

El objetivo de esta fase es que se exponga a las personas encargadas y responsables de TI los resultados obtenidos a través de la labor realizada y que fallas y vulnerabilidades se han detectado con este pentest, donde se deben dejar en dos tipos de informes (técnico y ejecutivo).

El informe técnico es aquel que se explica en lenguaje detallado y técnico todas las actividades realizadas describiendo herramientas utilizadas y los resultados que se obtuvieron con esto y que se debe hacer para mitigar y resolver las fallas encontradas.

El informe ejecutivo por su parte es un resumen más ligero donde se explique qué vulnerabilidades se han encontrado suprimiendo el lenguaje técnico por completo. Este debe ser explicado de una forma de fácil comprensión para cualquier persona que no trabaje en TI, pero explique los riesgos que existen actualmente en la organización, pero que explique detalladamente las recomendaciones que el profesional de seguridad informática debe listar.[10]

[10] ERAZO BASTIDAS, Carlos. *Identificación de vulnerabilidades de los servicios tecnológicos de la unión de cooperativas de ahorro y crédito del norte aplicando la práctica de Pentesting*. Ibarra. 2017. 98p. Tesis de Licenciatura. Universidad Técnica del Norte. Facultad de Ingeniería y Ciencias Aplicadas.

5 METODOLOGÍA

La metodología para aplicar en este informe es la de aprendizaje que se basa en la lectura y ejercicios prácticos que permiten desarrollar las habilidades necesarias para resolver las cuestiones teóricas y prácticas que se plantean para el desarrollo de cada una de las actividades. Basándose también en lecturas y recursos bibliográficos que permitan comprender a detalle las situaciones planteadas y dar solución con un criterio ético y profesional como se solicita.

6 DESARROLLO DEL INFORME

6.1 ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

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

6.1.1.1 Ley 1273 de 2009

La ley 1273 fue creada el 05 de enero de 2009 y fue denominada como “De la protección de la información y de los datos”, la cual va encaminada en la modificación del código penal, y en considerar que los hechos delictivos en contra de sistemas informáticos ya se contemplan como tal y se especifican sus sanciones.

Tabla 1 Delitos informáticos amparados por la Ley 1273 de 2009

Delito informático	Descripción	Articulo
ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	Explica que se considera delito el acceso parcial o total a un sistema informático sin autorización o que abusando de la confianza del que tiene el derecho a excluir, acceda y no quiera salir del mismo, incurrirá en pena de prisión de 48 a 96 meses de prisión y en una multa de 100 a 1000 SMLMV.	Artículo 269A de la Ley 1273 de 2009, Ley de Delitos Informáticos en Colombia

Tabla 1 (Continuación)

OBSTACULIZACIÓN ILEGITIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN	Toda acción que tenga como fin impedir u obstaculizar de alguna forma el acceso y/o el funcionamiento de cualquier tipo de sistema informático (llámese datos, red de telecomunicaciones) sin estar facultado para ello incurrirá en sanción de 48 a 96 meses de prisión y a multas de 100 a 1000 SMLMV.	Artículo 269B de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia
INTERCEPTACIÓN	Esta ley contempla a todo aquel individuo que sin pertenecer a la rama judicial o tenga permiso judicial, haga cualquier tipo de interceptación desde su origen o destino, aun desde un sistema informático. Tendrá una sanción que va desde los 36 a los 72 meses de prisión.	Artículo 269C de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia
DAÑO INFORMÁTICO	Contempla en la destrucción, daño, borrado, deterioro, algún tipo de alteración parcial o total de información ya sea que este en un sistema de tratamiento (base de datos) o atente en contra de este, la sanción va desde los 48 a los 96 meses de prisión y a la multa de 100 a 1000 SMLMV.	Artículo 269D de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia

Tabla 1 (Continuación)

USO DE SOFTWARE MALICIOSO	Aquí se contempla los delitos relacionados con software malicioso y virus, tanto la compilación, obtención, sustracción, lo compre o lo venda o cualquier hecho con el cual tenga beneficio propio o a una tercera persona, tendrá sanciones desde los 48 a 96 meses de prisión y a multas de 100 a 1000 SMLMV.	Artículo 269E de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia
VIOLACIÓN DE DATOS PERSONALES	Básicamente contempla todo lo relacionado en la divulgación y obtención de datos personales o datos sensible de una organización con fines delictivos tendrá sanción de 48 a 96 meses de prisión y a multas desde 100 a 1000 SMLMV.	Artículo 269F de la ley 1273, De 2009, Ley de Delitos Informáticos en Colombia

Tabla 1 (Continuación)

SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES	El cual dice, que una persona que con fines delictivos y sin tener las capacidades para hacerlo, diseñe, desarrolle, trafique, venda, ejecute, programe o le envié páginas web a enlaces fraudulentos a otra persona o entidad, o que este incurra en la modificación de algún sistema de resolución de nombres de dominio con el fin de engañar a la otra persona haciéndole creer que está entrando a algún sitio de confianza. Incurrirá en penas que van desde los 48 meses a los 96 meses de prisión y a pagar multas de 100 a 1000 SMLMV.	Artículo 269G de la ley 1273 de 2009, Ley de Delitos informáticos en Colombia

Tabla 1 (Continuación)

AGRAVANTES	Serán motivo de agravante de los artículos anteriores los siguientes casos. ➢ Todo tipo de delito u ataque a entidades estatales u oficiales ➢ Algún empleado o servidor público en ejercicio de sus labores ➢ Abusando de la confianza del poseedor o similares ➢ El que revele o divulgue alguna información buscando perjuicio para alguien ➢ El que lo haga con fines de lucro ➢ Cometer algún delito con fines terroristas o alguna acción que ponga en riesgo la seguridad y defensa nacional ➢ Manipulando una tercera persona la cual actué de buena fe ➢ Si se comprueba que el imputado tiene nexos o maneja esta información quedara inhabilitado para manejar algún tipo de información con sistemas computacionales por un periodo de 3 años. Como ha pasado en casos muy conocidos, han alterado páginas de bancos, entidades del Estado o páginas de carácter público. Todo esto a través de muchas modalidades como el Phishing en correos electrónicos o creando paginas fraudulentas a bancos.	Artículo 269H de la ley 1273 de 2009, Ley de Delitos informáticos en Colombia

Tabla 1 (Continuación)

HURTO POR MEDIOS INFORMÁTICOS	Este artículo es un ítem para el artículo 239 del código penal colombiano, donde especifica las propiedades del delito de hurto con el agregado que este artículo el cual específica que es sobre algún sistema informático, o suplante a un usuario ante los mecanismos de autenticación y autorización que estén establecidos, tendrá una sanción que se contempla en el artículo 240 del código penal.	Artículo 269I de la ley 1273 de 2009, Ley de Delitos informáticos en Colombia
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	Aplica a los individuos que, aprovechando el conocimiento de algún tipo de táctica o manipulación de un sistema informático, logre transferir algún tipo de activo perjudicando a una tercera persona y consiga alguna especie de lucro. Si en la ley no existe una sanción o existen agravantes deberá pagar una condena de prisión de 48 a 120 meses y en multa de 200 a 1500 SMLMV, también aplica para quien suministre, venda introduzca o fabrique programas de computación que se use para la comisión de un delito de las características del inciso anterior.	Artículo 269J de la ley 1273 de 2009, Ley de Delitos informáticos en Colombia

Como ha pasado en casos muy conocidos, han alterado páginas de bancos, entidades del Estado o páginas de carácter público. Todo esto a través de muchas modalidades como el Phishing en correos electrónicos o creando paginas fraudulentas a bancos.

6.1.1.2 Ley 1581 de 2012

La ley 1581 fue creada el 17 de Octubre de 2012 y tienen como finalidad de otorgar el derecho constitucional de cada persona de saber, actualizar, corregir todo tipo de información personal que se ha recogido en cualquier sistema de información (bases de datos o archivos) y que sean aplicables para ser tratados por cualquier tipo de entidad ya sea pública o privada

en el territorio colombiano y/o fuera de él siempre que esta ley sea aplicable en virtud de normas y tratados internacionales a que haya lugar.

Los principios que aplican esta ley son:

- **Legalidad:** Siempre que se haga tratamiento de datos personales, se deben realizar bajo lo establecido en esta ley
- **Finalidad:** Se debe realizar un tratamiento legítimo de los datos y ser informada al titular de estos datos
- **Libertad:** Solo se puede realizar el tratamiento de estos datos con previa autorización del titular
- **Veracidad o calidad:** Esta información a tratar debe ser precisa**,** veraz, completa, actualizada, comprensible y comprobable
- **Transparencia:** Se debe garantizar la transparencia para que el titular pueda obtener dicha información
- **Acceso y circulación restringida:** Debe estar sujeta a limites derivados de los datos personales dispuestos en la constitución y esta ley donde no podrá estar en internet u otros medios de divulgación masiva
- **Seguridad:** Se debe tener un tratamiento donde se garantice que estos datos estén seguros empleando todas las medidas posibles como técnicas, humanas y administrativas
- **Confidencialidad:** Se debe garantizar la reserva de la esta información por parte de cada persona que haga parte del proceso de tratamiento de estos datos

6.1.1.3 Decreto 1377 de 2013

Este decreto tiene como objeto el reglamentar de manera parcial la ley 1581 de 2012 para así dar claridad a las empresas sobre los aspectos importantes para la protección de datos personales y/o sensibles.

6.1.1.4 Ley 1266 de 2008

Esta ley regula el uso y la administración de las bases de datos para evitar que se dé la información contemplada en estas bases y esta no dañe el buen nombre comercial y crediticio de las personas naturales. También conocida como la ley de Habeas Data, es una acción constitucional que permite a cualquier persona saber, actualizar, corregir todo tipo de información personal que se ha recogido en cualquier sistema de información (bases de datos o archivos) y que sean aplicables para ser tratados por cualquier tipo de entidad ya sea pública o privada.

6.1.2 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.

Para poder ejecutar un pentesting es importante definir desde el principio la metodología que logre cubrir las necesidades de la organización a auditar, sin embargo, estas metodologías pueden ser estándar o se puede seguir un esquema propio siempre y cuando cumpla con los objetivos de realizar el pentesting. Para esto hay metodologías muy conocidas en el campo del pentesting, una de ellas es la OSSTMM (Open Source Security Testing Methodology Manual) del Instituto para la Seguridad y las Metodologías Abiertas (ISECOM). Existe también la OWASP (Open Web Application Security Project) enfocada en auditoria a páginas y aplicaciones web y por último esta ISSAF (Information Systems Security Assessment Framework).

Como se mencionó anteriormente, la metodología influye en el proceso de pentesting, cada metodología usa sus propios pasos para realizar un pestesting donde algunos ejecutan más procesos que otras o hay más fases. Por eso se toman algunos de los pasos fundamentales para un pestesting que la mayoría de las metodologías comparten y se describen a continuación:

- **Fase de Recolección de Información:** En esta se empieza con la recolección de toda la información, es muy importante ya que de esa información se comenzará un proceso que dispondrá en su totalidad de esta información. Estos datos van desde la razón de la empresa, su core o núcleo de negocios y hasta la conformación de la empresa. Todo esto a través de una recolección pasiva de información para que no haya interacción directa con los activos tecnológicos que se auditan, todo esto a través de consultas públicas en internet sobre el objetivo.

  Herramientas: Se puede hacer uso de Google, ya que este buscador permite agregar parámetros más específicos como búsqueda de puertos

- **Fase de Enumeración:** Similar a la fase de recolección con la diferencia que ya se puede hacer contacto con los activos tecnológicos, haciendo pruebas de intrusión con herramientas que sean para pentesting. Aquí quedaran identificados los objetivos a través de múltiples pruebas dependiendo del área a auditar (escaneo de puertos, identificación de servicios, sistemas operativos, etc.).

Herramientas: Entre las herramientas más utilizadas por los pentesters se tiene NMAP, el cual permite enviar paquetes que permiten revelar información sobre una dirección IP especifica como puertos abiertos y cerrados y con esto identificar la aplicación o servicio que suministra.

- **Fase de análisis:** Existe ya una interacción con los activos tecnológicos donde por medio de algunos ataques se busque explotar una vulnerabilidad comprometiendo activamente al servicio, equipo, o dispositivo. Para esto es necesario que el analista cuente con los permisos por parte de la empresa para hacer estos ataques para realizar este análisis. Esto se logra usando la información recolectada en las fases anteriores para así poder ejecutar los escáneres de vulnerabilidades que permitirán evidenciar los puntos débiles de los medios analizados.

  Herramientas: Una herramienta que permite analizar los objetivos de ataque es Nikto2, la cual permite verificar cuando un sistema operativo no está actualizado o archivos de configuración por defecto.

- **Fase de Explotación:** Como su nombre lo indica, en este punto los ataques ya son intrusivos y directos y van a un objetivo específico, para esto es necesario en algunos casos el uso de exploits ejecutados desde frameworks. Aquí se ejecutan ataques comunes como son fuerza bruta, cracking passwords, captura de paquetes de red, ingeniería social, ejecución de exploits conocidos, ataques DoS, pivoting, escalada de privilegios, etc.

  Herramientas: Para esta fase se puede utilizar una herramienta común como Metasploit, la cual permite explotar estas vulnerabilidades ya que cuenta con una librería extensa de vulnerabilidades explotables para muchos de los sistemas operativos y servicios.

- **Fase de Documentación:** Es la culminación después de ejecutadas las demás fases, obteniendo los resultados de los análisis y plasmándolos en un documento detallando los procesos realizados durante el pentest. En este documento es importante el plasmar las medidas de prevención que se sugieren para evitar que la empresa sea víctima de algún tipo de ataque reales a los que se ve expuesta.

  El objetivo de esta fase es que se exponga a las personas encargadas y responsables de TI los resultados obtenidos a través de la labor realizada y que fallas y vulnerabilidades se han detectado con este pentest, donde se deben dejar en dos tipos de informes (técnico y ejecutivo).

  El informe técnico es aquel que se explica en lenguaje detallado y técnico todas las actividades realizadas describiendo herramientas utilizadas y los

resultados que se obtuvieron con esto y que se debe hacer para mitigar y resolver las fallas encontradas.

El informe ejecutivo por su parte es un resumen más ligero donde se explique qué vulnerabilidades se han encontrado suprimiendo el lenguaje técnico por completo. Este debe ser explicado de una forma de fácil comprensión para cualquier persona que no trabaje en TI, pero explique los riesgos que existen actualmente en la organización, pero que explique detalladamente las recomendaciones que el profesional de seguridad informática debe listar.

Herramientas: Una herramienta que se incluye en el catálogo de Kali Linux es Magic Tree, la cual consolida toda la información de un pentesting realizado y la muestra en un esquema de árbol.

6.1.3 Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

Herramientas:

- **Metasploit:** A través de esta herramienta que se conoce tanto a nivel de seguridad como de los criminales informáticos para detectar y auditar las vulnerabilidades de un sistema, todo a través de comandos cortos y de funciones ya grabadas.

  Para el caso de Windows, Metasploit cuenta con múltiples tipos de ataques para explotar vulnerabilidades conocidas de Windows en muchas de sus versiones y que permite que se realicen los procesos necesarios para mitigar los riesgos. Una de esas herramientas permite realizar ataques de elevación de privilegios. La elevación de privilegios permite proporcionar permisos a un usuario que no los tiene inicialmente, en este caso se puede por medio de un payload llamado Meterpreter, el cual es un tipo de troyano que se carga en memoria lo cual le permite ocultarse y en este se definirán los parámetros de ataque.

- **Nmap:** Es una herramienta open source y de código abierto que nos permite escanear y rastrear el estado de los puertos de una red entera o de una dirección IP especifica. Además de permitir identificar el sistema operativo y en un nivel avanzado, encontrar vulnerabilidades con el fin de realizar una auditoría de red o en casos de los cibercriminales realizar un ataque dirigido.

- **OpenVas:** Esta herramienta open source y de software libre bajo la licencia GNU. Al igual que Nessus este compone de herramientas que ayudan identificar vulnerabilidades por medio de escaneo de seguridad de red, contiene una interfaz gráfica de usuario e integra aplicaciones de seguridad. Open Vas contiene un servidor y un cliente que se conecta a este permitiendo detectar seguridad en los sistemas por medio del cliente (NVT). Openvas también maneja lenguaje NASL, y tiene cerca de 17000 módulos de comprobación de seguridad.

  Openvas cuentas con los siguientes servicios y utilidades:

  - Supervisión de servicios de red
  - Escaneo de puertos abiertos
  - Detección de sistema operativo (hardware)
  - Interfaz gráfica para conectarse con varios agentes
  - Los agentes cuentan con desplazamiento
  - IDS
  - Escaneo de múltiples redes remotas
  - Guardado de estado red
  - No necesita privilegios de root

Servicios en línea:

- **ExploitDB:** Es una base de datos web donde es almacenado un repositorio de exploits gratuitos para realizar prácticas de laboratorio o como pruebas de penetración sobre vulnerabilidades encontradas. El objetivo de esta web es la poner al alcance y con fines netamente educativos o de ayuda para la investigación y detección de vulnerabilidades de cualquier sistema operativo investigado soportando plataformas Windows, UNIX, Linux, etc.

- **CVE:** Una plataforma en línea muy conocida en el mundo de la ciberseguridad, ya que proporciona un listado casi ilimitado de vulnerabilidades que han sido detectadas por diferentes entidades y hackers éticos sin fines de lucro y que ponen en conocimiento público con el objetivo de prevenir que sean explotadas. Esta plataforma usa una nomenclatura que facilita su identificación y cuenta con las respectivas características, así como la solución que puede ser una actualización, una línea de comando, parches de seguridad, etc. Cada una de estas vulnerabilidades, debe ser pasada por una revisión específica del grupo de CVE para garantizar que esta información sea constantemente actualizada y así pueda ser publicada.

6.1.4 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:

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

Ilustración 1 Descarga VirtualBox

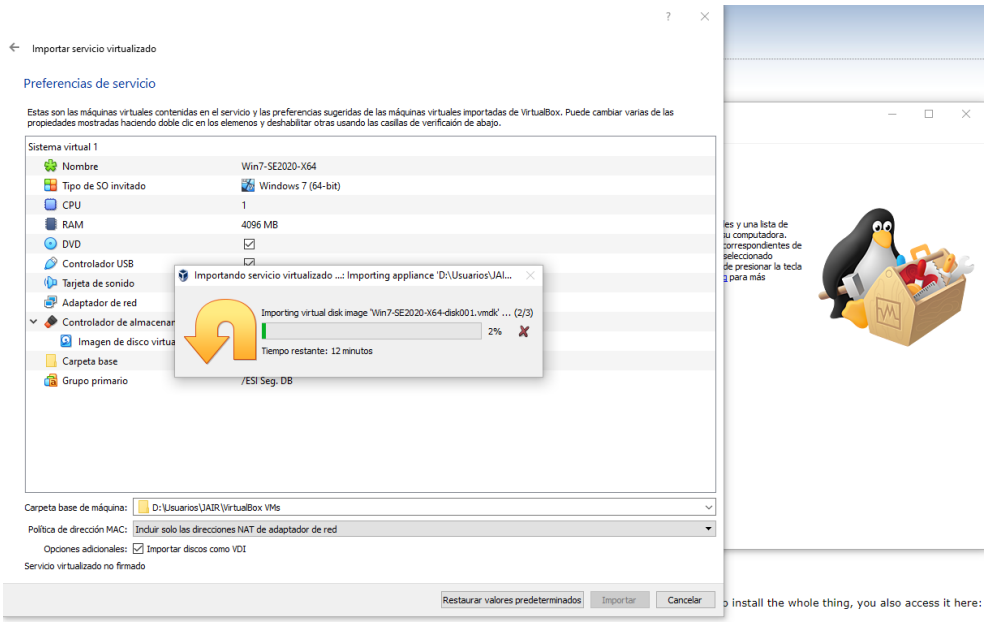
Fuente: Propia

Ilustración 2 Instalación completa de VirtualBox

Fuente: Propia

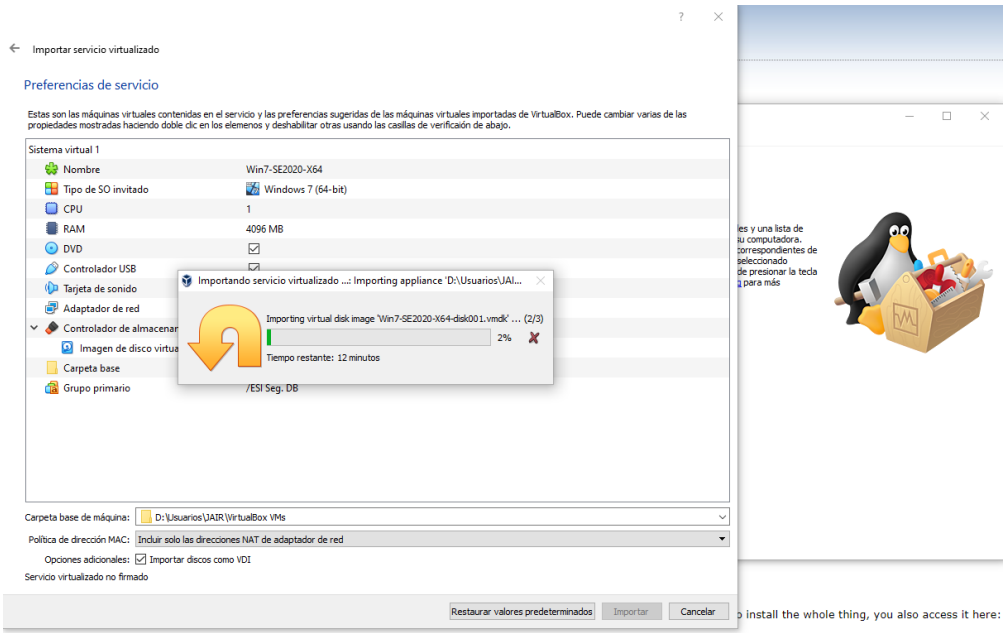
- **Paso B:** Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter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

