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

HERNAN CAMILO VELANDIA CASCAVITA

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

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

HERNAN CAMILO VELANDIA CASCAVITA

LUIS FERNANDO ZAMBRANO
DIRECTOR DE CURSO

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

CONTENIDO

Pág.

LISTA DE FIGURAS

RESUMEN

La creciente participación en el mundo digital de personas y compañías, ha incrementado la exposición a amenazas cibernéticas de estos actores y su información, por lo que, la ciber seguridad se ha convertido en un pilar fundamental para la protección de los datos. La evolución de esta disciplina ha permitido desarrollar marcos de trabajo y enfoques preventivos y proactivos en la implementación de controles, para mitigar cualquier amenaza antes de que se materialice el riesgo mediante un posible ataque. Dentro de los enfoques disponibles, se encuentra la implementación de equipos Red Team y Blue Team como parte de la estrategia de ciber seguridad de la organización, los cuales, tienen como objetivo detectar vulnerabilidades, remediarlas y generar recomendaciones que optimicen y fortalezcan los sistemas y políticas de seguridad existentes.

En este informe se presentarán el marco legal vigente en materia de ciber seguridad, donde se establece la definición jurídica de delito informático, las obligaciones sobre protección de datos personales, los acuerdos internacionales sobre ciber seguridad y los organismos estatales encargados de la ciber seguridad del país. En cuanto a los equipos Red Team y Blue Team, se aborda su función como equipos complementarios, parte de la estrategia de ciber seguridad de la organización, desde diferentes enfoques: Red Team como un equipo que simula el rol de atacante para identificar vulnerabilidades y remediarlas, y Blue Team como un equipo de defensa que audita e identifica aspectos a fortalecer en el esquema integral de seguridad de la organización. Para estos equipos, se abordará la metodología de trabajo para la ejecución de sus funciones, a través de mecanismos de Pentesting y generación de reportes y recomendaciones de hardening para la infraestructura de la organización. La información contenida en el presente documento es la recopilación de las actividades realizadas en el seminario especializado de Equipos estratégicos en ciberseguridad: Red Team & Blue Team, y su objetivo es comprender los aspectos más importantes a la hora de plantear estrategias para la prevención, contención y mitigación de ataques informáticos.

Palabras claves: Blue Team, Ciber seguridad, Hardening, Pentesting, Red Team.

GLOSARIO

Bien jurídico: Objeto de protección de la ley, utilizado para clasificar los delitos. El bien jurídico se refiere a una condición valorada por la sociedad, como el patrimonio, la integridad o la protección de la información y los datos. Se diferencia del objeto material del delito, que pueden ser los objetos, bienes o datos sustraídos o afectados en una acción ilegal. Así, en un delito informático, el bien jurídico afectado será la protección de la información y los datos, mientras que el objeto material serán los datos sustraídos.

Delito informático: Acción o conducta ilícita que comete un individuo en entornos digitales. Se identifican como delitos informáticos el acceso ilícito o no autorizado a un sistema informático, la interceptación no autorizada de datos informáticos, el daño a sistemas informáticos y datos, el hurto por medios informáticos, entre otros.

Red Team: Equipo especializado de ciber seguridad que actúa en el rol de atacante para probar los controles existentes del sistema de seguridad de la organización, con el objetivo de identificar vulnerabilidades y activos de información expuestos, para generar recomendaciones y planes de remediación.

Blue Team: Equipo especializado de ciber seguridad que actúa en el rol de protector de los activos de información de la organización, mediante el análisis continuo de los controles, políticas y sistemas de seguridad para identificar puntos a fortalecer en los mismos.

Pentesting: Test de Penetración, es una técnica que consiste en realizar ataques a la infraestructura tecnológica para identificar vulnerabilidades, de forma tal que puedan implementarse controles y medidas de remediación de forma preventiva, para fortalecer el sistema ante un posible ataque real.

Vulnerabilidad: Debilidad existente en un sistema, que puede ser utilizada por un actor malicioso para comprometer la seguridad de dicho sistema mediante un ataque o explotación. Se identifican vulnerabilidades en software, hardware, procedimientos o recurso humano.

CSIRT: Equipo de respuesta ante emergencias informáticas, es un organismo o equipo encargado de atender incidentes de seguridad en sistemas informáticos. Se compone de especialistas en ciber seguridad que se encargan de atender posibles

incidentes y determinar planes de mitigación, remediación y retorno a la normalidad en caso de ataque.

Hardenización: Proceso de fortalecimiento de un sistema informático en materia de seguridad, mediante la implementación de controles que reduzcan las vulnerabilidades existentes en el mismo, implementando metodologías como confianza cero y privilegio mínimo, para reducir el área de exposición ante un posible ataque.