Ilustración 3 Instalación Maquina Windows 7 64Bits



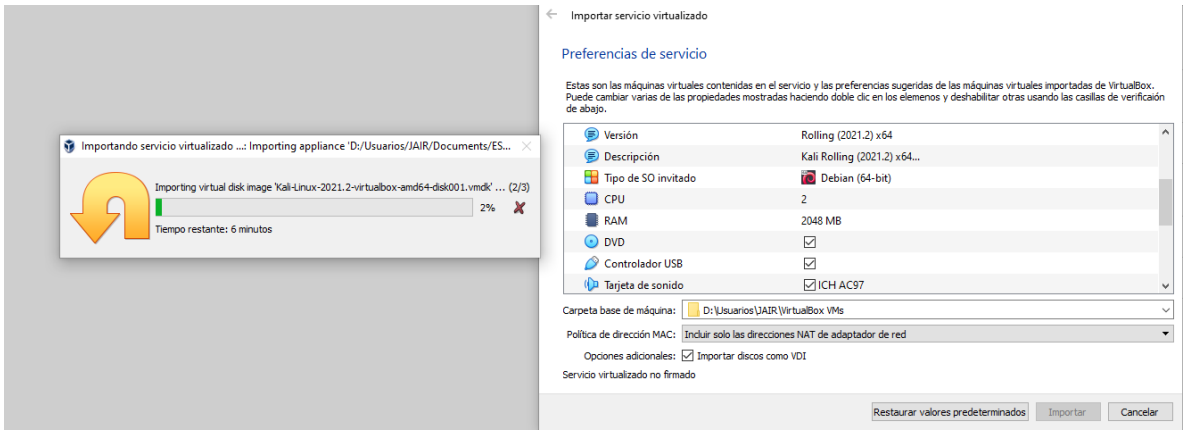
Fuente: Propia

Ilustración 4 Instalación Maquina Windows 7 32 Bits



Fuente: Propia

Ilustración 5 Instalación Kali Linux

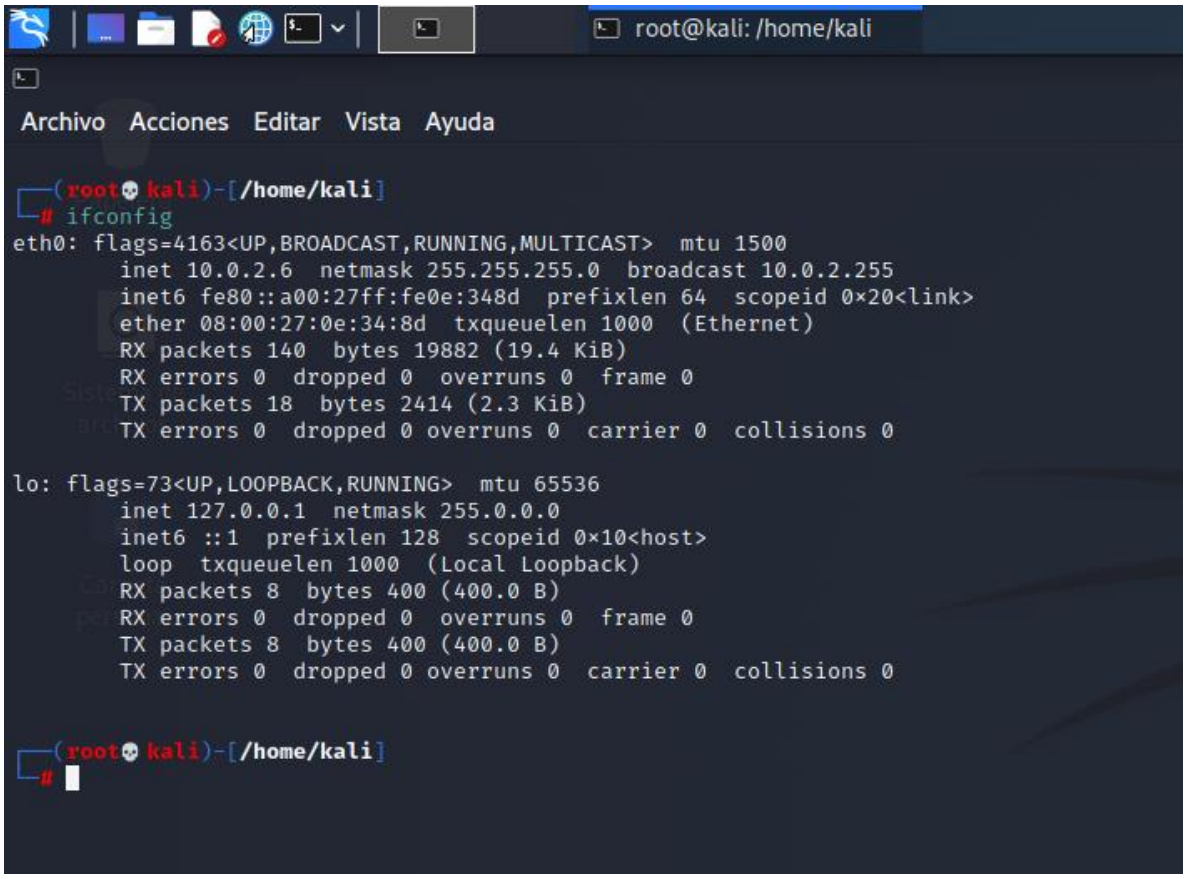


Fuente: Propia

- **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.

Se verifica el direccionamiento IP de la maquina con Kali Linux

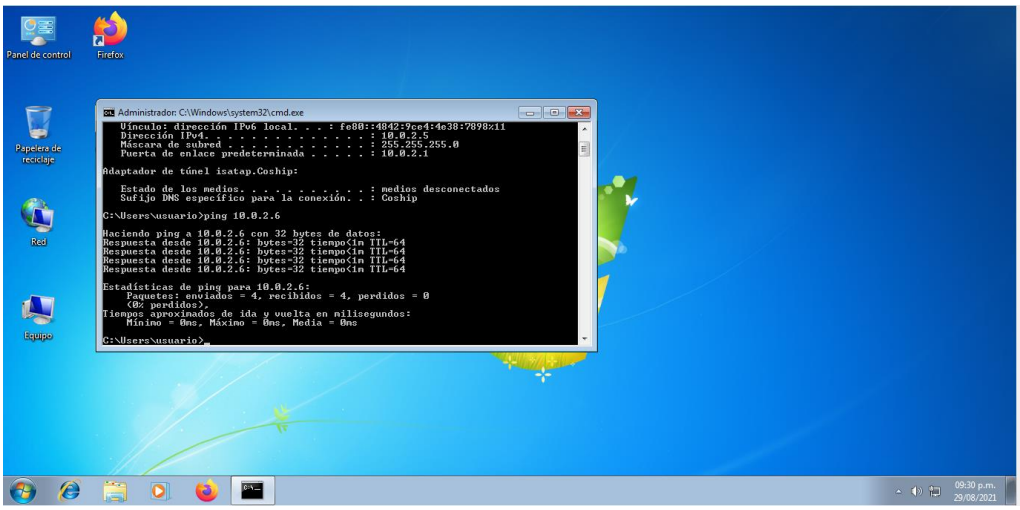
Ilustración 6 Dirección IP Kali Linux



Fuente: Propia

Se verifica el equipo Windows 7 de 64 Bits la dirección IP y si responde a ping el equipo con Kali Linux

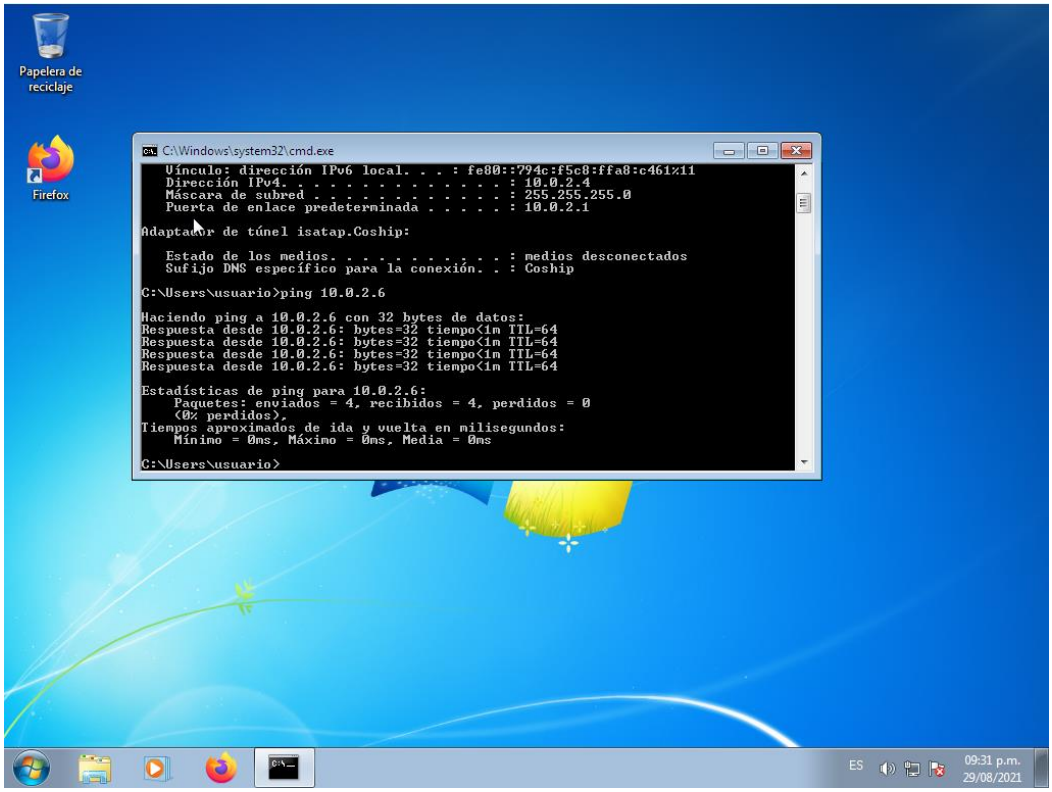
Ilustración 7 Evidencia Ping Windows 7 64 Bits



Fuente: Propia

También se observa respuesta de ping desde el equipo con Windows 7 32 Bits

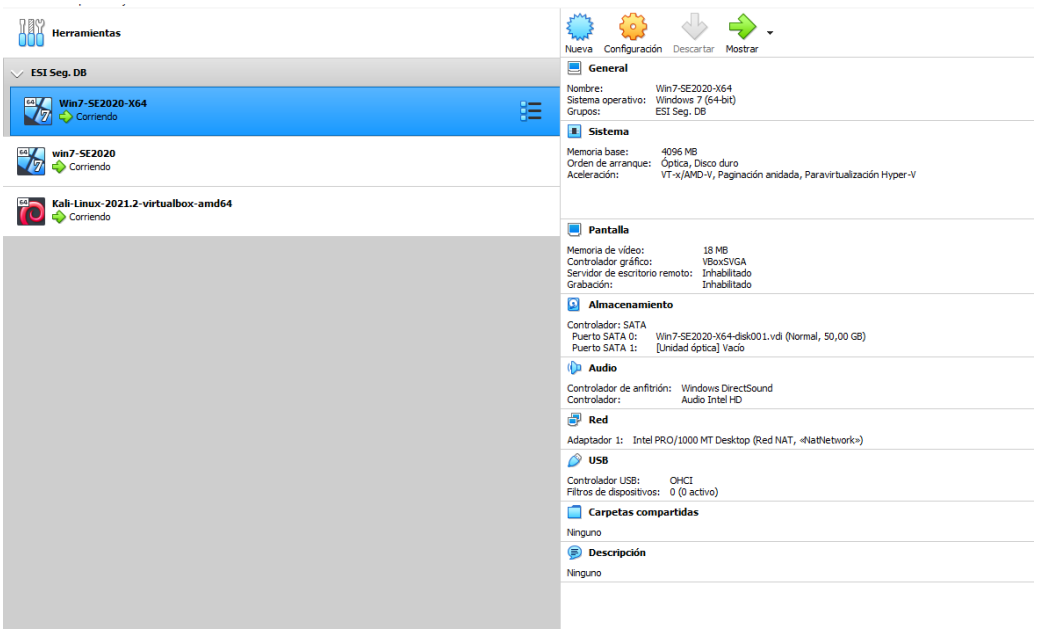
Ilustración 8 Respuesta a ping equipo Windows 7 32 Bits



Fuente: Propia

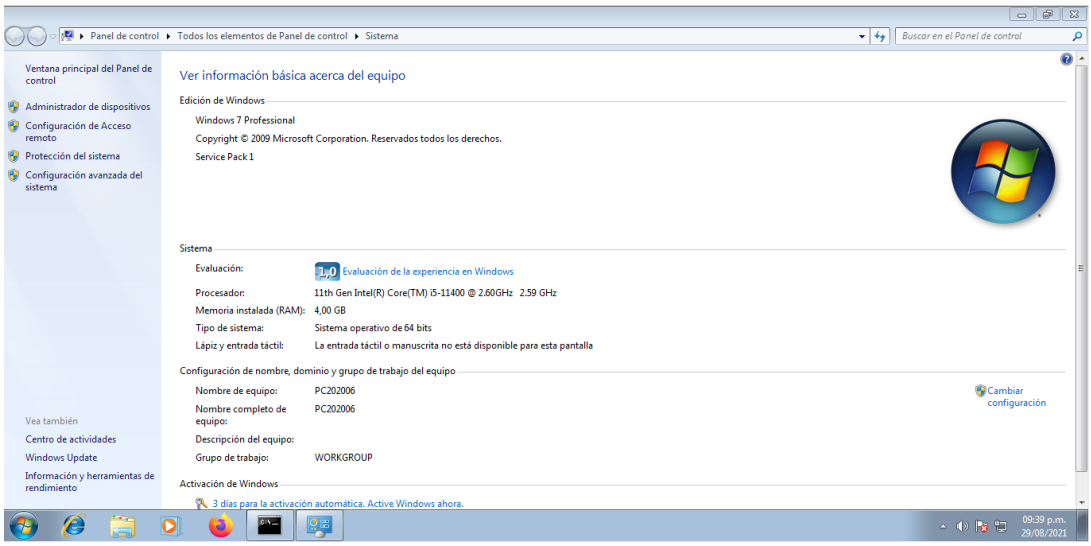
- **Paso D:** Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Ilustración 9 Hardware Windows 7 64 Bits



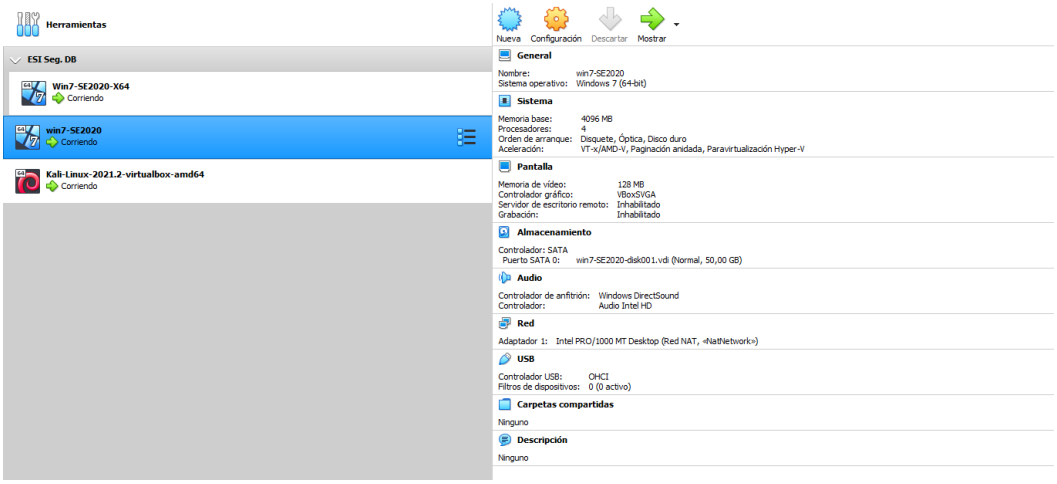
Fuente: Propia

Ilustración 10 Características Windows 7 64 Bits (Propiedades)



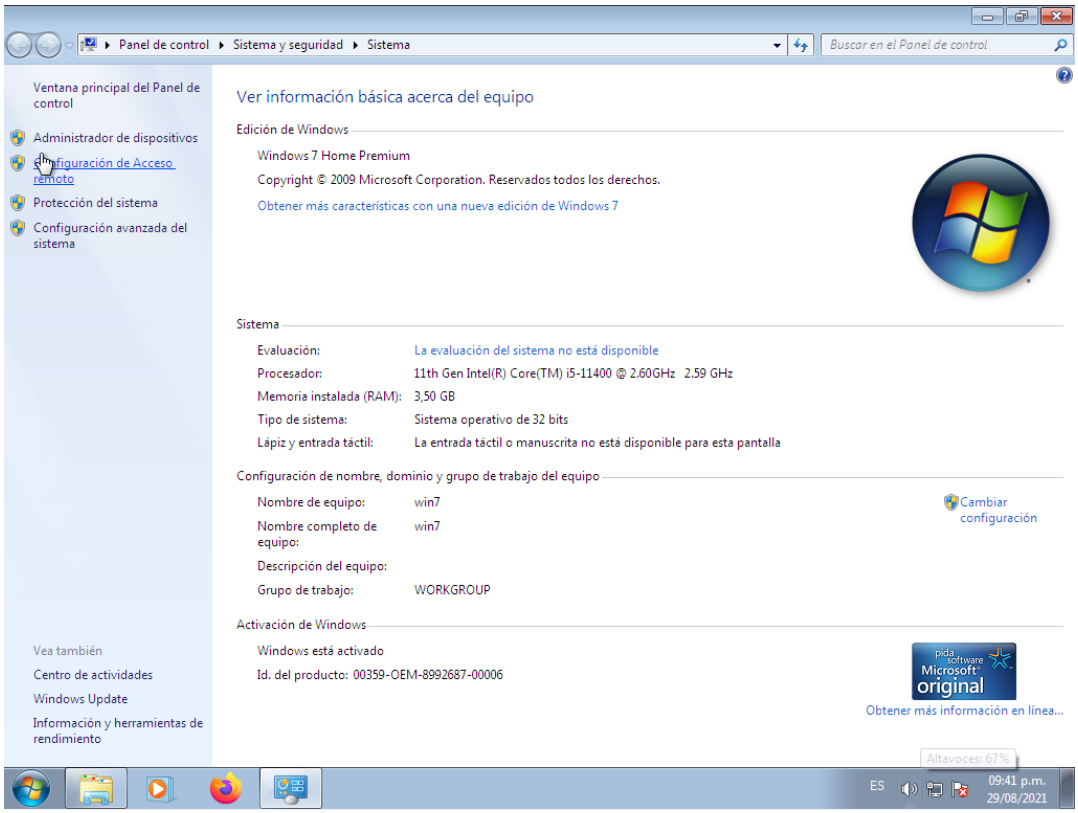
Fuente: Propia

Ilustración 11 Hardware Windows 7 32 Bits



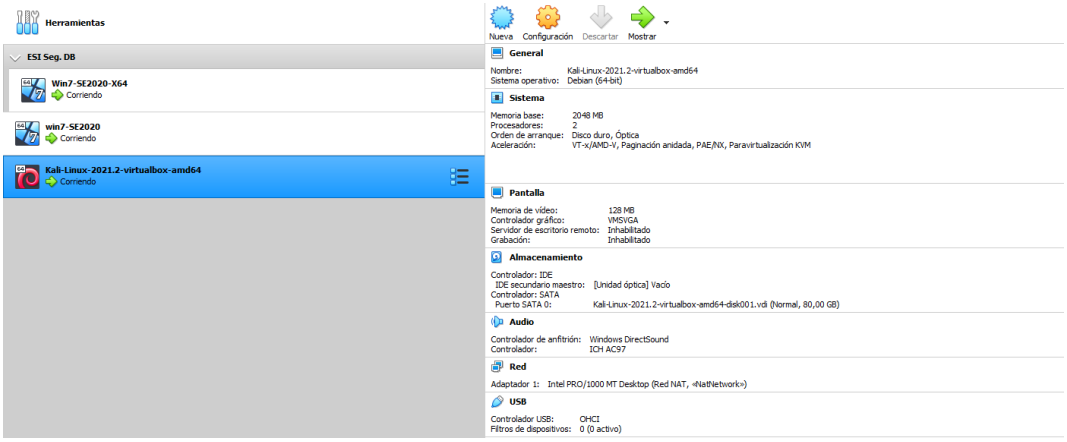
Fuente: Propia

Ilustración 12 Características Windows 7 64 Bits (Propiedades)



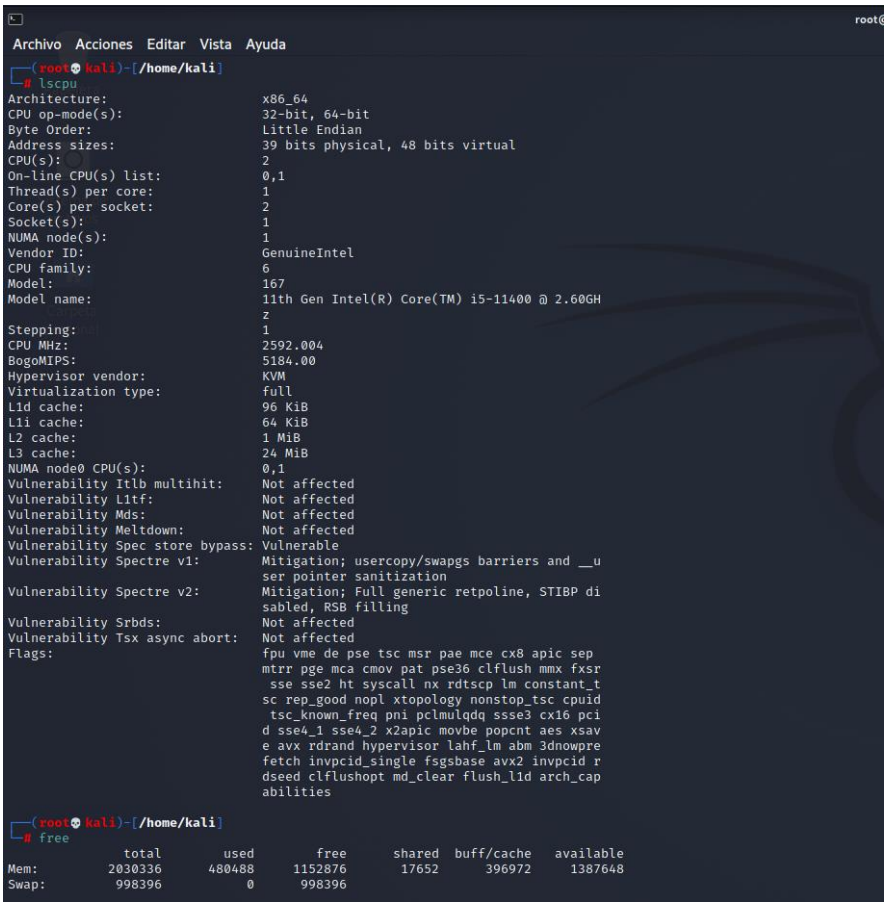
Fuente: Propia

Ilustración 13 Características Kali Linux



Fuente: Propia

Ilustración 14 CPU y Memoria RAM Kali Linux



Fuente: Propia

6.2 ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL

6.2.1 ¿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.

Fragmento del acuerdo

Consideraciones

1. Que la información compartida en virtud del presente acuerdo pertenece a Whitehouse Security, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del proceso de selección de personal.

2. Que la información de propiedad de Whitehouse Security Whitehouse Security ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal*, Jairo Orlando Acevedo Jiménez* que para el presente caso actual como **revelador, guarda y administrador** de la información de propiedad de Whitehouse Security*.*

Análisis

Como primera medida, la empresa Whitehouse Security está llevando a cabo un proceso de contratación para elegir a su personal que hará parte de los equipos red Team y red Blue a través de un acuerdo entre los candidatos y la empresa. Este acuerdo, sin embargo, bajo un punto de vista personal y ético, no es correcto ya que este acuerdo de entrada compromete de una manera legal y ética al candidato a custodiar, salvaguardar y proteger información antes de incluso firmar dicho acuerdo porque está revelando dicha información y casi obligando al candidato a recibir esta información antes de firmar el acuerdo. Además, utilizan el título de secreto industrial, donde según la Decisión 486 del 2000 por la Comunidad Andina de Naciones (CAN) a la cual pertenece Colombia, define el Secreto Industrial o Empresarial a la información no divulgada que se posea por cualquier tipo de

persona (Natural o Jurídica) de manera **Legitima y/o Legal**[11]**.** Esto demuestra que, la persona que elaboro dicho contrato obvio la explicación sobre esta definición a fin de delimitar dicha definición y amparar toda la información como secreto industrial.

Fragmento del acuerdo

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.

Análisis

De acuerdo con lo que considera la persona que redacta el acuerdo, el candidato no divulgara ante ningún ente externo incluyendo a las autoridades legales sobre procesos **ilegales,** es decir que a concepto personal no es nada ético ni profesional obligar a un candidato a encubrir estas actividades ya que está contemplado en la Ley 842 de 2003 del Consejo Profesional Nacional de Ingeniería Copnia Capitulo II Articulo 14[12]; como una falta disciplinaria sancionable el encubrir un ejercicio ilegal de la ingeniería.

Fragmento del acuerdo

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:
1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.
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

[11] La Decisión 486 de 200 en su artículo 260 establece que es un secreto empresarial y define los casos en que una información es susceptible de ser secreto empresarial; estas condiciones son: que sea secreta, es decir que no sea de fácil acceso, que tenga un valor comercial, y, por último, que haya sido objeto de medidas razonables para proteger su secreto.

[12] ARTÍCULO 14. ENCUBRIMIENTO DEL EJERCICIO ILEGAL DE LA PROFESIÓN. El servidor público que, en el ejercicio de su cargo, autorice, facilite, patrocine, encubra o permita el ejercicio ilegal de la ingeniería o de alguna de sus profesiones afines o auxiliares, incurrirá en falta disciplinaria, sancionable de acuerdo con las normas legales vigentes.

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.
3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Análisis

La explicación de **Información confidencial** concuerda en principio en que es toda información no publica de carácter confidencial. Sin embargo, el concepto se delimita de lo legal al insinuar que se puede manejar información producto de hechos ilegales y de poca ética como “Chuzadas, accesos abusivos a sistemas informáticos y/o interceptación de información”. Esto está contemplado en los Artículos 269A, 269B y 269C de la Ley 1273 de 2009 sobre Delitos Informáticos en Colombia y son sancionables con pena de prisión y multas.

Fragmento del acuerdo

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.

Análisis

Se comprende correctamente como son los medios de transmisión de la información que puede ser confidencial o pública. Sin embargo, están obviando la responsabilidad de aclarar si esta es información confidencial o no, dejando un vacío legal donde pueden aprovechar para culpar al candidato por algún tipo de filtrado de información que a criterio propio puede ser información no confidencial, pero para la empresa sí. Algo poco ético a criterio personal porque es deber de la empresa dar en conocimiento que información es de carácter confidencial.

Fragmento del acuerdo

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:
De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

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

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

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.

5. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

6. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

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

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.

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.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información como confidencial.

Análisis

Dentro de los artículos de la **Decisión 486 del 2000,** específicamente en el **Articulo 262,** donde se constituye en competencia desleal todo lo relacionado con la explotación, divulgación y adquisición de un secreto empresarial bien sea por parte de un tercero que haya accedido a dicho secreto de manera ilegal o legal con el deber de reservar dicha información.

En esto, obligan al candidato a no denunciar estos actos, sabiendo que esto es obligación de un profesional y que está contemplado en el Copnia como falta a la Ética y profesionalismo de un ingeniero en Colombia.

En una de las obligaciones coloca en posición de responsable al candidato para así liberar a la empresa de cualquier culpa en caso de algún tipo de allanamiento donde se encuentre procesos o información ilegales es usar un chivo expiatorio que faltando totalmente a la ética y afectando el buen nombre de una persona logran cubrir los intereses ilegales y faltos de todo pundonor a una empresa.

Todo esto a su vez que, la persona que redacto este acuerdo sabiendo que de presentarse alguna irregularidad de carácter ilegal y que llegue a manos del candidato, este no podrá realizar ningún tipo de acción sin el consentimiento de la misma, obviamente para evitar que las autoridades sean informadas de dichas actividades y evitar tramites y procesos legales y jurídicos que afecten a la misma.

Fragmento del Acuerdo

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la información confidencial hasta tanto

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia

del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Análisis

Deja un vacío en lo que se comprende sobre las obligaciones de la **parte Reveladora**, donde prácticamente deja sin ninguna obligación en el acuerdo y con el candidato y así poderse entender a su conveniencia cualquier tipo de reclamo o queja que llegue por parte del candidato.

Fragmento del Acuerdo

Octava. Solución de controversias: Las partes *(Jairo Orlando Acevedo Jimenez – WhiteHouse Security)* 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.

Análisis

Prácticamente exonera a la empresa de cualquier tipo de culpabilidad en casos de ilegalidad, indicando que no proporcionará ningún tipo de auxilio jurídico al candidato y que deberá asumir este costo por el mismo y dejar en limpio el nombre de la empresa, lo cual es muy irresponsable, ya que no asumirá ningún tipo de culpabilidad por los delitos o actos ilegales cometidos y con previo conocimiento de estos.

Fragmento del Acuerdo

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Análisis

Hacen la salvedad que se rigen en las leyes colombianas y a lo largo del documento se evidencio que no es cierto ya que vulneran bastantes leyes y artículos sobre delitos informáticos e información en Colombia como se ha explicado anteriormente.

También indican que ambas partes han leído y estudiado el acuerdo, pero como se dice en el **Anexo 2,** esto no es cierto ya que la empresa no ha analizado este documento.

6.2.2 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.

Para este caso, como se ha indicado, la empresa está realizando un tipo de prueba para elegir a los candidatos que conformaran sus equipos Red y Blue Team, si permite que este documento este dentro de los documentos legales de contratación estaría violando las leyes laborales ya que no da ningún tipo de garantías al candidato de protección y prácticamente esta condenando al mismo por cualquier delito pasado, presente y futuro del que pueda ser responsable la empresa y obviamente también vulnera las leyes laborales en el país.

Para los artículos que no respeta este acuerdo según la ley 1273 de 2009 sobre delitos informáticos en Colombia, se vulneran los siguientes según al concepto y basado en lo encontrado y analizado del mismo.

Tabla 2 Artículos Ley 1273 de 2009

Fragmento del Acuerdo	Artículo de la Ley 1273 de 2009	Descripción	Sanción
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.	• Artículo 269A de la Ley 1273 de 2009, Ley de Delitos Informáticos en Colombia • Artículo 269C de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia	• Explica que se considera delito el acceso parcial o total a un sistema informático sin autorización o que abusando de la confianza del que tiene el derecho a excluir, acceda y no quiera salir del mismo • Esta ley contempla a todo aquel individuo que sin pertenecer a la rama judicial o tenga permiso judicial, haga cualquier tipo de interceptación desde su origen o destino, aun desde un sistema informático.	• Incurrirá en pena de prisión de 48 a 96 meses de prisión y en una multa de 100 a 1000 SMLMV. • Tendrá una sanción que va desde los 36 a los 72 meses de prisión.

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.	• Artículo 269A de la Ley 1273 de 2009, Ley de Delitos Informáticos en Colombia • Artículo 269C de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia	• Explica que se considera delito el acceso parcial o total a un sistema informático sin autorización o que abusando de la confianza del que tiene el derecho a excluir, acceda y no quiera salir del mismo • Esta ley contempla a todo aquel individuo que sin pertenecer a la rama judicial o tenga permiso judicial, haga cualquier tipo de interceptación desde su origen o destino, aun desde un sistema informático.	• Incurrirá en pena de prisión de 48 a 96 meses de prisión y en una multa de 100 a 1000 SMLMV. • Tendrá una sanción que va desde los 36 a los 72 meses de prisión.

6.2.3 ¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿usted como experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, 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.

A título personal y basado en mi formación profesional y sobre todo los valores y principios que he formado a lo largo de mi vida profesional y personal **NO APLICARIA.** Esto debido a que el ejercicio de la profesión no debería ser solo con fines lucrativos, sino también en desempeñar una función muy importante y de mucho valor para las empresas y las personas a nuestro alrededor. Sentir la satisfacción del deber cumplido y la conciencia tranquila de hacer las cosas con respeto y honradez es una de las recompensas que debería impulsar a la gente a desempeñar esta y todas las profesiones.

En base a esta argumentación, el Consejo Profesional Nacional de Ingenierías Copnia en la **Ley 842 de 2003 sobre la Ética Profesional** en el **Capítulo II Articulo 31**, basa estos deberes también en valores éticos y morales como el respeto, imparcialidad a cada una de las personas que estén involucradas en el ejercicio de

la profesión. Al igual que de valores y profesionalismo propios de cualquier profesión como el de custodiar y cuidar cada uno de los bienes que por producto de la profesión y la labor ejercida se tenga acceso o sean encomendados. Como se demuestra en el Acuerdo entregado, ellos no autorizan el acceso a las autoridades nacionales en caso de necesitar investigar algún hecho que corresponda y se deba por ser profesional inscrito ante este consejo, permitir el acceso a documentos e información que para la empresa es considerada **confidencial** a sabiendas que es información de actividades ilegales como reza el **Artículo 31** Inciso **E**. Al igual que también como parte de esos deberes está la de denunciar cualquier falta, contravención o delito que en el ejercicio de las funciones profesionales este enterado, algo que claramente va en contra de este Acuerdo con la empresa y que se especifica claramente en el Inciso **F** del **Articulo 31** de la Ley expuesta. Al igual que lo anteriormente expuesto, el **Articulo 32** en los incisos **B y C** de permitir, tolerar y/o facilitar el ejercicio de manera ilegal de cualquiera de las profesiones que están contempladas en esta Ley, así como el de solicitar y/o aceptar comisiones en dinero por ejercer la profesión sin estar debidamente contratado o estar legalizado con el cliente, empresa, entidad, etc. Al igual que los Artículos expuestos anteriormente, el **Articulo 34** en el inciso **A** reza que no Ofrecer y/o aceptar trabajos que vayan en contra de las disposiciones legales Vigentes, como lo que se ha expuesto en el Acuerdo, esto claramente viola este articulo y no sería ético ni profesional aceptar esta propuesta sabiendo de antemano que va en contra de esto, al igual que lo que se expone en el **Artículo 40** Inciso **A** donde el ofrecer cualquier tipo de prestación de servicio de cualquier índole (técnico, jurídico o económico y social entre otros) sea de dudoso cumplimiento o vaya en contra de las circunstancias o la idoneidad personal. Como se puede observar, el Copnia en la Ley 842 de 2003, ha reglamentado y más a socializado todos los aspectos que van ligados directamente a la ética no solo profesional sino la personal en el cumplimiento de cualquier profesión amparada por ellos.

6.2.4 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.

Este caso deja en evidencia que el hacking ético en ese tiempo era un tema muy distorsionado, para este caso en particular, el reclutamiento de talento técnico y sobresaliente en técnicas de computación disfrazado de comunidad de ethical hacking, fue la estrategia perfecta para esconder de la vista de todo el mundo la parte delictiva de esta práctica tan importante para las personas y empresas a través del mundo digital. Se veía como una iniciativa muy buena para compartir el conocimiento sobre la seguridad informática y nuevas tecnologías y a través de la tecnología y los eventos destinados a la tecnología como el Campus Party al igual que en blogs y hasta en Twitter fue que su creador y fundador Carlos Betancur que se hacía llamar “Bender” hizo de Buggly el templo para algunos donde se podía

hablar y vivir en este mundo de tecnología a simple vista. Combinando tecnología, comida, tatuajes y ocio y demás fue que Buggly tomo fuerza y empezó a atraer talentos que poco a poco fueron empezando a sumar para lo que sería una de las grandes fuentes de interceptación de datos que ha tenido Colombia ya que como se supo después, esto fue directamente financiado por el Ejército Nacional y que todo era para cazar talentos que con el pensamiento de transmitir y absorber conocimiento terminaron siendo utilizados para temas de espionaje a grupos guerrilleros como las FARC (incluso a los comisionados del proceso de paz que se llevaba a cabo en la Habana para esos tiempos) y el ELN. Ver que usaban a personas con habilidades para la seguridad informática para realizar interceptaciones que para el Ejercito eran “Legales” a simple vista no lo eran tanto ya que según información que se ha divulgado sobre este caso, miembros del mismo ejercito habrían vendido información recolectada de estas interceptaciones a personas comunes y hasta a bandas criminales para otros fines, dejando la legalidad de lado y lucrándose de estos actos de forma ilícita yendo totalmente en contra de lo que se ha establecido en leyes como la Ley 1273 de 2009, Ley 842 de 2003 y la Ley 1581 de 2012. Independientemente del objetivo principal de esta operación llamada ANDROMEDA, la forma de hacerlo engañando a jóvenes ingenuos, a profesionales que solo buscaban aprender y rodearse de gente que compartiera su pasión por la seguridad informática y tener un espacio donde esto fuera natural no tiene nada de ético ni de profesional, sobre todo al pensar que fue concebido desde un ente gubernamental y más aún, una Entidad que vela por la seguridad y la justicia de un país, deja una gran decepción en los profesionales que como yo quieren aprender y expandir el conocimiento y que ese conocimiento pueda llevarse a construir un mejor país, pero al mismo tiempo demuestra que existe talento y sobre todo existe la honestidad de todos aquellos que nos estamos formando y los que ya son expertos en seguridad informática y que la ética es uno de los pilares más fuertes que se deben tener para ejercer esta labor que siempre está en constante cambio y que necesita que más profesionales estén dispuestos a poner su conocimiento a disposición para que se vea el hacking ético y a los pentesters no como criminales, sino como profesionales altamente capacitados y entrenados para evitar que nuestra información pase de ser confidencial a ser publica sin nuestro consentimiento y proteger la confidencialidad, integridad y disponibilidad de nuestra información basados en todos los aspectos legales y éticos que tenemos disponibles.

6.3 ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

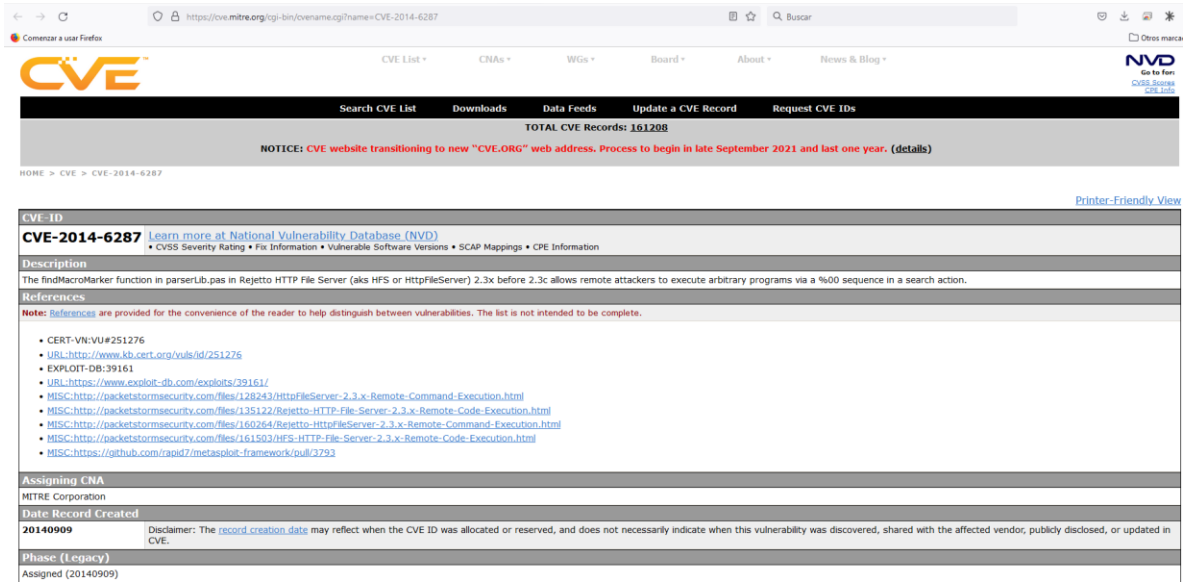
6.3.1 Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

Para poder realizar este pentesting, se hace uso del sistema operativo Kali Linux y las herramientas de pentesting con las que cuenta para este proceso. Se ejecutarán las etapas para la realización de un pentesting y corroborar si efectivamente es posible explotar una vulnerabilidad en este equipo Windows 7 con arquitectura x64.

6.3.1.1 Fase de Recolección de Información

Para saber que vulnerabilidad tiene la aplicación Rejjeto la cual, según una búsqueda realizada en Google sobre esta, es una aplicación para el uso compartido de archivos a través de internet. La cual tiene una vulnerabilidad en la función "findMacroMaker" en la librería parserLib.pas en versiones anteriores a la 2.3c y por la cual los atacantes de manera remota pueden ejecutar programas de manera arbitraria a través de una secuencia %00 en una acción de búsqueda.[13] Para esto, ya existe un exploit conocido para poder explotar esta vulnerabilidad a través de la herramienta de Metasploit de Kali Linux.

Ilustración 15: Vulnerabilidad CVE2014-6287



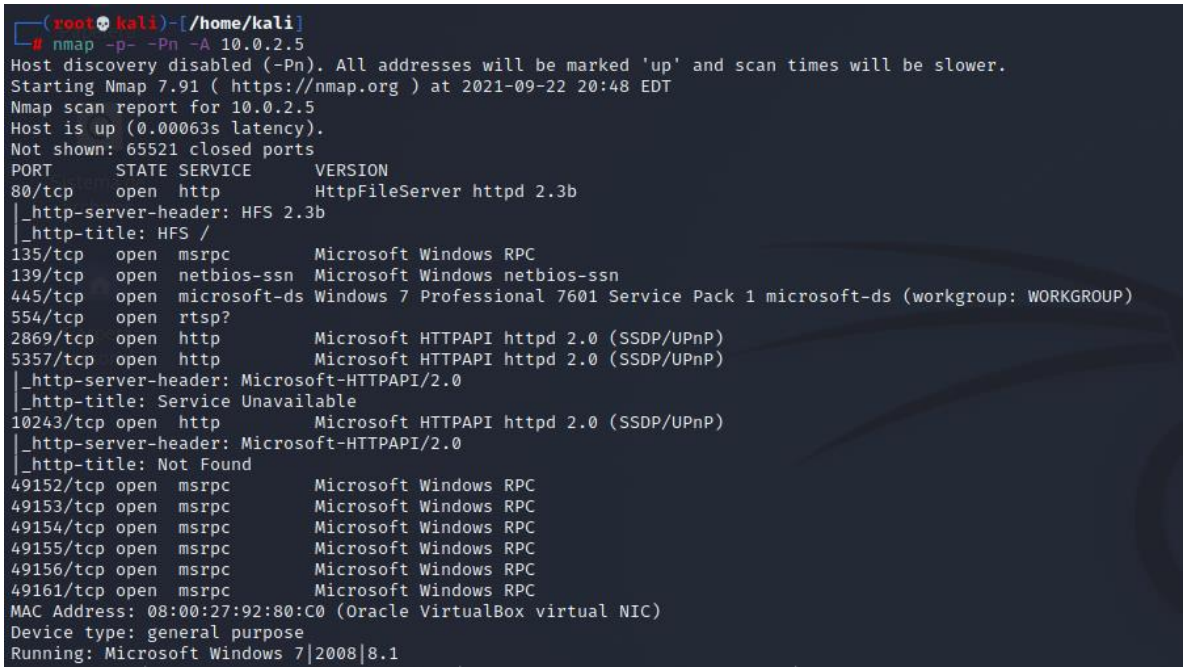
Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

[13] CVE-2014-6287 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.