INTRODUCCIÓN

Los marcos de trabajo en materia de ciber seguridad establecen enfoques preventivos y proactivos para mitigar amenazas informáticas. Este enfoque plantea la implementación de equipos Red Team y Blue Team a la estrategia de ciber seguridad de la organización, como complemento a las políticas y controles existentes. El objetivo de estos equipos es identificar amenazas y vulnerabilidades para generar controles y planes de remediación que permitan mitigarlas, esto desde dos enfoques diferentes y complementarios: los equipos Red Team ejecutan ataques a la infraestructura tecnológica para determinar puntos vulnerables y activos de información comprometidos; por su parte, los equipos Blue Team evalúan la infraestructura, políticas y controles existentes desde un enfoque interno para generar planes de fortalecimiento en materia de ciber seguridad. En el presente documento, se abordará con mayor profundidad el rol de estos equipos, el marco regulatorio existente y las metodologías de trabajo que utilizan para la ejecución de estas actividades.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

- Construir un informe técnico que contenga los elementos fundamentales implementados en la definición de estrategias preventivas y reactivas de ciber seguridad para su aplicación en escenarios de ataques informáticos.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar la normativa vigente en materia de ciber seguridad en Colombia, con el fin de poder evaluar eventos informáticos y determinar su legalidad.

- Ejecutar pruebas de penetración en sistemas informáticos que permitan identificar vulnerabilidades, en el marco del rol de Red Team.

- Formular planes de remediación, contención y fortalecimiento de los sistemas informáticos en materia de seguridad, para subsanar las vulnerabilidades identificadas, en el marco del rol de Blue Team.

2 DESARROLLO DEL INFORME TÉCNICO

2.1 AMBIENTE ÉTICO Y LEGAL

En Colombia, la ley fundamental relacionada con delitos informáticos es la ley 1273 de 2009, que definió el concepto de protección de la información y de los datos al establecer las formas de atentar contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, los delitos a través de medios informáticos, así como el alcance de las autoridades y las penas correspondientes[1].

La ley establece que el acceso a un sistema informático sin autorización o por fuera de la autorización definida, sin importar si el sistema cuenta o no con medidas de protección y seguridad, se considerará delito informático; de forma similar, impedir el acceso o funcionamiento normal de un sistema informático o una red de telecomunicaciones, interceptar información sin autorización judicial, generar cualquier tipo de daño a datos o sistemas informáticos, estar vinculado con la cadena de producción y uso de software malicioso, robar o comerciar datos personales por diferentes medios incluyendo la suplantación de sitios web, se consideran delitos informáticos. Las penas aplicables varían entre 36 y 96 meses y multas de entre 100 y 1.000 salarios mínimos mensuales legales vigentes, excepto si la conducta se puede tipificar en un delito con penas mayores. Igualmente, se considerarán agravantes los casos en los que se afecten sistemas de interés público, como los sistemas oficiales o financieros, nacionales o internacionales, así como si el sindicado es un funcionario público, una persona que abusa de la confianza dada por el propietario o responsable de la información, o si es el responsable de la administración o control del sistema. De igual forma, se consideran agravantes las finalidades del ataque si están relacionadas con fines terroristas, si al revelar la información afecta a otras personas o si busca obtener provecho para el atacante o un tercero.

En cuanto a los delitos cometidos por medios informáticos, establece que el hurto mediante la manipulación de sistemas informáticos o la suplantación de usuarios, se considerarán delitos informáticos y se aplicarán las mismas penas vigentes para el hurto calificado. En cuanto a la transferencia no autorizada de activos mediante la manipulación de sistemas informáticos, establece penas de 48 a 120 meses y multas de 200 a 1500 salarios mínimos mensuales legales vigentes. Además, establece como agravantes para otros delitos no tipificados en esta ley, el uso de medios informáticos y extiende el alcance de los jueces hacia este tipo de delitos.

[1] Superintendencia de Industria y Comercio [página web]. [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

En lo que respecta a protección de datos personales, se aplica la ley 1581 de 2012. La ley aplica para cualquier base de datos que, por su contenido son sujetas a tratamiento, y establece principios sobre el tratamiento de los datos como la finalidad, la veracidad, la calidad, la transparencia, entre otros. De igual forma, define la categoría de datos sensibles y establece que solo pueden ser utilizados cuando se cuente la autorización expresa del titular o su uso esté relacionado con proteger la vida del titular o con procesos judiciales[2].