6.3.1.2 Fase de Enumeración

Para conocer un poco a detalle si el equipo a analizar es vulnerable a un ataque de tipo Shell Reversa por el uso de la aplicación Rejjeto en su versión 2.3 la cual actúa sobre el protocolo HTTP, se hará uso de la herramienta NMAP la cual permite examinar los protocolos abiertos de un host y así poder verificar si el puerto 80 usado para HTTP está a la escucha por alguna aplicación instalada en el equipo y tener datos de la versión específica del software utilizado y poder explotar dicha vulnerabilidad.

Ilustración 16: Escaneo de puertos con Nmap



Fuente: Propia

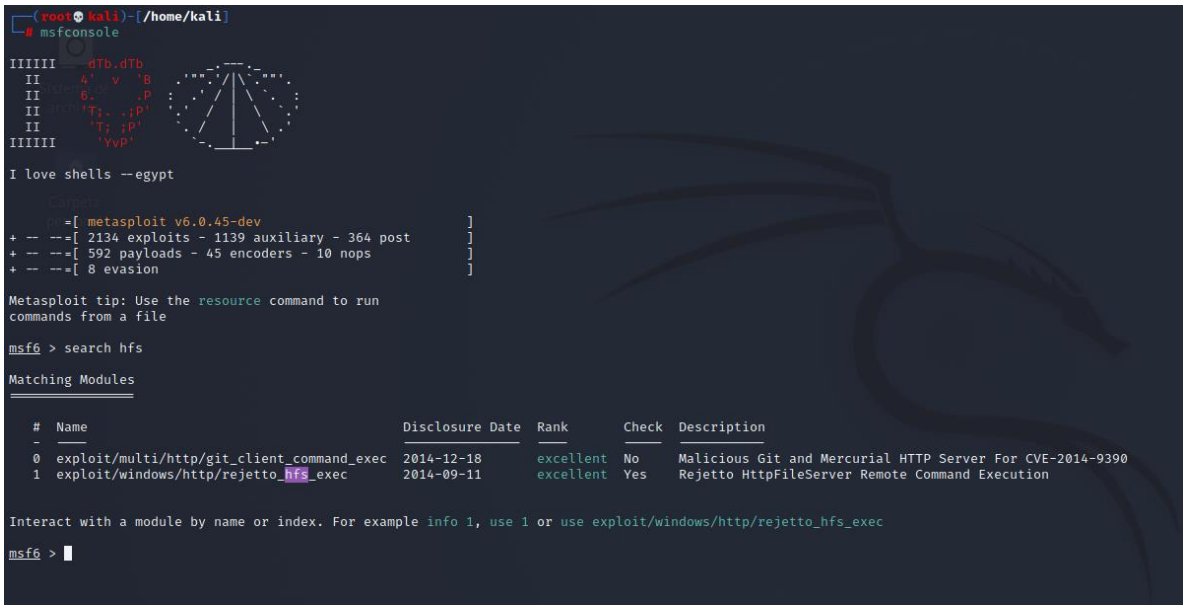
Al ejecutar Nmap desde Kali Linux con el argumento **-p-** se pudieron evidenciar que puertos se encuentran a la escucha, al igual que la opción **-Pn-** que permite conocer información del Sistema operativo del Host. Se observa que el **puerto 80** se encuentra en estado **open.** En el cual se observa que está siendo utilizado por la aplicación **HFS 2.3b** lo cual permitirá correr el exploit para explotar la vulnerabilidad.

6.3.1.3 Fase de análisis

Ahora se procede a realizar el análisis de la vulnerabilidad con la información recolectada de las fases anteriores. Esta versión de HFS tiene un exploit en la herramienta **Metasploit** integrada en el paquete de Kali Linux y con la cual se llevará a cabo el proceso con permiso de la empresa.

Esta herramienta también nos permite buscar exploit a través del comando **search.** Como no se sabe exactamente el exploit que se puede explotar usaremos este comando para encontrar el exploit a utilizar.

Ilustración 17: Búsqueda de vulnerabilidades con Metasploit



Fuente: propia

Se observa en los parámetros arrojados que la aplicación rejetto tiene dos exploit, uno de ellos (1 rejetto_hfs_exec) con un Rank excelente y chequeado (Yes); lo cual significa que se puede utilizar para explotar esta vulnerabilidad en la host víctima.

6.3.1.4 Fase de Explotación

Ya con la información recolectada de las demás fases, se procede a realizar la explotación de la vulnerabilidad hallada en la aplicación del host. Para lo cual se procede a cargar el exploit rejetto_hfs_exec en el Metasploit para proceder a ejecutarlo en el host víctima.

Ilustración 18: Cargando exploit a ejecutar

Fuente: Propia

El siguiente paso es configurar este exploit para ser utilizado sobre la dirección IP del equipo con Windows 7 x64. Para lo cual se hace uso del comando **set** en Metasploit para así establecer las variables necesarias para poder ejecutar con éxito este exploit. Las variables son:

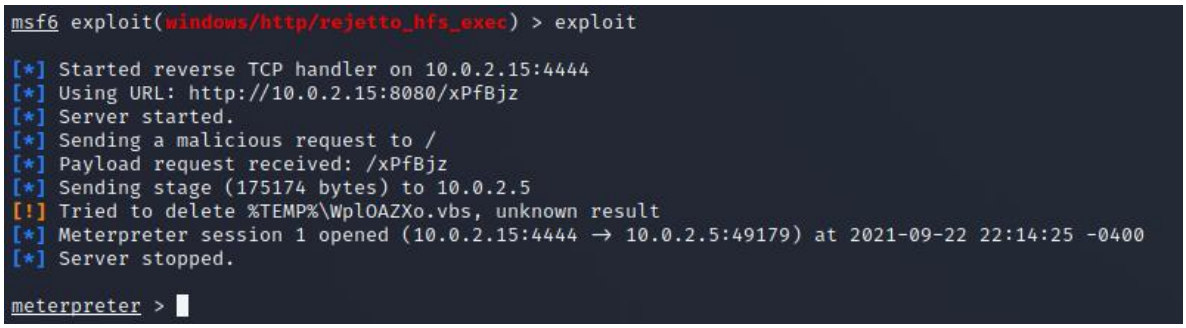
- **RHOST:** Se establece la dirección IP del host que se va a atacar
- **SRVHOST:** Se establece la dirección IP del equipo atacante, en este caso nuestro equipo con Kali Linux

Ilustración 19: Configuración variables

Fuente: Propia

Ya con estas variables configuradas, se procede a ejecutar el exploit que explotara la vulnerabilidad seleccionada.

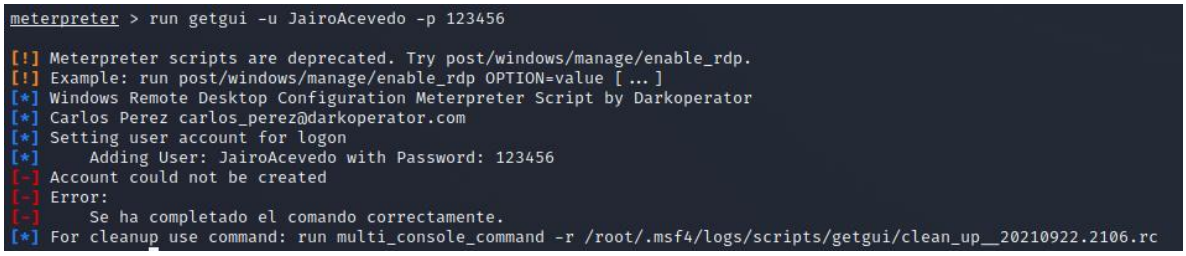
Ilustración 20: Ejecución del exploit



Fuente: Propia

Ya se tiene acceso para ejecuta el código para crear usuario, por lo cual se procede a crearlo para comprobar que la explotación fue un éxito.

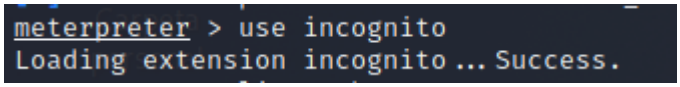
Ilustración 21: Creación de usuario



Fuente: Propia

Ahora se procede a darle privilegios de Administrador al usuario que se acaba de crear a través del comando **Incognito.** El cual nos permitirá asociar el usuario creado al grupo de Administradores.

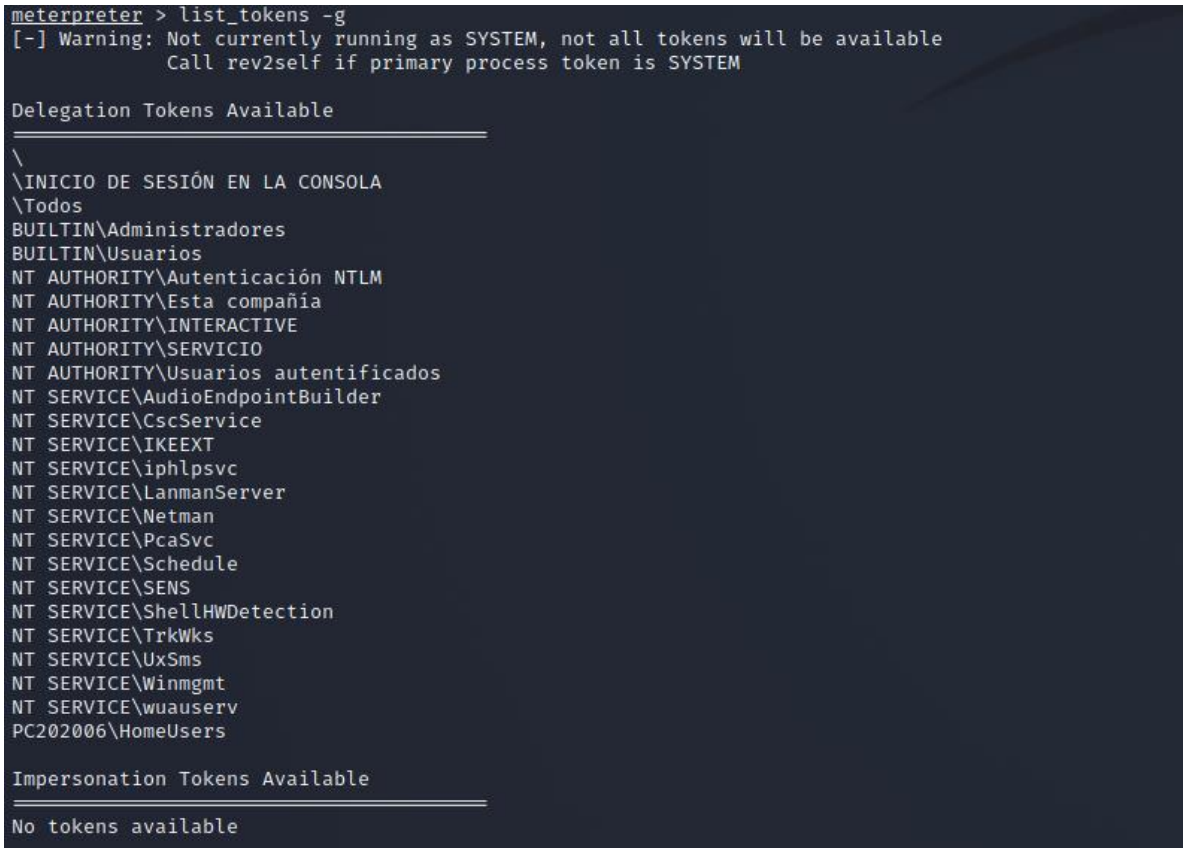
Ilustración 22: use incognito



Fuente: Propia

Para ver los grupos en este equipo, hacemos uso del comando dentro de incognito **list_tokens -g.**

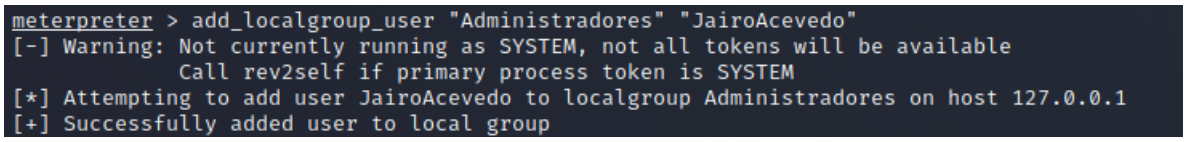
Ilustración 23: Vista de grupos Windows 7



Fuente: Propia

Ahora a través del comando **add_localgroup_user** se agrega el usuario **JairoAcevedo** al Grupo de **Administradores.**

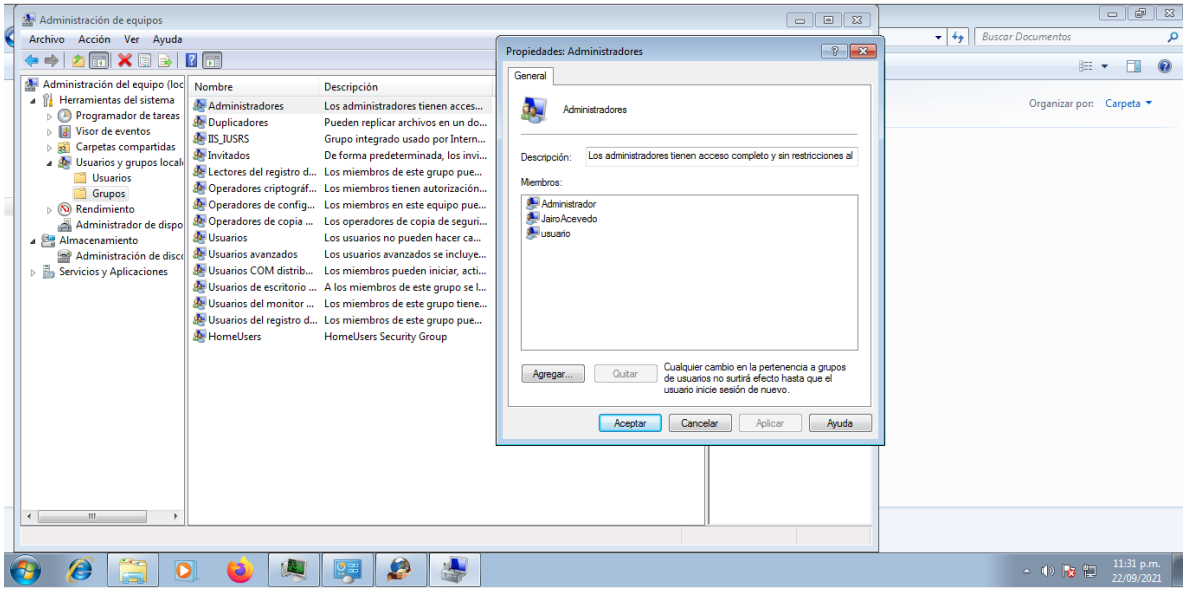
Ilustración 24: Agregar usuario a Administradores



Fuente: Propia

Ahora en el equipo con Windows 7 x64 se comprueba la creación del usuario **JairoAcevedo** y que está en el grupo de **Administradores.**

Ilustración 25: Creación usuario JairoAcevedo



Fuente: Propia

6.3.1.5 Fase de Documentación

Se pudo evidenciar que a través de la aplicación Rejetto HFS 2.3 fue posible realizar un ataque de Shell inversa y explotar esta vulnerabilidad de nivel crítico, ya que permitió la creación y acceso al equipo sin ningún tipo de autenticación y dar permisos de administrador a un usuario creado de manera remota. Esto es debido a que esta aplicación está en una versión en la cual se han expuesto múltiples vulnerabilidades y las cuales son de nivel crítico ya que permite realizar las acciones que se hicieron en esta prueba de laboratorio. Se debe tener en cuenta también que el sistema operativo donde se ejecuta la aplicación está en una versión obsoleta y sin ningún tipo de soporte por parte de Microsoft, lo cual la hace vulnerable a todo tipo de ataques ya que, al no contar con actualizaciones y parches de seguridad, es una puerta abierta a los atacantes para poder tener acceso a la información de la empresa. Para el equipo de seguridad de la información y TI es muy importante conocer y remediar este tipo de vulnerabilidades ya que esto es una violación a los pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) y se debe tener medidas en las cuales este contemplado este tipo de dispositivos y el riesgo que representan.

6.3.2 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.

1. Para este caso, se tiene ya conocimiento por parte de la empresa que se ha presentado una fuga de información dentro de la misma.

2. Se tiene identificado el equipo donde se presenta la fuga de información, el cual tiene instalada una aplicación para compartir archivos hacia internet llamada **Rejetto v. 2.3,** la cual está corriendo sobre un Sistema operativo Windows 7 con arquitectura a 64Bits.

3. Teniendo esta información, lo primero que se realiza es una investigación a través del buscador Google donde se encuentra que esta aplicación trabaja sobre el protocolo HTTP, lo cual es el primer indicio para sospechar que la aplicación no es segura ya que si funciona como un servidor de archivos debe tener un método de encripción o usar protocolos seguros que permitan que la información viaje de manera segura.

4. También se encuentra que efectivamente esta aplicación y más específicamente en esta versión, ya cuenta con menciones en bases de datos de vulnerabilidades como **CVE, exploit.db, etc.** Por lo cual es fácil encontrar información de como poder llevar a cabo un ataque de Shell Reversa o similares que permitan acceder a la información de manera ilegal.

5. Para este escenario, el equipo funciona como un servidor de archivos a través del protocolo HTTP, donde cualquier equipo cliente inicia una comunicación de tipo Shell remota y el servidor como está a la escucha de peticiones por este puerto predeterminado las recibe e inicia la transferencia. Aunque existe la forma de invertir la situación y que el cliente pueda escuchar también esas peticiones conociendo el puerto por el cual se realizan dichas peticiones.

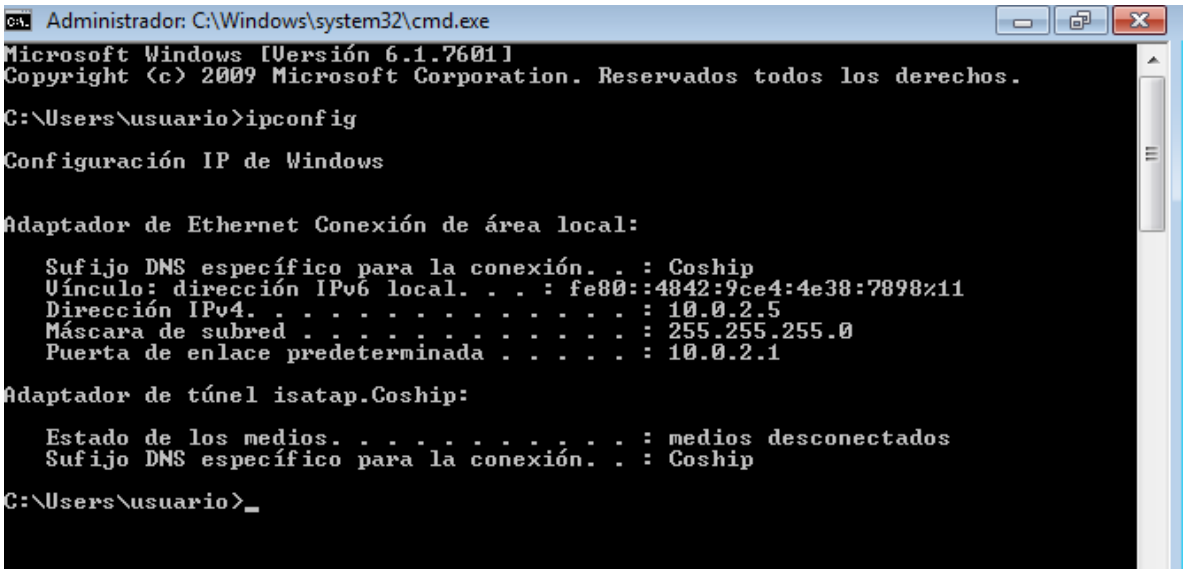
6. Al tener conocimiento de los puertos utilizados por el servidor, y que se pueda comprobar que efectivamente están escuchando peticiones por estos puertos que normalmente son permitidos por algún Firewall o aplicación y los cuales pueden ser detectados a través de aplicaciones de identificación de puertos como Nmap, Nessus, Metasploit, etc. Y además que estos puertos no se filtran en ocasiones y permiten recibir todo el

tráfico que vaya por ellos, y para el atacante resulta fácil realizar una intrusión a un sistema vulnerable.

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

Para la detección de los fallos de seguridad se hizo uso de una herramienta muy común para escaneo de puertos como lo es **Nmap**. Teniendo la dirección IP del equipo con Windows 7 se hizo el escaneo de esta dirección IP a través de **Nmap** que viene ya preconfigurado en **Kali Linux.**

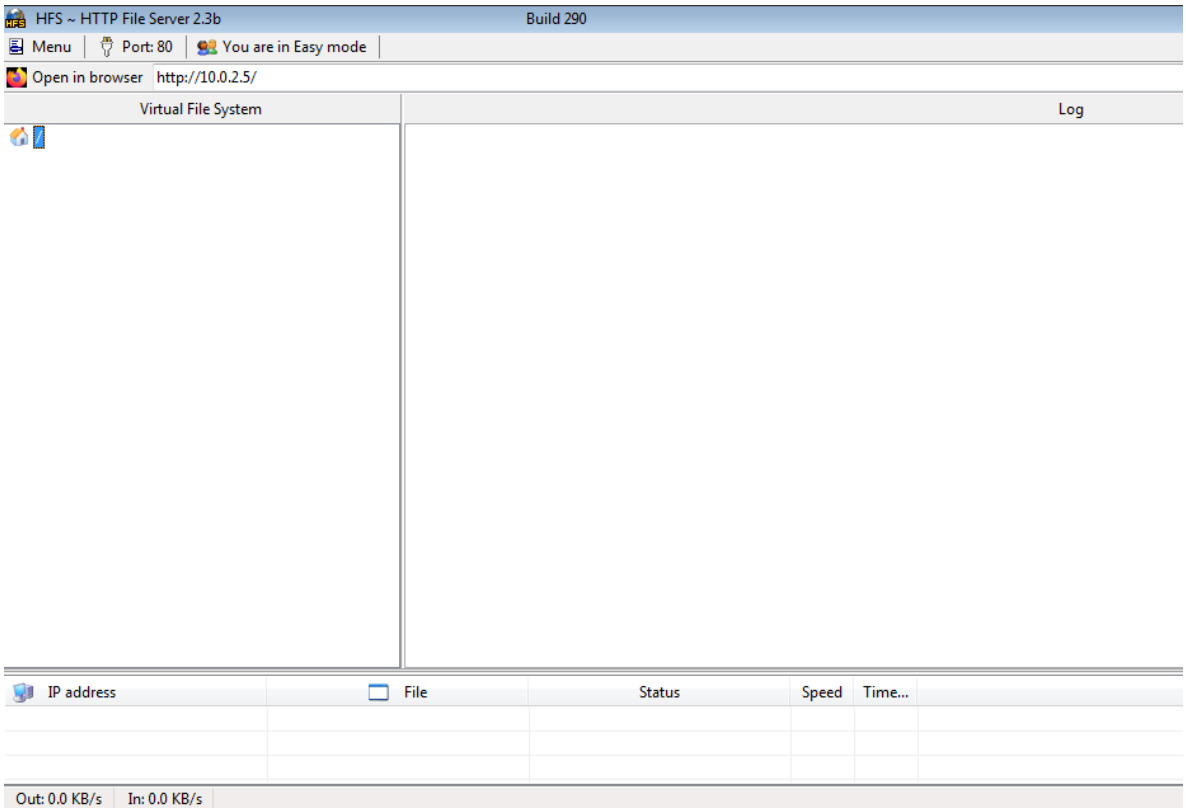
Ilustración 26: Información ipconfig Windows 7 x64



Fuente: Propia

Se puede observar que la dirección IP del equipo con Windows 7 es 10.0.2.5, lo cual al realizar el escaneo con **Nmap** permitirá saber que puertos se encuentran en estado **open.** Para esto corremos la aplicación **HFS v 2.3** en este equipo para identificar el puerto correctamente y la aplicación que está escuchando por este puerto.

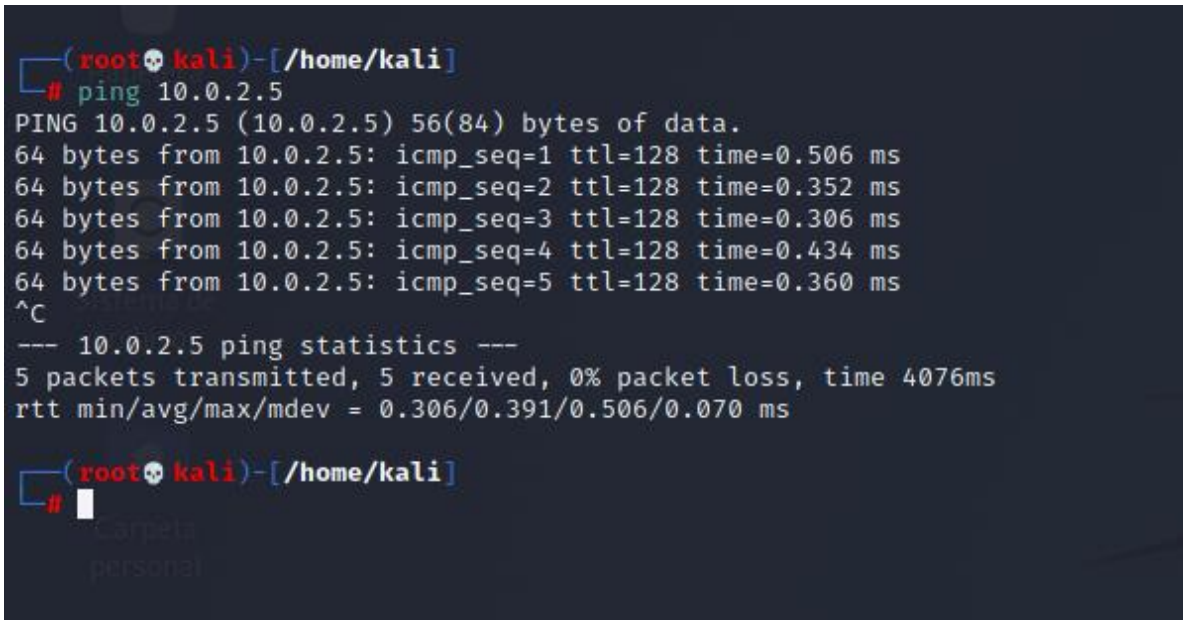
Ilustración 27: HFS en Ejecución



Fuente: Propia

Ya en la maquina con Kali Linux se puede realizar un ping para comprobar que la dirección del host sea accesible.

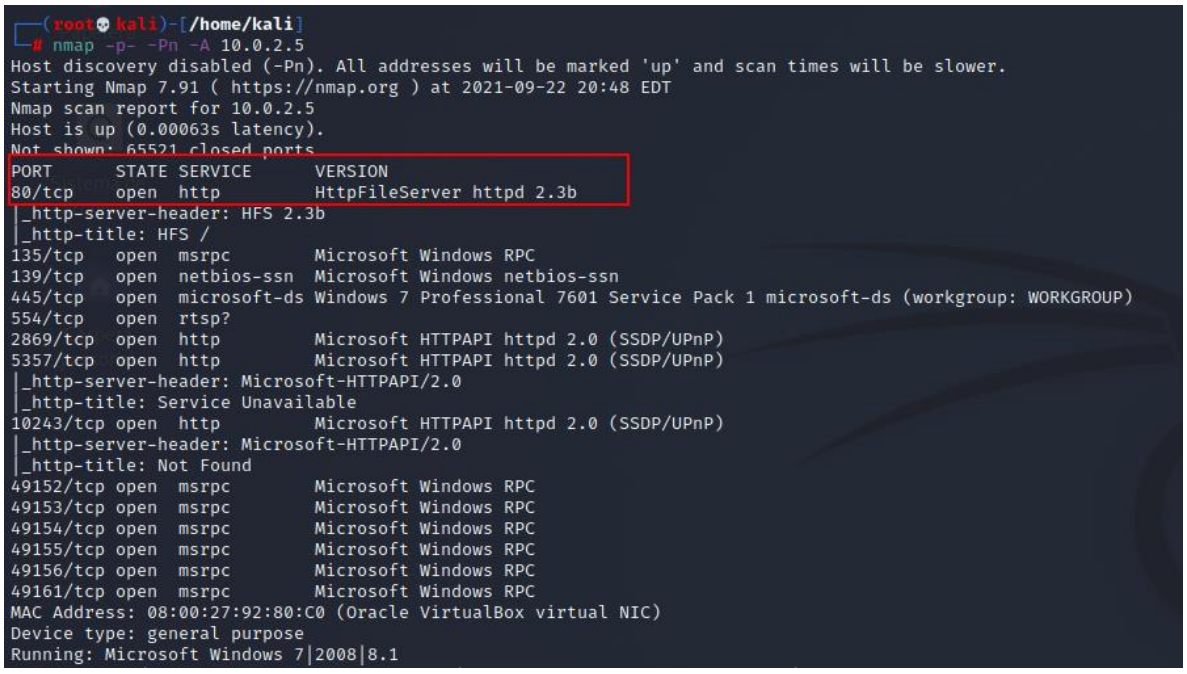
Ilustración 28: Ping desde Kali Linux



Fuente: Propia

Haciendo el uso de Nmap, se detectará que puertos están abiertos y también que aplicación gestiona ese puerto.

Ilustración 29: Nmap con el puerto 80



Fuente: Propia

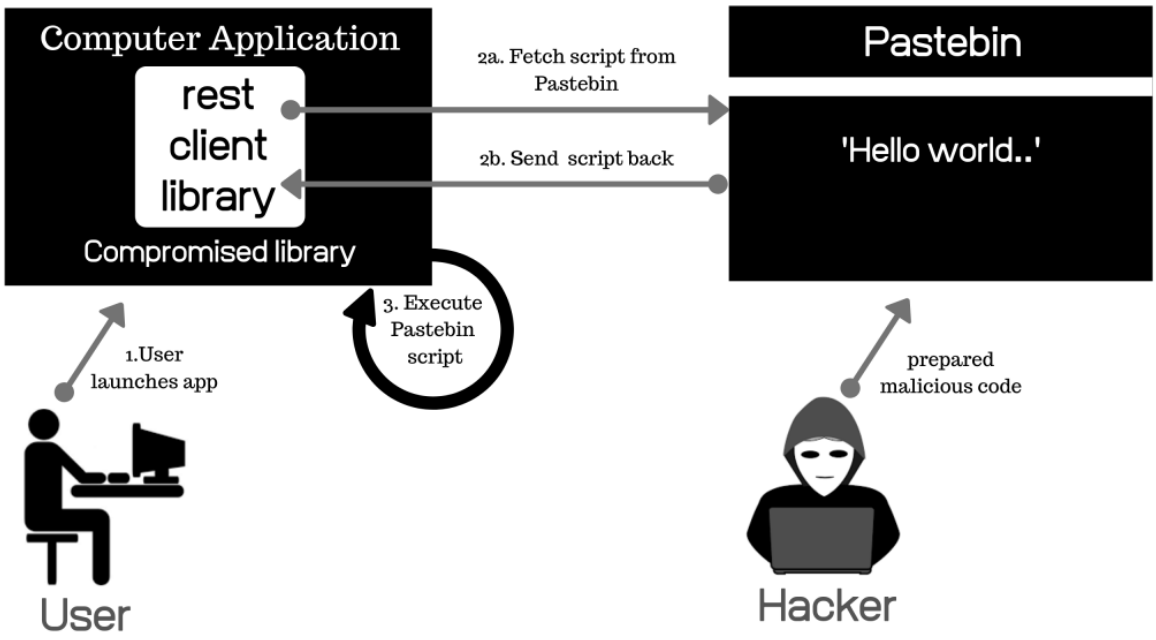
Se observa no solo que el puerto 80 (HTTP) está en estado open, sino que además muestra la aplicación que lo usa y la versión actual del software.

6.3.4 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.

Como se observa, este host maneja una versión del software que ya ha sido expuesta como una versión con vulnerabilidades críticas que pueden poner en riesgo la información que se maneja en el mismo o que se pueda ejecutar cualquier tipo de proceso con permisos de administrador, ya que al explotar esta vulnerabilidad, el atacante puede crear un usuario sin necesidad de autenticarse dentro de la misma y además darle permisos de administrador al mismo, lo cual permitiría tener control absoluto del host. En este caso se puso en práctica la explotación de la vulnerabilidad conocida como CVE-2014-6287 y con uso de herramientas de Pentesting que son las mismas que podría utilizar un atacante explotar con éxito esta vulnerabilidad.

La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (aks HFS o HttpFileServer) 2.3x antes de 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia% 00 en una acción de búsqueda. Como se observa en el siguiente gráfico.

Ilustración 30: Ataque de Shell inversa

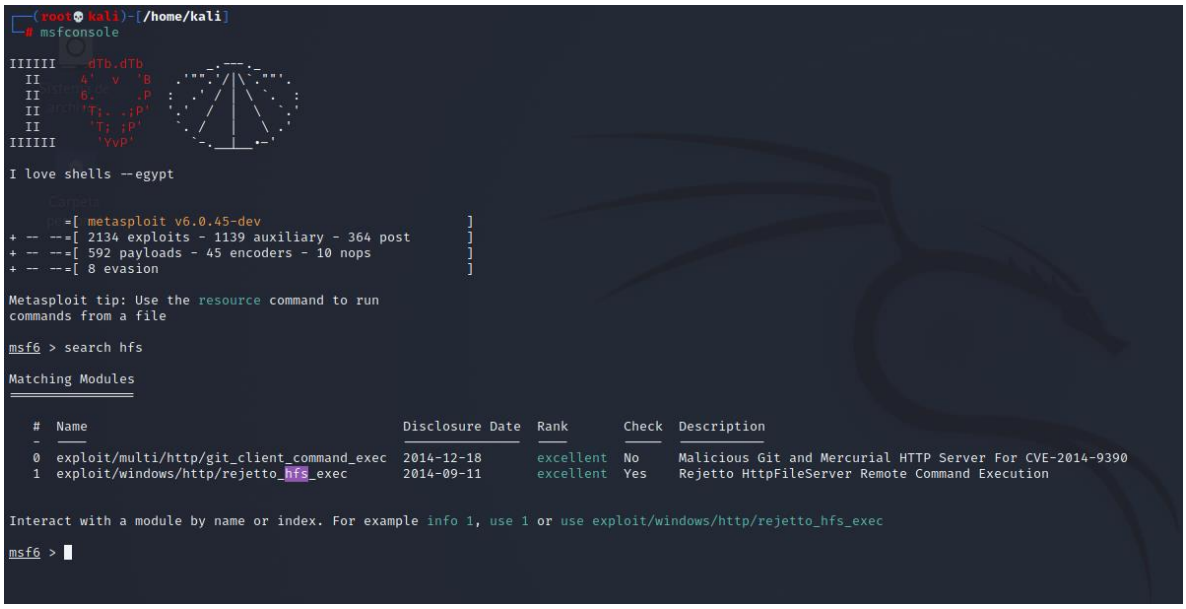


Fuente: https://blog.meterian.com/2019/08/27/vulnerability-focus-remote-code-execution-rce-attacks/

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

Sabiendo que el equipo está ejecutando una aplicación con una vulnerabilidad Alta a través del puerto 80, se muestra como fue exitoso el ataque ejecutado a través de una Shell Reversa utilizando Metasploit. Lo primero fue buscar que vulnerabilidades están asociadas a la aplicación, por lo cual se usa el comando **search hfs.**

Ilustración 31: Búsqueda de vulnerabilidades con Metasploit



Fuente: propia

En este caso se usó el exploit 1 (rejetto_hfs_exec) para explotar esta vulnerabilidad en el host víctima.

Ilustración 32: Cargando exploit en Metasploit

Fuente: Propia

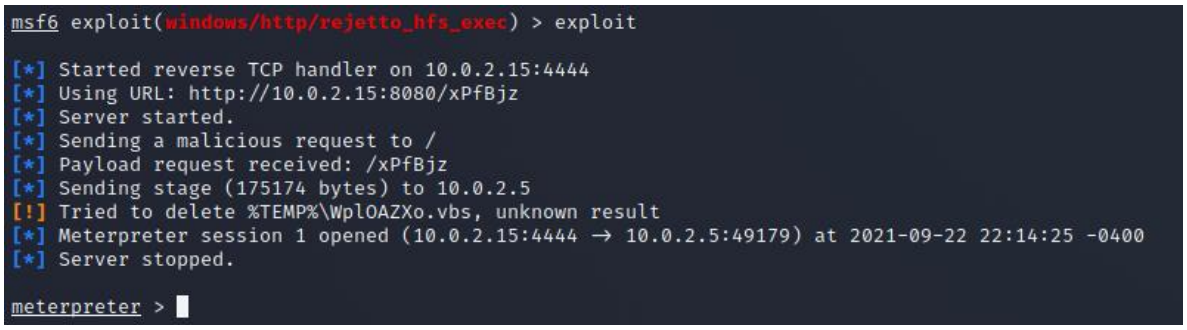
El siguiente paso es configurar las variables para la ejecución del exploit. Este exploit para ser utilizado sobre la dirección IP del equipo con Windows 7 x64 se configuran las variables **RHOST y SRVHOST** donde definimos la IP del Host y la del equipo donde se ejecutará el exploit.

Ilustración 33: Configuración variables

Fuente: Propia

Ya con estas variables configuradas, se procede a ejecutar el exploit que explotara la vulnerabilidad seleccionada.

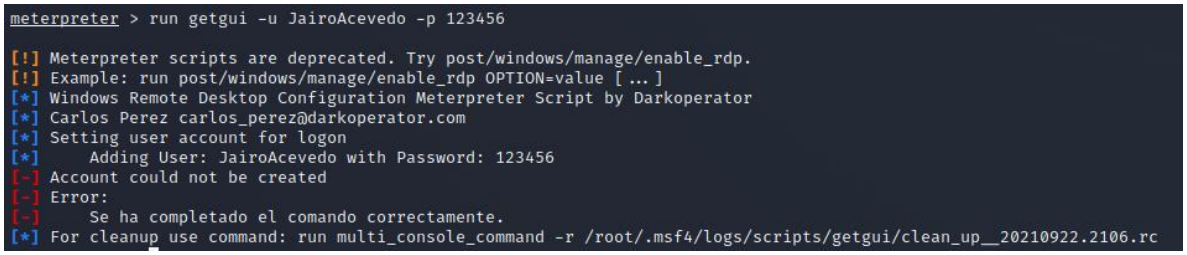
Ilustración 34: Ejecución del exploit



Fuente: Propia

Ya se tiene acceso para ejecutar el código para crear usuario, el cual quedará registrado en Windows y se podrá acceder de manera remota o en el mismo equipo.

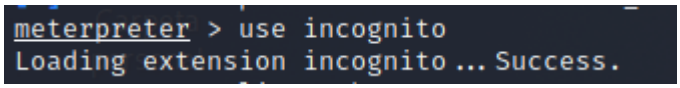
Ilustración 35: Creación de usuario



Fuente: Propia

Ahora se procede a darle privilegios de Administrador al usuario que se acaba de crear a través del comando **Incognito.** El cual nos permitirá asociar el usuario creado al grupo de Administradores.

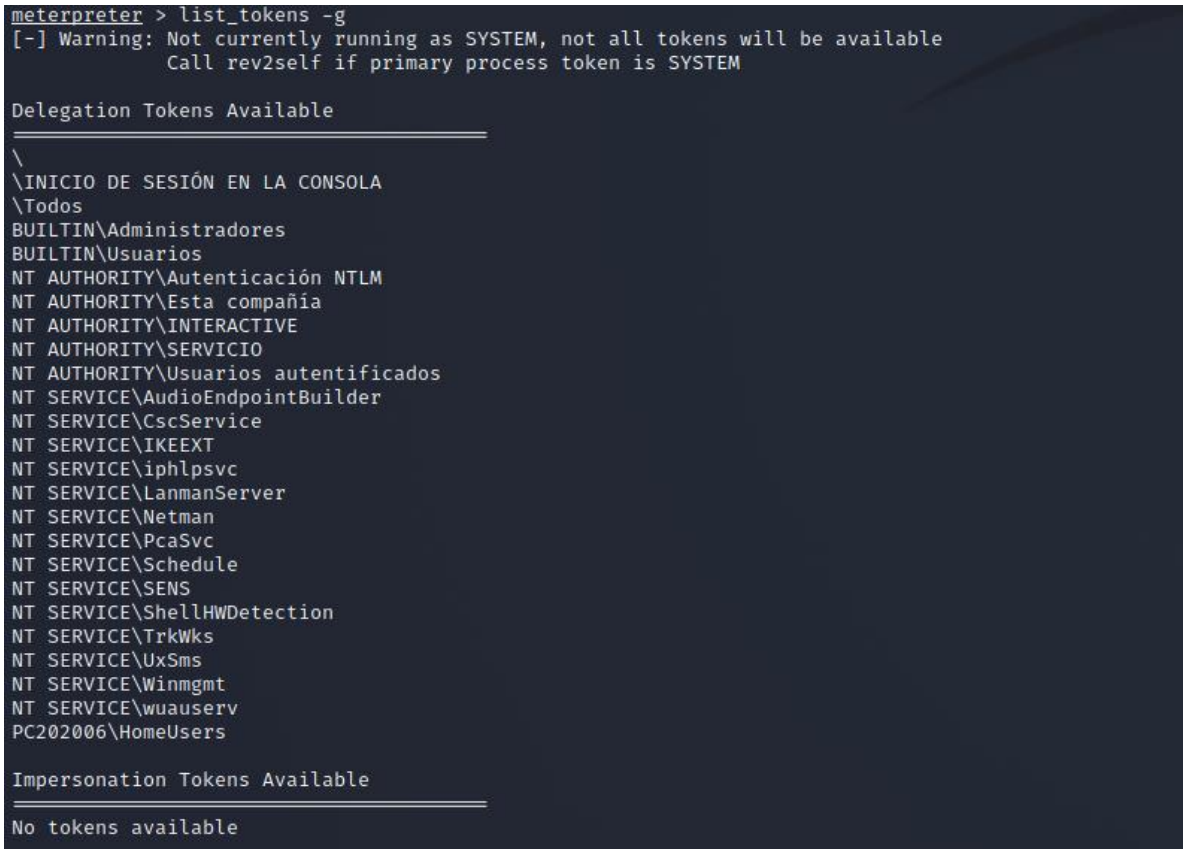
Ilustración 36: use incognito



Fuente: Propia

Para ver los grupos en este equipo, hacemos uso del comando dentro de incognito **list_tokens -g.**

Ilustración 37: Vista de grupos Windows 7



Fuente: Propia

Ahora a través del comando **add_localgroup_user** se agrega el usuario **JairoAcevedo** al Grupo de **Administradores.**