En cuanto a los titulares de los datos personales, establece sus derechos, como conocer, actualizar o rectificar sus datos, autorizar o revocar el uso de sus datos, conocer el uso que se dará a sus datos, entre otros. La ley también define los casos en los que no se requiere autorización para el tratamiento de los datos, como cuando los datos a usar son públicos, ante urgencias sanitarias o cuando se cuenta con autorización legal dependiente del uso a darles.

Respecto a los responsables (quien decide sobre los datos y su tratamiento) y encargados (quien realiza el tratamiento de los datos) del tratamiento, establece que los responsables deben garantizar los derechos del titular, proteger la información que custodian, mantenerla actualizada de acuerdo con lo suministrado por el titular, informar al titular sobre el uso de sus datos e informar a las autoridades ante cualquier vulneración de los datos, entre otros. En cuanto a los encargados, estos deben garantizar los derechos del titular, proteger la información que manipulan, realizar las tareas de actualización y rectificación de los datos requeridas, registrar los comentarios a los datos ordenados por ley, informar a las autoridades cuando se presenten vulneraciones de los datos, entre otros.

A su vez, la Superintendencia de Industria y Comercio SIC, está autorizada para vigilar y sancionar a las entidades que deban acatar esta ley. Para ello, La SIC podrá investigar y ordenar la aplicación de medidas que garanticen el derecho al habeas data, así como divulgar la norma aplicable o sugerir modificaciones y ajustes a la misma. El organismo también podrá dar instrucciones sobre los procesos y solicitar información a responsables y encargados del tratamiento de datos personales. Ante el incumplimiento de la norma, la SIC podrá imponer sanciones a responsables y encargados del tratamiento de datos personales, que irán desde multas a personas o instituciones hasta la suspensión, cierre temporal o definitivo de las operaciones relacionadas con el tratamiento de los datos persona les. La gravedad de la sanción dependerá de factores como el tamaño del daño causado, la reincidencia de las acciones o el desacato a las órdenes impartidas por la SIC.

[2] LEY 1581 de 2012 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#:~:text=La%20presente%20ley%20tiene%20por,el%20artículo%2015%20de%20la>.

En cuanto a acuerdos internacionales, la ley 1928 de 2018 aprueba el Convenio sobre la Ciberdelincuencia de Budapest, firmado en 2001. El Consejo de Europa invitó al país a unirse en 2013 y finalmente Colombia se adhiere a este Convenio en 2020[3]. El Convenio obliga al país a adoptar medidas de derecho penal sustantivo sobre el acceso e interceptación ilícita, ataques contra los datos y los sistemas, los dispositivos y programas informáticos para cometer delitos informáticos, la falsificación y el fraude informático, delitos relacionados con pornografía infantil, derechos y propiedad intelectual. Las medidas deben incluir la tentativa y complicidad en los actos tipificados, así como la responsabilidad y las sanciones aplicables[4].

En resumen, la normativa vigente en Colombia tiene 3 grandes frentes, la Ley 1273 de 2009, que recoge la inclusión de los delitos cibernéticos en el Código Penal Colombiano, y establece las definiciones de las conductas, responsables, penas, agravantes y jueces competentes en esta materia. Esta norma es la base para establecer el tratamiento de los delitos cibernéticos.

El segundo frente es la Ley 1581 de 2012, que reglamenta la protección de datos personales, estableciendo las definiciones de datos personales, sus características, normativa aplicable, responsabilidades y obligaciones de los participantes en el tratamiento de los datos, las sanciones correspondientes ante los incumplimientos y los agravantes en las mismas. Esta ley es la base para la protección de los datos personales y sus titulares.

En tercer lugar, Ley 1928 de 2018 vincula al país al Convenio sobre la Ciberdelincuencia de Budapest, estableciendo las definiciones homologables a nivel internacional sobre delitos informáticos, que previamente se han recogido en la Ley 1273 de 2009. Adicionalmente, establece los mecanismos de cooperación internacional para combatir la ciberdelincuencia.

Acompañando estas leyes, se encuentran los Documentos CONPES 3701 y 3854, que han establecido la estrategia de ciberseguridad del país, definiendo los organismos estatales encargados de responder ante amenazas y la estrategia de acción desde la gestión del riesgo como el mejor mecanismo para la protección de la información.

---

[3] COLOMBIA SE adhiere al Convenio de Budapest contra la ciberdelincuencia | Cancillería [Anónimo]. Cancillería | Ministerio de Relaciones Exteriores de Colombia [página web]. [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia#:~:text=Colombia%20se%20adhiere%20al%20Convenio%20de%20Budapest%20contra%20la%20ciberdelincuencia,-2020-03-17&text=Estrasburgo%20(mar.,la%20lucha%20contra%20la%20ciberdelincuencia>.