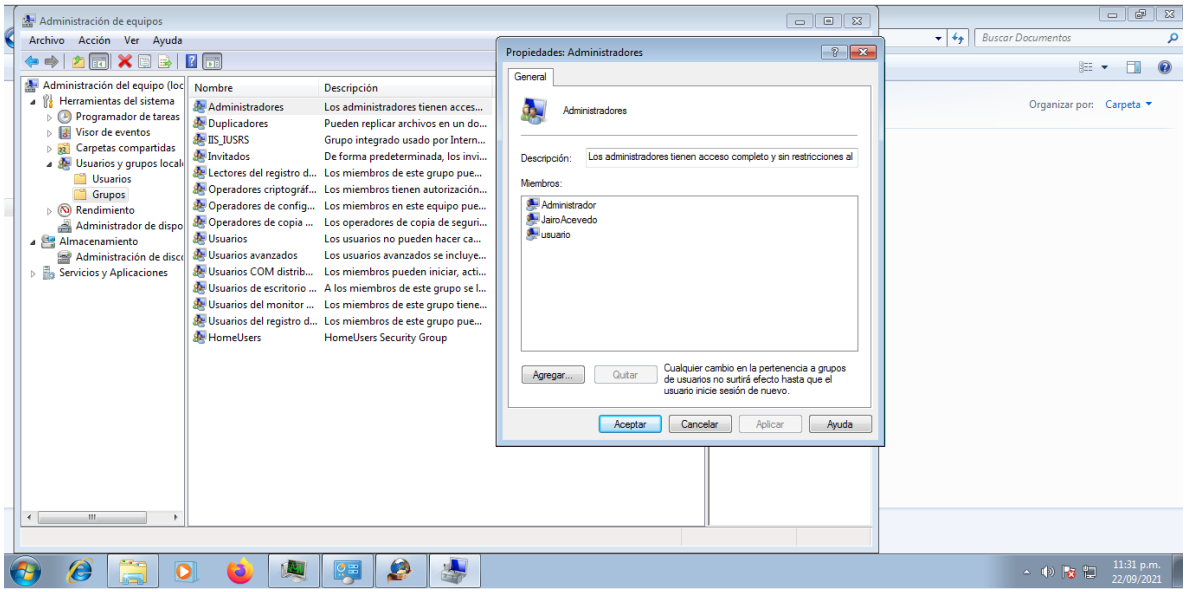
Ilustración 38: Agregar usuario a Administradores

```
meterpreter > add_localgroup_user "Administradores" "JairoAcevedo"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[*] Attempting to add user JairoAcevedo to localgroup Administradores on host 127.0.0.1
[+] Successfully added user to local group
```

Fuente: Propia

Ahora en el equipo con Windows 7 x64 se comprueba la creación del usuario **JairoAcevedo** y que está en el grupo de **Administradores.**

Ilustración 39: Creación usuario JairoAcevedo



Fuente: Propia

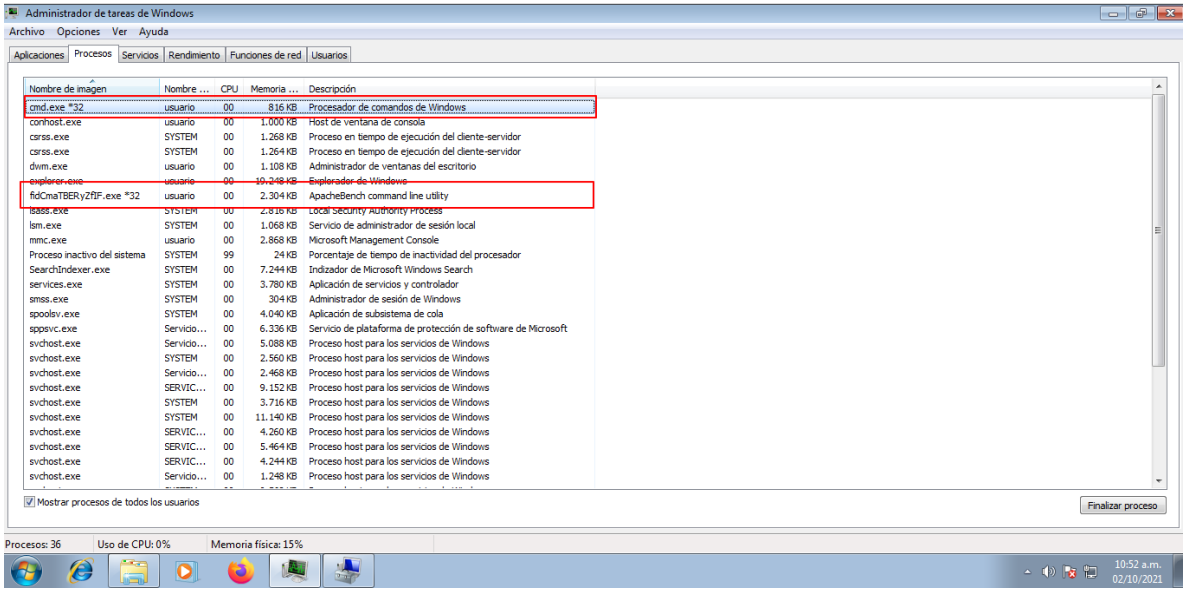
6.4 ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

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

Como una primera medida se debe evaluar que tan importante es el recurso informático que está siendo atacado y el impacto que tiene el que este recurso se retire o aislé para contener el ataque y que este no se expanda hacia la red de la empresa. Para este caso, el equipo Windows 7 X64 tiene un servicio esencial para la empresa ya que comparte información con otros equipos de la red y funciona como servidor de archivos, por lo que se debe mantener este servicio estable por lo cual se debe analizar las posibles formas de ataque que está presentando.

Como primera medida, se va a revisar el administrador de tareas a fin de buscar procesos extraños o no ejecutados directamente desde el equipo atacado.

Ilustración 40: Administrador de Tareas Windows 7 X64

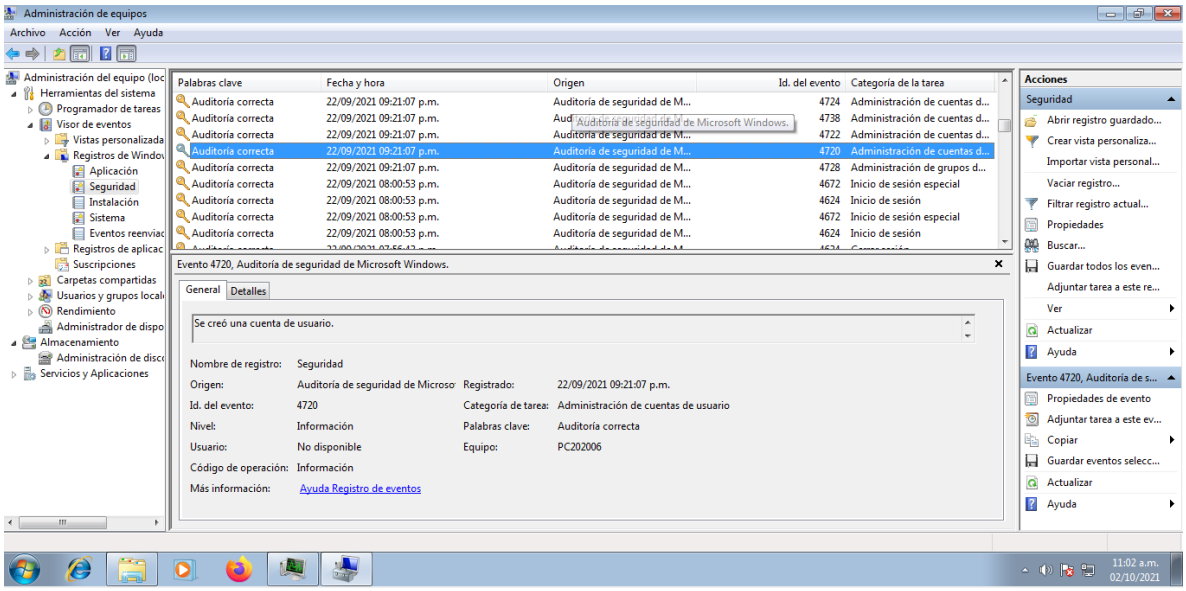


Fuente: Propia

Se puede observar que el equipo está ejecutando el proceso **cmd.exe** que equivale al **Símbolo del sistema** de Windows el cual permite ejecución de instrucciones al sistema operativo con privilegios de administrador. Otro proceso que se ejecuta es **fidCmaTBERyZftF.exe** el cual es un proceso de **Apache bench command line utility,** el cual es una línea de comandos de Apache. Estos dos procesos resultan extraños ya que se pueden correr cualquier tipo de sentencias de comandos y al no estarse ejecutando en un primer plano o con algún programa asociado es sospechoso para un posible ataque.

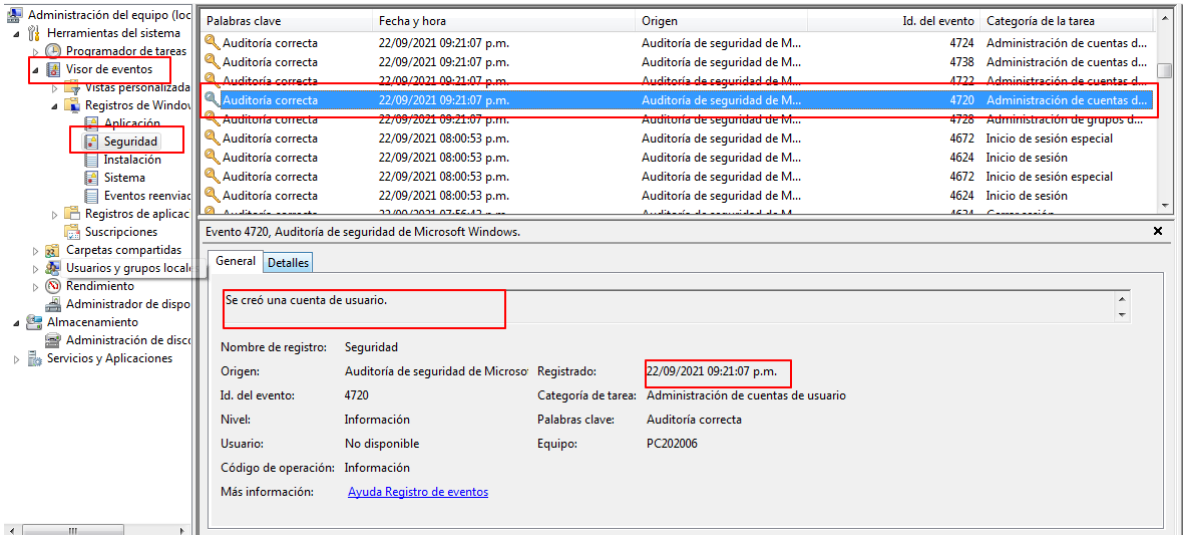
El siguiente paso al realizar el primer hallazgo es revisar los registros de eventos del sistema a fin de encontrar algún evento o actividad sospechosa que permita tener un acercamiento al ataque que se esté presentando o qué últimos cambios se han realizado de manera anormal. Para esto, se hace uso del visor de eventos de Windows que viene nativo en el sistema operativo y permitirá ver todo tipo de eventos de seguridad, aplicaciones, etc.

Ilustración 41: Visor de eventos



Fuente: Propia

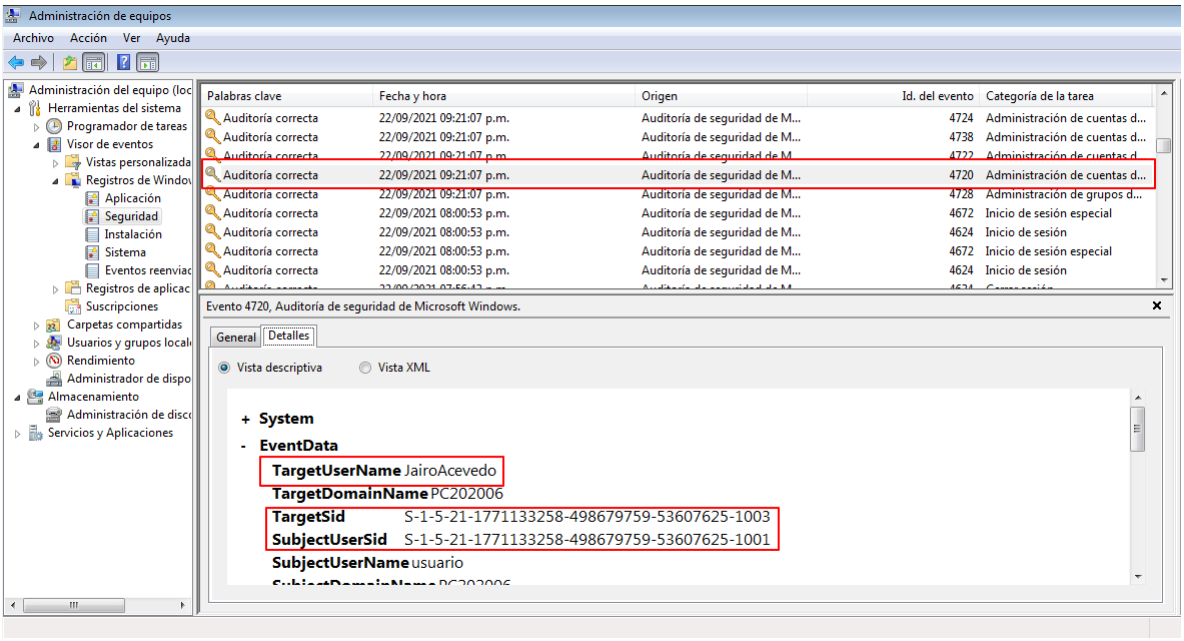
Ilustración 42: Creación de una cuenta



Fuente: Propia

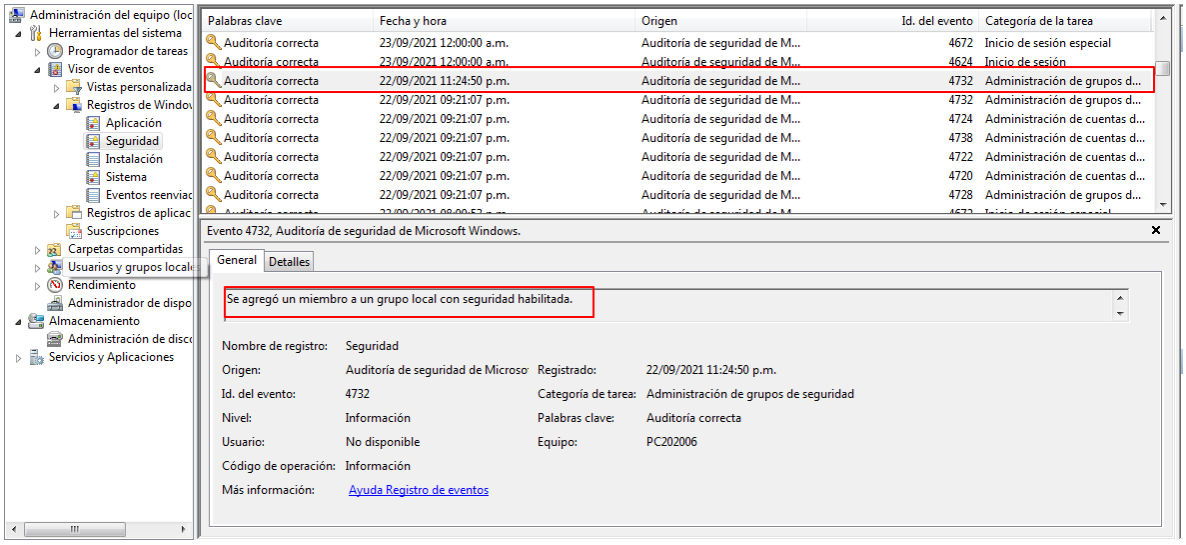
Se puede observar que se hizo la creación de una cuenta de usuario. Al revisar los detalles del evento se puede constatar lo siguiente.

Ilustración 43: Detalles del usuario creado



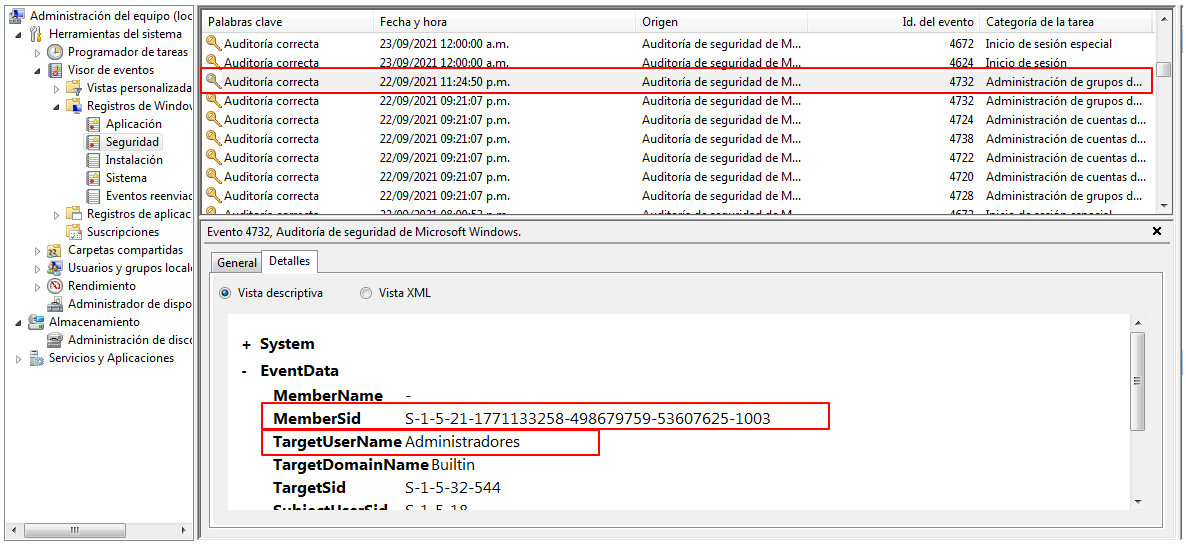
Fuente: Propia

Ilustración 44: Evento cambio de grupo



Fuente: Propia

Ilustración 45: Detalles del cambio de grupo

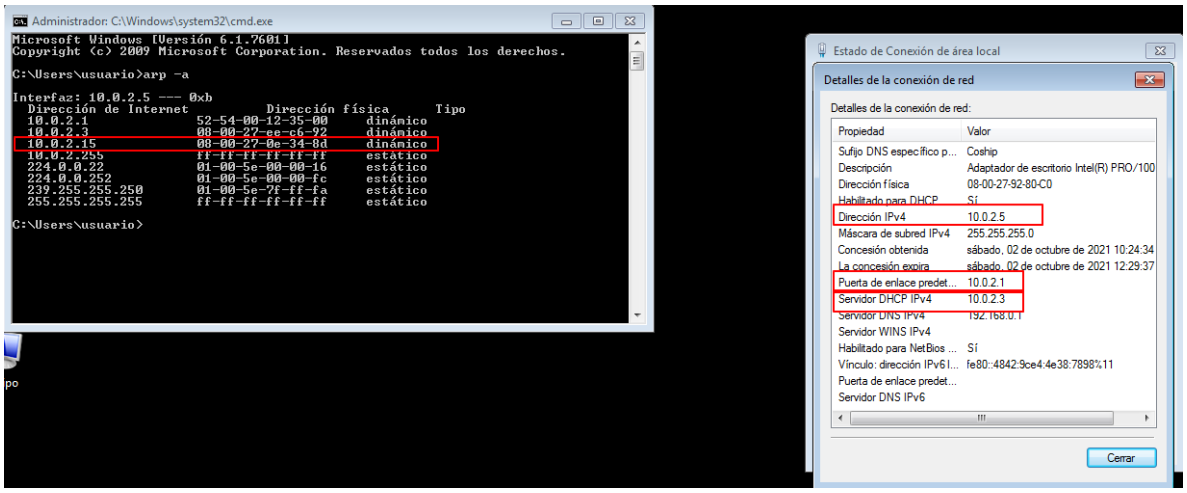


Fuente: Propia

Se observa en los detalles que se ha creado un usuario de nombre **JairoAcevedo** con el ID de usuario **S-1-5-21-1771133258-498679759-53607625-1003** el cual no está relacionado en las actividades del usuario que utiliza el equipo o de alguien de la empresa. Lo cual evidencia que se hizo la creación de esta cuenta con el fin de poder acceder al equipo. También se observaron eventos de cambio de grupo del usuario hacia el grupo **Administradores** lo cual evidencia que este usuario ya tiene privilegios de Administrador y que puede realizar cambios en la configuración y tener acceso total a la información de todos los usuarios del equipo.

Teniendo en cuenta lo anterior, se sabe que se ha creado una cuenta de usuario y agregada en el grupo local de Administradores, se indaga con el Departamento de Sistemas quienes indican que esta acción no fue realizada por esta área, lo cual aclara la sospecha de que fue de manera remota y este evento está relacionado con un ataque informático. Esto podría monitorearse en tiempo real si la empresa contara con un Sistema de Alerta de Eventos y configurada con este tipo de eventos, sin embargo, como la empresa no cuenta con esto, se deben hacer estos hallazgos de manera manual. Para seguir con la verificación del equipo, se puede hacer uso de herramientas nativas que permitan verificar si existe todavía la conexión entre el equipo victima (en este caso el equipo Windows 7 X64) y el equipo atacante. Para eso se usa la herramienta de Windows a través de línea de comando **cmd,** la herramienta nos permite ver la tabla de **ARP** de la interfaz de red del equipo donde nos muestra las direcciones IP y la dirección MAC de los dispositivos que han realizado comunicación de ARP en la red.

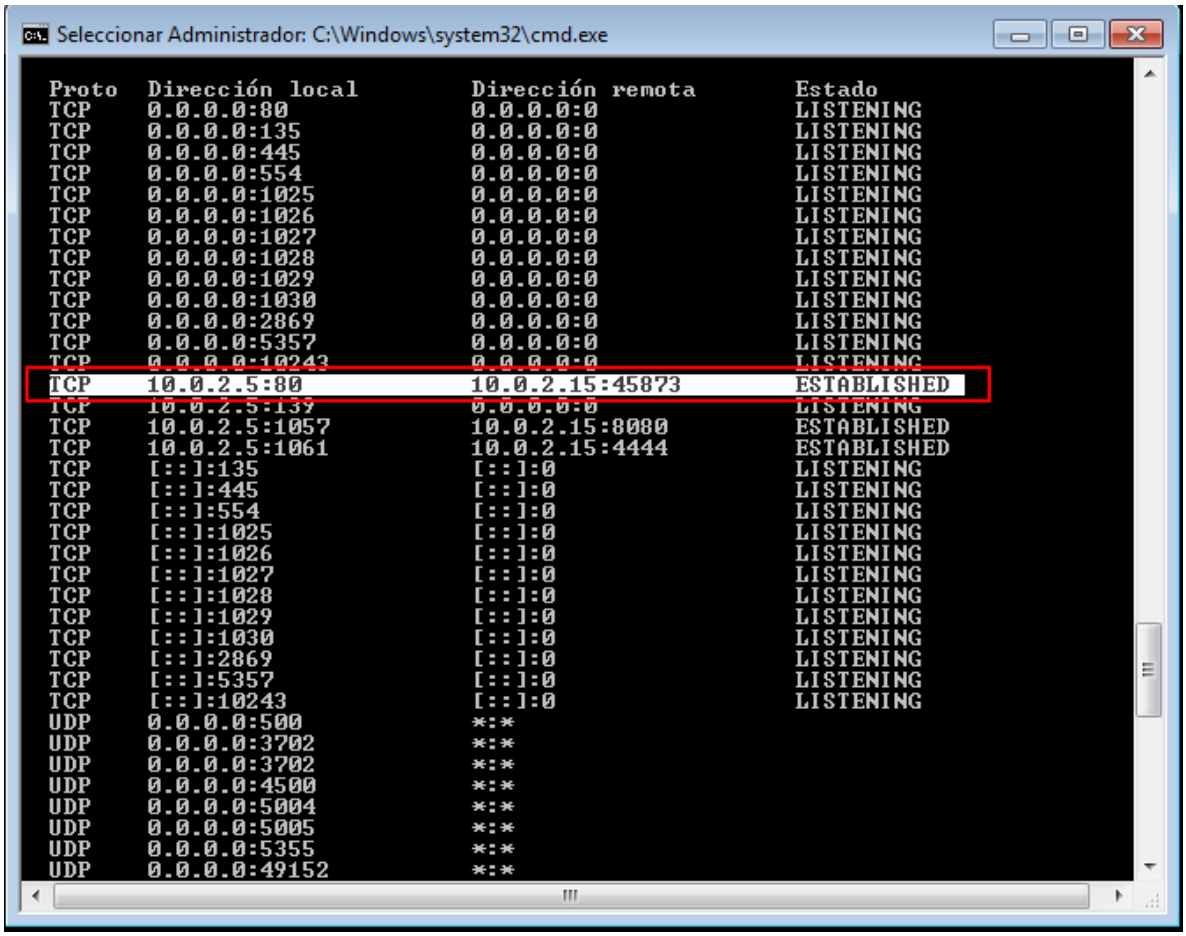
Ilustración 46: Tabla ARP Windows 7 X64



Fuente: Propia

Se puede observar en la tabla ARP que han tenido comunicación algunas direcciones IP, una ha sido la puerta de enlace (10.0.2.1), la otra es el Servidor DHCP (10.0.2.3) y una dirección IP 10.0.2.15 la cual no se reconoce en la conexión. Se hará uso de una herramienta muy útil para detectar si esta dirección tiene una conexión establecida con el equipo Windows 7 X64 y esta es netstat.

Ilustración 47: Tabla de conexiones con netstat



Fuente: Propia

Se puede observar que se tiene conexiones establecidas hacia esta dirección IP **10.0.2.15** por lo cual se deduce que esta IP está involucrada en el ataque informático.

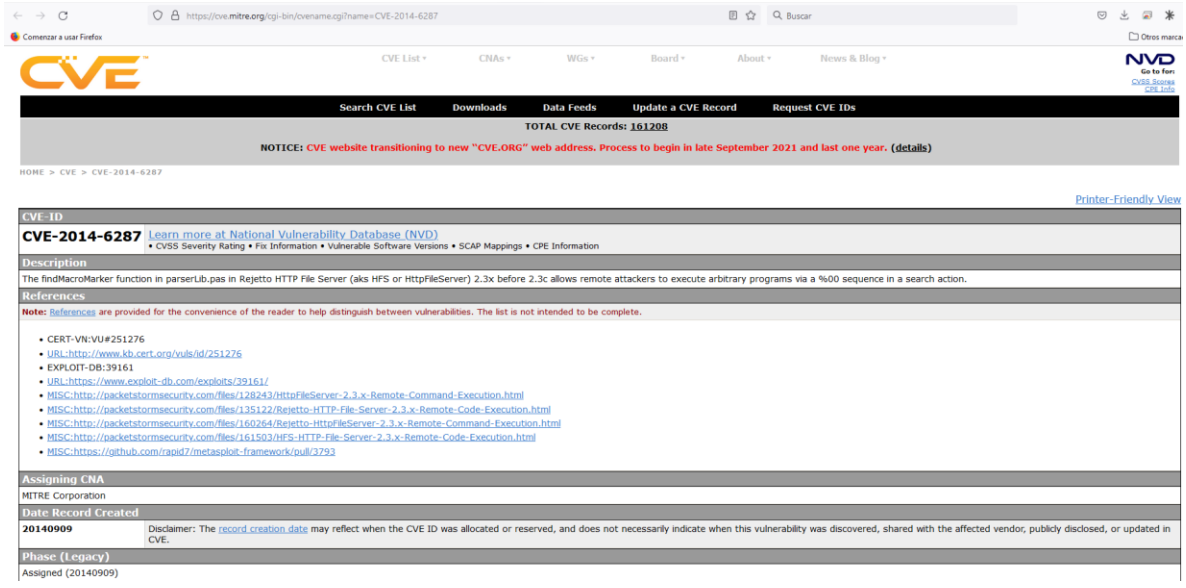
Lo que se puede evidenciar es que hay una vulnerabilidad aprovechada para ingresar de manera arbitraria al equipo y poder ejecutar procesos y comandos para acceder y controlar el equipo, todo a través del puerto 80, se puede observar que en este equipo usan un software para compartir archivos en red llamado HTTP File Sever, el cual usa el puerto 80 para compartir los archivos y el cual está en una versión vulnerable a ataques de Shell Reversa ya muy conocidos. Por lo cual como primera medida se debe actualizar el software utilizado en el equipo a una versión que ya haya corregido la vulnerabilidad, sin embargo, también se observa que el sistema operativo ya no cuenta con soporte por parte del fabricante (Microsoft) y por lo cual ya no recibe ningún tipo de actualización de seguridad que pueda parchar más vulnerabilidades que aún no se han hallado.

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

Como ya se expuso anteriormente, el equipo atacado hace uso de un software para compartir archivos con una vulnerabilidad que ya se ha expuesto en varios sitios de vulnerabilidades y cuenta con varios CVE conocidos y con exploit desarrollados para explotar esta vulnerabilidad. Por lo cual se proponen las siguientes medidas de Harderización:

- Cambiar la versión del software afectado a una versión estable que ya haya corregido esta vulnerabilidad haciendo una revisión con el proveedor de que versión es la más apropiada para seguir utilizando el servicio por otros equipos de la empresa

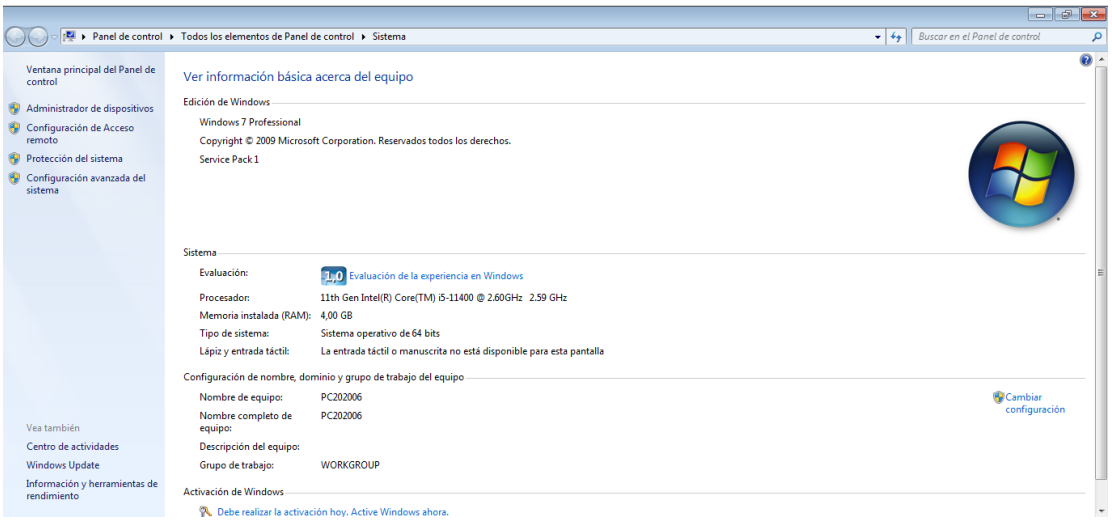
Ilustración 48: Vulnerabilidad CVE2014-6287



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

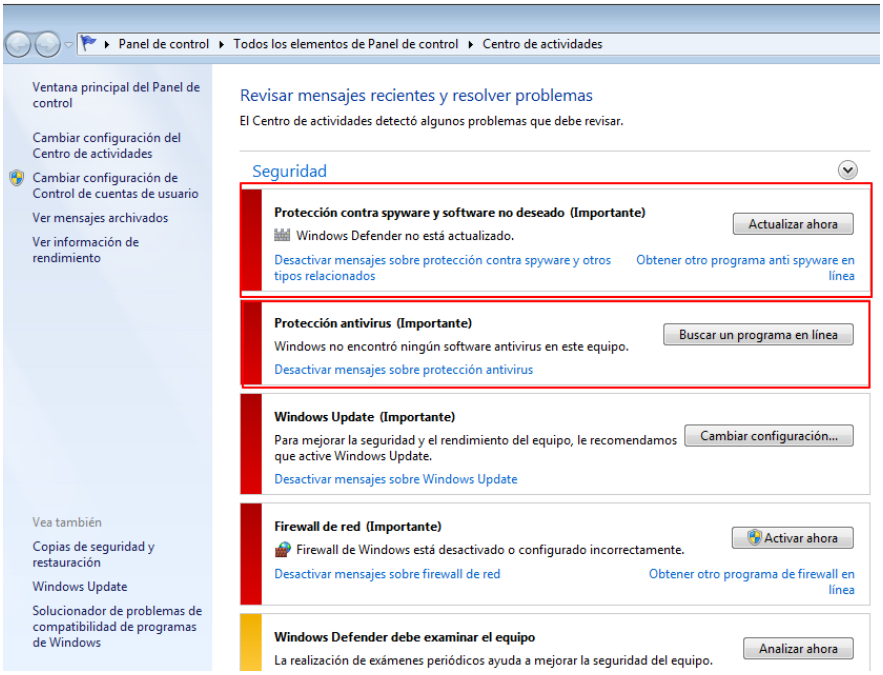
- En los hallazgos encontrados, se evidencia que el sistema operativo no cuenta con una solución de Antivirus y que la opción de Antivirus del Sistema operativo se encuentra desactualizado. Estos elementos ayudan a mitigar los riesgos de ataques de tipo Malware o de Accesos no Concedidos por lo cual una de las medidas sería optar por una solución de este tipo para así cerrar esa brecha de seguridad.

Ilustración 49: Versión de Windows



Fuente: Propia

Ilustración 50: Centro de Seguridad de Windows 7 X64

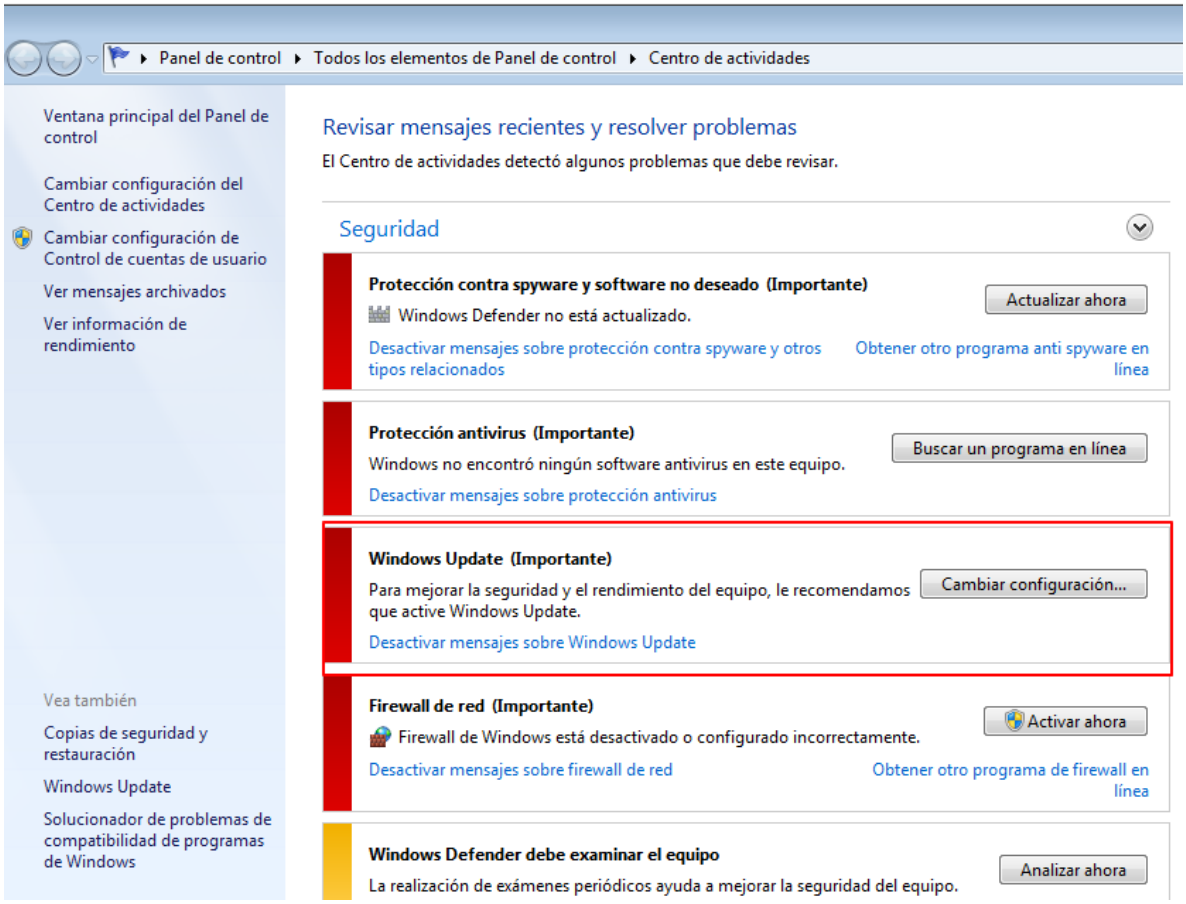


Fuente: Propia

- Se puede observar también que el sistema operativo tiene las actualizaciones automáticas deshabilitadas, lo cual no le permite tener parches de actualización de seguridad y del software del sistema operativo, lo cual puede ser un riesgo de ataque ya que existen muchas vulnerabilidades que no están corregidas y pueden ser aprovechadas por

atacantes para comprometer el sistema y la red de la empresa por lo cual esta sería una propuesta de harderización

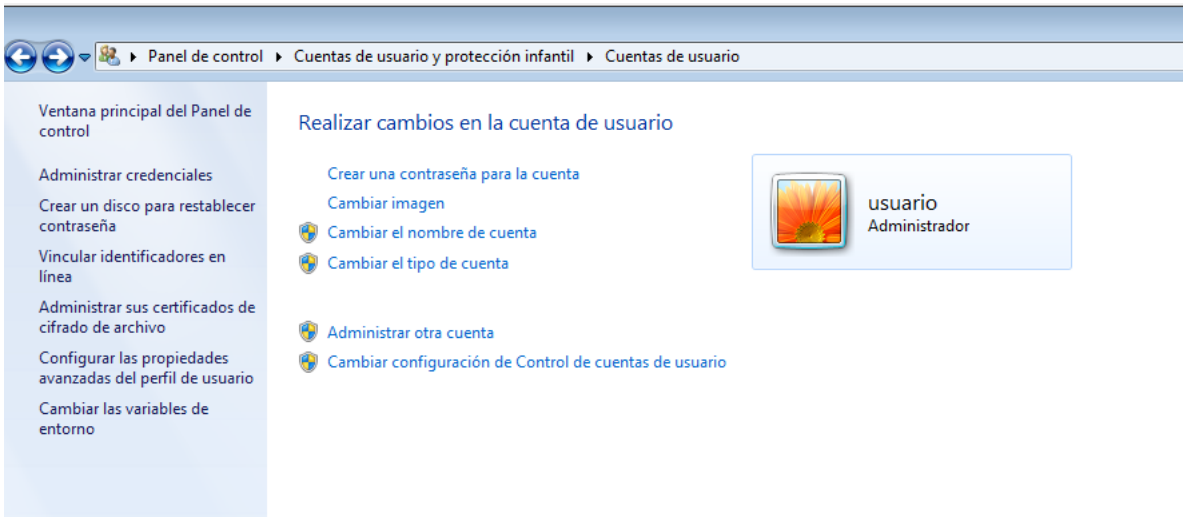
Ilustración 51: Windows Update desactivado



Fuente: Propia

- A nivel de seguridad de usuarios se observa que el usuario actual (usuario) no tiene ninguna contraseña y es un usuario local con privilegios de administrador, lo cual permite que se acceda a él por cualquier otro usuario sin ninguna dificultad y realizar cambios en el sistema. Se propone también el uso de un dominio de trabajo donde los usuarios sean administrador por un servidor principal con un control de contraseñas robusto y de cambio constante que permita asegurar que no cualquier persona pueda tener acceso a los equipos de la empresa. Además de eliminar estas cuentas locales y las cuentas de administrador sean deshabilitadas de cada equipo para evitar su uso

Ilustración 52: Cuenta de usuario



Fuente: Propia

- Hacer uso de NAS (Network Attached Storage “Almacenamiento Conectado en Red”) que permita compartir datos de manera segura en la red para no hacer uso de software que podría poner en riesgo la información por no contar con la seguridad necesaria o que tenga vulnerabilidades que puedan ser explotables

- Tener un control de Software permitido, el cual solo sea custodiado por el Departamento de Sistemas y que solo ellos puedan realizar dicha instalación conforme a las necesidades de los usuarios sin que estos puedan instalar otro software que no sea el permitido

- Tener el Firewall del Sistema operativo habilitado y funcionando que permita controlar los servicios y puertos que no son utilizados por los usuarios y los cuales funcionen como backdoors a los atacantes

- Controlar el acceso de forma remota a los equipos de los usuarios a menos que estos lo requieran para el cumplimiento de sus funciones, tener abiertos protocolos como SSH y TELNET facilitan el acceso de externos y puede desencadenar un riesgo de ataque informático.

6.4.3 ¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Tabla 3: Diferencias entre Blue Team y CSIRT

Blue Team	Equipo de Respuesta a Incidentes Informáticos
Los Blue Team se encargan de proteger a la empresa de ataques informáticos de una manera proactiva no solo conteniendo las amenazas actuales sino evaluando posibles amenazas futuras	El Equipo de Respuesta a Incidentes Informáticos son los que reciben los reportes e incidentes de seguridad, analizando la situación y dando una respuesta al incidente
El Blue Team realiza un monitoreo constante de los recursos informáticos a fin de encontrar patrones y anomalías que puedan representar un riesgo de seguridad de la información	El Equipo de Respuesta a Incidentes Informáticos realizan una acción en el momento que se presenta el incidente informático, investigando como se atacó el recurso informático, ayudar a recuperar el mismo y gestionando la vulnerabilidad detectada
Los Blue Team pueden ser recursos internos o externos de la empresa o pueden ser agentes externos contratados para la detección y corrección de vulnerabilidades	El equipo de Respuesta a Incidentes Informáticos son normalmente un área de la compañía que se encarga de gestionar los incidentes que se presentan sobre los recursos informáticos

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

Dado el contexto de lo que CIS representa, siendo una organización sin fines de lucro que busca que las empresas, gobiernos y cualquier persona que tenga acceso a la tecnología y a la información lo haga de la manera más segura posible adoptando una serie de estándares y mejores prácticas que permitan protegerse contra ataques y amenazas digitales en un mundo evolucionado y cambiante donde la información y la tecnología van de la mano. Esta organización ofrece una serie de estándares y guías para que le permitan al personal a cargo de la seguridad de la información, mitigar, contrarrestar y defenderse de cualquier amenaza que se presente a nivel tecnológico y cibernético. Todo esto mostrando por medio de ataques reales y metodologías propuestas por expertos para que estos ataques fueran contrarrestados de manera efectiva.

Por esto, mi respuesta si lo utilizase, ya que es una herramienta muy efectiva para estructurar un esquema de seguridad de la información y tener un punto de partida para tener una política de seguridad de la información para una empresa y así poder tener un plan de acción efectiva y confiable que le permita a la misma protegerse de cualquier amenaza y de paso conocer que nuevas amenazas se pueden presentar a futuro.

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

SIEM

Un SIEM es la unión de dos tecnologías como son el SIM (*Security Information Management*), y el SEM (*Security Event Management*). El SIM se encarga de administrar todo lo relacionado con la seguridad de la información y el SEM se encarga de la administración de los eventos de seguridad. Un SIEM realiza ambas tareas y realiza la recolección y almacenamiento de logs de forma centralizada para así poder mostrar eventos y detectar amenazas para así mismo dar respuesta a incidentes de seguridad en tiempo real y basándose en el análisis histórico de los eventos presentados que viene de distintas fuentes.

Un SIEM se basa en buscar dentro de todos los eventos y las tareas que se presentan en el día a día en los dispositivos de red de una empresa y de una manera eficaz y rápida contrarrestar dichos eventos inusuales para prevenir que se conviertan en una amenaza a la información.

Las principales ventajas que ofrece un SIEM son las siguientes:

- Proactividad en la resolución de incidentes de seguridad
- Rapidez en la detección de eventos e incidentes detectados
- Detección de amenazas no conocidas a través de la analítica avanzada de eventos
- Mayor rapidez al momento del análisis de las alertas generadas
- Detectar amenazas a través de logs históricos usando la analítica del dispositivo SIEM
- Garantiza la protección de la información y mejora las operaciones de la empresa
- Evalúa todos los activos de red mediante escaneo activo, monitoreo pasivo e inventarios de hardware y software
- Evalúa vulnerabilidades identificando estas vulnerabilidades por cada sistema que administra, al mismo tiempo que realiza pruebas de

vulnerabilidades a nivel de red y monitoriza de manera continua para detectar vulnerabilidades no conocidas

Un SIEM cuenta entre sus funciones principales las que se describen a continuación:

- **Agregación de datos:** este componente permite agregar los eventos de seguridad que se utilizara en los demás componentes, los cuales vienen de muchas fuentes y se debe a estos categorizar con el fin de estimar si estos deben ser indexados o no según su importancia
- **Correlación:** Vincula todos los eventos y datos relacionados entre sí para detectar posibles incidentes de seguridad reales, así como amenazas, vulnerabilidades, etc. Esto gracias a la capacidad que tiene el equipo SIEM para realizar este tipo de consultas.
- **Analítica:** Es el uso de los datos estadísticos y el método de aprendizaje automático con el que cuentan los SIEM (Machine Learning) para así identificar relaciones de datos y anomalías en eventos que no se pueden detectar inicialmente.
- **Uso de fuentes externas de tipo Threat Intelligence:** Se combinan con los datos internos recopilados, estas fuentes tienen datos relacionados con vulnerabilidades, patrones o métodos de ataque y otro tipo de indicadores maliciosos
- **Alertas:** Se configuran con el fin de buscar alguna actividad sospechosa y que esta genere un aviso cuando se cumplen ciertas condiciones y avisar por distintos medios sobre alguna eventualidad
- **Dashboards y visualizaciones:** Son las ayudas graficas que se generan en base a los datos recopilados y así facilitar la revisión de eventos relacionados con la seguridad
- **Compliance:** Sirve para automatizar la correlación de eventos que permiten la generación de informes necesarios para temas de auditoría y control de los sistemas de información
- **Retención:** Es el almacenaje de los datos por el tiempo necesario, los cuales sirven para analizar más detalladamente sobre cada actividad que se esté monitoreando
- **Threat Hunting:** Esta función es muy importante, ya que permite por medio de los datos recopilados descubrir amenazas y vulnerabilidades de manera más proactiva.
- **Incident Response:** Son las acciones que se deben tomar al momento de presentarse un incidente, proporcionando la gestión de los incidentes, así como la colaboración y cambio de conocimiento sobre los mismos haciendo que este proceso sea más eficaz y al mismo tiempo ágil

- **Automatización SOC:** Denominado como SOAR (Security Orchestration, Automation and Response), es la parte que se integra con otros appliance de seguridad por medio de APIs y así crear playbooks y workflows de manera automática ante determinados eventos

6.4.6 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.

- **DMZ (Desmilitarized Zone):** es un tipo de red LAN aislada, la cual cuenta con servicios que los provee solo hacia la red externa, sin que haya una conexión directa con la red interna, es decir, tanto la red externa como la interna pueden tener acceso a la DMZ; pero la DMZ solo puede tener acceso a la red externa. Para que estos segmentos queden debidamente separados, es necesario que entre ellos se coloque un Firewall para separarlos. Normalmente los equipos que se colocan en una DMZ son equipos servidores que proporcionan servicios de carácter público como son Servidores Web, DNS, Exchange o Servidores de Correo, FTP y/o SFTP.

  Los componentes de una DMZ son normalmente los siguientes:

  - Una red Externa WAN: la cual normalmente se trata de una conexión a Internet
  - Uno o dos Firewall dependiendo de la arquitectura que se desee usar en la DMZ
  - Una red interna en la cual se alojarán los servidores o equipos de la DMZ
  - Una red interna LAN donde estarán los hosts de la red LAN a la cual no tendrá acceso la DMZ.

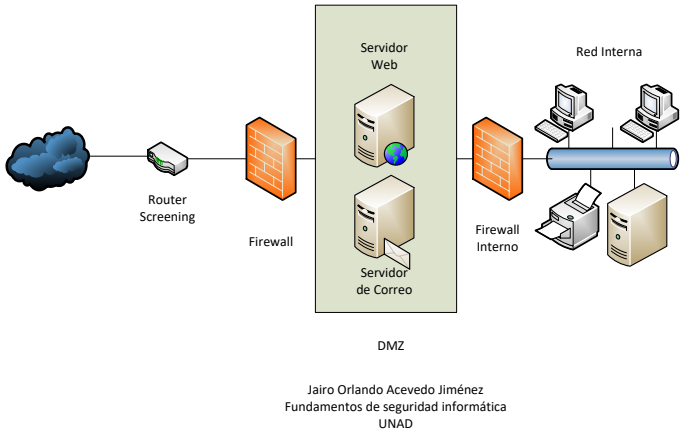
  Las arquitecturas del Firewall de una DMZ se pueden clasificar de la siguiente forma:

  - **Firewall Dual-Homed:** cuenta con dos interfaces de red, las cuales usa una para la red externa que va a un router y la otra para la red interna en la cual no permite el paso de paquetes IP, actuando como un servidor proxy en caso de que un host de la red interna quiera conectarse a un servicio externo.
  - **Firewall Multi-homed:** este cuenta con más de dos interfaces de red, lo cual le permite conectar varias redes. Es muy útil si una empresa necesita usar varias DMZ para aislar diferentes servicios o servidores.
  - **Screened Host:** cuenta con un router o enrutador perimetral al cual lo conecta directamente a la red interna. Este router recibe el tráfico de

red de internet y por medio de filtrado de paquetes, para luego enviarlo al Firewall y este se encarga de enviar los paquetes permitidos a la red.

- **Screened Subnet:** es una reforma de seguridad a la arquitectura Screened host, donde hay dos Firewalls. Uno de ellos protege los datos que entran a la DMZ, pero en vez de enviar los paquetes a la red interna, van a otro Firewall que filtra el tráfico hacia esta red.

Ilustración 53: Estructura de una DMZ



Fuente: Propia

- **Honeynets:** Una honeynet consiste en una red de equipos honeypots los cuales sirven de laboratorio para determinar los blancos de ataque de los blackhat. Es bastante versátil, ya que permite interactuar con varios sistemas en simultáneo.

  Los componentes para la creación de una honeynet se describen a continuación:

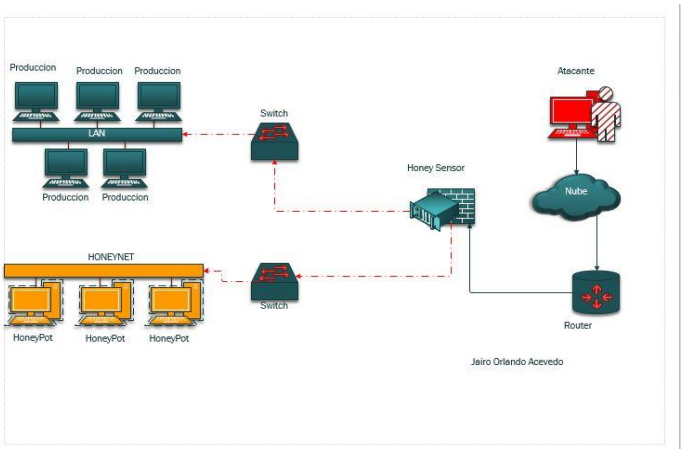
  - **Control de Datos.** Con el objetivo de evitar ataques a través de la misma, esta debe tener control sobre el flujo de datos asegurando que este tenga permisos casi totales, aunque esto implique algún nivel de riesgo. Una forma de especificar qué enfoque de control sobre esta red es la de montar un sistema de DID (Defense In Depth) el cual va por capas.

  - **Captura de Datos.** Las amenazas que se detectan sobre la honeynet deben ser registradas para llevar un seguimiento que permita su análisis posterior. Este proceso debe llevarse a cabo bajo cautela para que el atacante no note que el objetivo está siendo una honeynet, al

igual que el componente de control de datos, es necesario que esta información pase por varios mecanismos de control para registrar estos eventos. Almacenándose en capas, a las cuales se le designaran un entorno independiente de equipos honeypots.

- **Análisis de Datos.** Este componente se basa en la conversión de los datos recogidos en datos vitales que permitan detectar características y esquemas comunes de los ataques. En este punto todo dependerá del tipo de información y de las necesidades que maneje cada entidad.

Ilustración 54: Diagrama HoneyNet



Fuente: Propia

- **Firewall UTM (Unified Threat Management):** Es un equipo o dispositivo encargado de reunir muchas funciones de seguridad y en tiempo real proteger a la red de las amenazas que existen y puedan existir en una red en la actualidad. Haciendo un interfaz entre Hardware y Software y de acuerdo a la tecnología vigente en seguridad de red, este dispositivo es capaz de detectar y combatir amenazas que se puedan encontrar en contenidos de correo electrónico, gusanos, intrusiones, sitios web maliciosos y toda amenaza que pueda provenir del tráfico de red.

  En este punto se debe hablar de que tan importante sería la implementación de una UTM a una organización, para esto se debería pensar si es más factible que cada uno de los servicios que presta una UTM fuera descentralizado y se destinara un servidor o equipo para cubrir cada una de estas áreas de seguridad, seguramente el resultado sería que se tendrían muchos dispositivos que generarían costos y, además sobre cargarían la red

y los dispositivos estaría trabajando en un solo servicio que a largo plazo terminaría subvalorando el rendimiento del equipo.

Por cuestiones de costo se podría decir que es muy viable implementar un sistema de UTM, pero también se debe mirar la cuestión de que al estar centralizada toda la seguridad en un mismo punto, se debe contar con un dispositivo de hardware que tenga los recursos suficientes para lograr mantener esta seguridad siempre vigente y actuar en tiempo real como debe ser. Otro aspecto para resaltar de una UTM es que también tiene la funcionalidad de actuar como Firewall, un firewall realiza el filtrado del tráfico de la red para enviarlo hacia la red interna de la empresa. Sin embargo, un problema de unificar todos estos servicios de seguridad es que todos los sistemas de protección como antivirus, antimalware, firewall, es que minimizan el uso de recursos entre ellos para poder trabajar todos al tiempo y en el mismo dispositivo o software, lo cual hace que no todas sus características se puedan usar de manera completa, como lo sería si cada servicio estuviera en un dispositivo separado. Esto no es conveniente si la red de la organización maneja servicios externos y que estos manejen mucho tráfico en la red, y que generaría un exceso de trabajo en el dispositivo UTM haciendo que pueda llegar a colapsar uno o todos los servicios.

7 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM

Se debe tener en cuenta que para que este tipo de estrategias tenga el éxito esperado, ambos equipos deben tener presente su rol en la investigación para así conseguir el objetivo principal de esta estrategia, la cual es evaluar si los controles o mecanismos de seguridad de la información y ciberseguridad son lo suficientemente efectivos para prevenir, contener y controlar un riesgo informático y/o se presente un ataque informático, se tengan claros los lineamientos tanto técnicos como organizacionales para que este ataque no genere un impacto negativo importante para la empresa. El Red Team debe estar coordinado con el Blue Team para lograr poner a prueba la efectividad de los controles que pueda tener la empresa en materia de ciberseguridad y si no los tiene que sea el primer paso para construir esta política que es muy importante para las empresas de hoy, aplicando todas las técnicas y habilidades para que se pueda montar el escenario necesario para ver qué puntos débiles o vulnerabilidades tiene la empresa y como fortalecerlos y al tiempo probar si los puntos fuertes lo pueden ser más. Tomando en cuenta este propósito, esta estrategia es muy completa ya que se analiza tanto la parte técnica y como un atacante ve a la empresa como un blanco de ataque y que vulnerabilidades encuentra realizando un análisis de esta, como la empresa respondiendo a dicho ataque con estrategias coordinadas y supervisadas por profesionales que usaran los medios que se tengan al alcance para que este ataque no se materialice.

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

Como principal recomendación, se debe concienciar a las empresas de la importancia que ha tomado la información digital para todo el mundo y que la información se ha convertido en uno de los activos más importante para las mismas. Aún existen empresas que no cuentan con un modelo de seguridad de la información o que aún no lo han implementado en su totalidad viendo que las amenazas digitales existen, pero no le dan la importancia que se necesita para estar preparados por si llegan a materializarse.

Al igual que la seguridad de la información, la seguridad informática debe ser tenida muy en cuenta en un modelo estratégico tanto para la organización como para cada una de las áreas que la conforman. Es por eso que se debe tener dentro de la empresa, un área encargada de analizar cómo se encuentra la empresa a nivel de ciberseguridad e ir auditando periódicamente si estas estrategias cumplen con el cometido de proteger la información. Realizar pruebas de vulnerabilidades e informar a la alta gerencia y a todo el personal necesario de los hallazgos encontrados y los puntos a mejorar ya que no hay una estrategia que controle y elimine las amenazas que existen sobre la información.

Contar con el personal técnico capacitado para hacer frente a amenazas potenciales que se puedan presentar, haciendo un control de vulnerabilidades y como poderlas mitigar o eliminar de manera segura y con el menor coste para la empresa.

En la parte técnica, mantener los sistemas operacionales y todo el software vital para la empresa con actualizaciones constantes y parches de seguridad que el fabricante produzca para así reducir el riesgo de que se materialice una amenaza. Evitando el uso de software que ya sea obsoleto o que el fabricante ya no de ningún tipo de soporte o que ya haya terminado su tiempo de vida, ya que es en este software donde se concentran la mayoría de los ataques y amenazas que son aprovechadas por los ciberdelincuentes.

Tener un software de antivirus es de vital importancia para las empresas ya que la muchos de los ataques que se presenta en las empresas se presentan por malware o código malicioso que un antivirus puede detectar, al igual este debe contar con las actualizaciones de su base de datos para evitar que sea obsoleto antes amenazas nuevas.

A nivel de red, implementar medidas como uso de red segmentada por áreas que permita aislar las mismas y que toda la información sea accesible para toda la empresa. El uso de DMZ permite aislar toda la infraestructura de Data Canter en una zona de acceso restringido y que solo administradores y personal autorizado pueda tener acceso a estos recursos.

Tener dentro de los recursos informáticos, herramientas de IDS e IPS que detecten y hagan frente a ataques que se estén presentando en tiempo real y contenerlos de manera eficaz antes que afecten la información sensible o los recursos informáticos de la empresa

9 CONCLUSIONES

La seguridad de la información es un aspecto muy importante para evaluar al momento que las organizaciones se dan a conocer. Para muchas empresas tienen la necesidad de darse a conocer a los clientes y ofrecer su portafolio de servicios y bienes de la forma más eficiente, para esto se han tenido que ver cada vez más forzados a interconectar sus redes privadas a la red mundial es decir internet. ¿Es ahí donde se empieza a pensar que se está haciendo para que la información sensible para las empresas que cada vez se está viendo más atacada por personas externas o en muchos casos internas a la organización este protegido de los Hackers que quieren obtener o modificar esta información con fines delictivos?

En el desarrollo de este informe se llegan a las siguientes conclusiones

- Las leyes en Colombia están reguladas ya para detener algunos delitos que se cometen por medios informáticos. Sin embargo, debe haber un estudio de la ley 1273 de 2009 en algunos artículos ya que para algunos de estos protegen más a las empresas que a las personas naturales o existen algunos vacíos que aplicarían solo a las empresas.

- Las certificaciones en seguridad informática han tenido una gran evolución en el mundo, ya que cada vez las empresas entre sus roles principales esta que se cuente con algún profesional que ya cuente con alguna de estas. Sin embargo, cada certificación tiene un enfoque y un área que la caracteriza por lo cual siempre se necesitara un profesional que reúna lo mejor de todas ellas.

- La estrategia de Red Team y Blue Team es una de las más completas que existen para evaluar la seguridad de una empresa, ya que permite emular un ataque real y al mismo tiempo que estrategias y procesos técnicos se pueden ejecutar para enfrentar estos ataques de manera eficaz para así poder cambiar aspectos y medir la efectividad de otros frente a las amenazas.

10 BIBLIOGRAFIA

Congreso de la República. Ley 1273 de 2009 [En línea] Disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html)

Congreso de la República. Ley 1581 de 2012 [En línea] Disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html)

Ministerio De Comercio, Industria Y Turismo. Decreto 1377 de 2013 [En línea] Disponible en: (http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf)

Méndez, Yohanna & Rojas, Carmen, "Análisis jurisprudencial de la ley 1266 de 2008 (Ley hábeas data) en Colombia" [En línea] Disponible en: (http://www.pensamientopenal.com.ar/system/files/2014/07/doctrina39446.pdf)

Erazo Bastidas, Carlos Guillermo "Identificación de vulnerabilidades de los servicios tecnológicos de la unión de cooperativas de ahorro y crédito del norte aplicando la práctica de Pentesting (Bachelor's thesis)" [En línea] Disponible en: (http://repositorio.utn.edu.ec/bitstream/123456789/7396/1/04%20ISC%20447%20TRABAJO%20DE%20GRADO.pdf)

Zhou, A. T., Blustein, J., & Zincir-Heywood, N, Improving intrusion detection systems through heuristic evaluation. EN Canadian Conference on Electrical and Computer Engineering 2004 (3: 2-5, mayo, 2004: Niagara Falls, ON, Canada). pp. 1641-1644. [En línea] Disponible en: (https://ieeexplore.ieee.org/abstract/document/1349725)

Esteban, Samuel, "Metasploit: Atacando a Windows. Backtrack Academy" [En línea] Disponible en: (https://backtrackacademy.com/articulo/metasploit-atacando-a-windows)

Daza Castillejo, Miguel Angel, "Capacidades técnicas, legales y de gestión para equipos blueTeam y redTeam." [En línea] Disponible en: (https://repository.unad.edu.co/bitstream/handle/10596/37153/77032013.pdf?sequence=1&isAllowed=y>).

OLIVARES SERRANO, JAVIER, librería ENI, "Seguridad informática" [En línea] Disponible en: (https://books.google.com.co/books?id=4X32wbgtNfUC&pg=PA244&lpg=PA244&dq=exploit+y+su+utilidad&source=bl&ots=PrGTxlHfOk&sig=ElysJRYJvKRgUyOaeJVqwRKnDVQ&hl=es&sa=X&ved=0ahUKEwjo24e14dTaAhXS3VMKHc-8DX04ChDoAQglMAA#v=onepage&q=exploit%20y%20su%20utilidad&f=false)

Enríquez López, Mayerly Rocio, “Capacidades técnicas, legales y de gestión para equipos blueteam y redteam” [En línea] Disponible en: (https://repository.unad.edu.co/bitstream/handle/10596/40285/mrenriquezl.pdf?sequence=1&isAllowed=y)

Sanín Restrepo, Jaime, “El secreto empresarial: concepto teórico y fallas a la hora de alegar su violación ante la Superintendencia de Industria y Comercio” [En línea] Disponible en: (https://repositorio.uniandes.edu.co/bitstream/handle/1992/47630/secreto-empresarial.pdf?sequence=1)

Serna-Montoya, Edgar, “Ley 842 de 2003 sobre Ética Profesional” [En línea] Disponible en: (https://www.funlam.edu.co/revistas/index.php/lampsakos/article/view/753/722)

Baquero Rozo, Cesar Efren, “Naturaleza jurídica del consejo profesional nacional de ingeniería–COPNIA-y el ejercicio de la inspección y vigilancia de la ingeniería, sus profesiones afines y sus profesiones auxiliares a la luz de la Constitución Política de 1991” [En línea] Disponible en: (https://repositorio.uniandes.edu.co/bitstream/handle/1992/47630/secreto-empresarial.pdf?sequence=1)

Peñarredonda, José Luis, “Detrás de Buggly: la historia de la fachada Andrómeda” En: Enter.co. Noviembre-diciembre, 2015 [En línea] Disponible en: (https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/)

WhiteSource Vulnerability Database. WhiteSource [En línea] Disponible en: (https://www.whitesourcesoftware.com/vulnerability-database/CVE-2014-6287)

Khan Z., Afrozulla y Balajinarayan B, “A Study on Metasploit Payloads. International Journal of Cyber-Security and Digital Forensics” [En línea] Disponible en: (https://link.gale.com/apps/doc/A632092863/AONE?u=anon~58eb12b4&sid=googleScholar&xid=5eebd9c4)

Unir. Área de Ingeniería y Tecnología, “Red Team, Blue Team y Purple Team” [En línea] Disponible en: (https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/)

Alberts, Chris. y Dorofee, Audrey y Killcrece, Georgia y Ruefle, Robin y Zajicek, Mark, “Defining incident management processes for CSIRTs: A work in progress” [En línea] Disponible en: (https://apps.dtic.mil/sti/citations/ADA453378)

M. (s. f.). What are the CIS Controls? | Implement the CIS Critical Security Controls with ManageEngine. ¿Qué son y cómo implementar los Controles de Seguridad Crítica CIS? Recuperado 2 de octubre de 2021 [En línea] Disponible en: (https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html)

Veloy Mora, Angel Luis, “Ventajas e Implementación de un sistema SIEM” [En línea] Disponible en: (http://openaccess.uoc.edu/webapps/o2/handle/10609/107546)

Murphy, Jack J, “The Demilitarized Zone as an Inforamtion Protection Network” [En línea] Disponible en: (https://www.igi-global.com/viewtitlesample.aspx?id=18389&ptid=380&t=the+demilitarized+zone+as+an+inforamtion+protection+network)

Vinueza Jaramillo, Tatiana. Alexandra, “Honeynet virtual híbrida en el entorno de red de la Universidad Técnica del Norte de la ciudad de Ibarra” [En línea] Disponible en: (http://repositorio.utn.edu.ec/handle/123456789/1058)

Madera Salgado, Luis Enrique, "IMPLEMENTACIÓN DE UN UTM (UNIFIED THREAT MANAGEMENT) PARA LA SEGURIDAD INFORMÁTICA EN LA UNIVERSIDAD PONTIFICIA BOLIVARIANA SECCIONAL MONTERÍA" [En línea] Disponible en: (https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/13323/1/6882628.pdf)

11 ENLACE AL VIDEO DE SUSTENTACIÓN

https://youtu.be/c09aMG84rMQ

12 RESULTADO DE PRUEBA ANTI-PLAGIO

Ilustración 55 Resultado prueba anti-plagio

	Título de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud	Calificación
Ver recibo digital	Informe Seminario	1669770997	9/10/2021 22:15	12%	N/A

Fuente: Propia