[4] COUNCIL OF EUROPE. Convenio sobre la ciberdelincuencia. (23, noviembre, 2001). [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.oas.org/juridico/english/cyb_pry_convenio.pdf>.

2.2 PROCESO DE PENTESTING

El Pentesting es un proceso de seguridad que busca identificar vulnerabilidades y brechas en los sistemas y redes de la organización, para tratar de explotarlos con el fin de determinar la gravedad de los mismos. El objetivo de estas pruebas es poder implementar planes de parcheo y remediación que minimicen los riesgos asociados a estas vulnerabilidades y brechas. El proceso de Pentesting cuenta con diferentes etapas, entre 5 y 7 dependiendo de la fuente, pero coinciden en el flujo de las actividades y la forma de construir el plan de ejecución, a continuación, se detallarán las 5 etapas principales.

La fase inicial de reconocimiento busca obtener toda la información posible del sistema a probar. Para esto, se utilizan diferentes herramientas que permitan obtener información de múltiples frentes, como Nmap para realizar escaneos de puertos, Recon-ng para realizar recopilación y análisis de información de hostnames, IPs, contenido de los paquetes, etc. Las herramientas mencionadas se enmarcan en técnicas como la recopilación automática de datos con frameworks de trabajo y la recopilación de metadatos, sin embargo, existen otras técnicas como el uso de Google Dorks, en la que no se requieren herramientas de software, sino que, utilizando únicamente el buscador de Google, se puede recopilar información de sitios web mediante las opciones avanzadas del buscador, que pueden encontrar archivos de usuarios y contraseñas, conversaciones de chats, información de dispositivos como cámaras de vigilancia, archivos de logs, etc[5].

En la fase de análisis de vulnerabilidades, el atacante tomará toda la información recopilada, para establecer los patrones de ataque a implementar. El objetivo es atacar en todos los frentes posibles, para comprometer al objetivo. El listado de vulnerabilidades posibles es amplio, abarcando desde problemas en el diseño del sistema hasta fallos en los procesos o fallos inducidos por ataques intencionales. Se destacan vulnerabilidades como el diseño inseguro, que incluye debilidades en el diseño de los controles de seguridad de los sistemas; componentes vulnerables y obsoletos, como sistemas operativos, controladores de hardware, sistemas de seguridad perimetral, etc., que debido a falta de actualizaciones y parches, o por descontinuación del producto, exponen al sistema a vulnerabilidades que probablemente se solucionaron en versiones posteriores del componente; inyección, una vulnerabilidad en la que el sistema permite el envío de cadenas que serán interpretadas como instrucciones de código para alterar su funcionamiento normal, como inyección de SQL, XML o LDAP.

[5] EC-COUNCIL. Understanding the Five Phases of the Penetration Testing Process. Cybersecurity Exchange [página web]. [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/>.

La siguiente fase se enfoca en explotar las vulnerabilidades encontradas mediante el uso de exploits, herramientas diseñadas específicamente para explotar estos fallos del sistema, o bien, directamente usando la información recopilada en las fases anteriores, como usuarios y contraseñas. Dependiendo de las vulnerabilidades identificadas, se utilizarán exploits y suites específicamente diseñadas para dicha vulnerabilidad. Destacan herramientas como SQLMap, que realiza explotación de vulnerabilidades de inyección SQL de forma automática, y Metasploit Framework, un marco de trabajo completo para explotación de más de 1.600 vulnerabilidades diferentes[6].

La fase de post explotación consiste en, una vez obtenido el acceso al sistema objetivo, ya sea mediante la explotación de una vulnerabilidad o el uso de credenciales obtenidas, ampliar el ataque al comprometer otros sistemas vinculados o aumentar el nivel de acceso mediante la obtención de credenciales con privilegios de administrador o similares. Esta fase no siempre es posible de ejecutar, ya que dependerá de haber encontrado vulnerabilidades explotables previamente, con suficiente alcance como para comprometer otros sistemas u otros niveles de acceso, algo que no siempre se logrará, sobre todo, si el diseño del sistema objetivo inicial es lo suficientemente robusto como para superar exitosamente las pruebas de Pentesting.

La fase de informes consiste en construir un resumen de todas las actividades realizadas en la prueba, los resultados obtenidos, los activos de información o sistemas comprometidos y los impactos que podría tener la organización debido a las vulnerabilidades identificadas. Dependiendo de lo acordado con la organización, pueden incluirse muestras de la información obtenida, recomendaciones de remediación sobre las vulnerabilidades identificadas, planes de acción para fortalecer los sistemas y documentación sobre las cadenas de custodia de la información obtenida de la prueba.

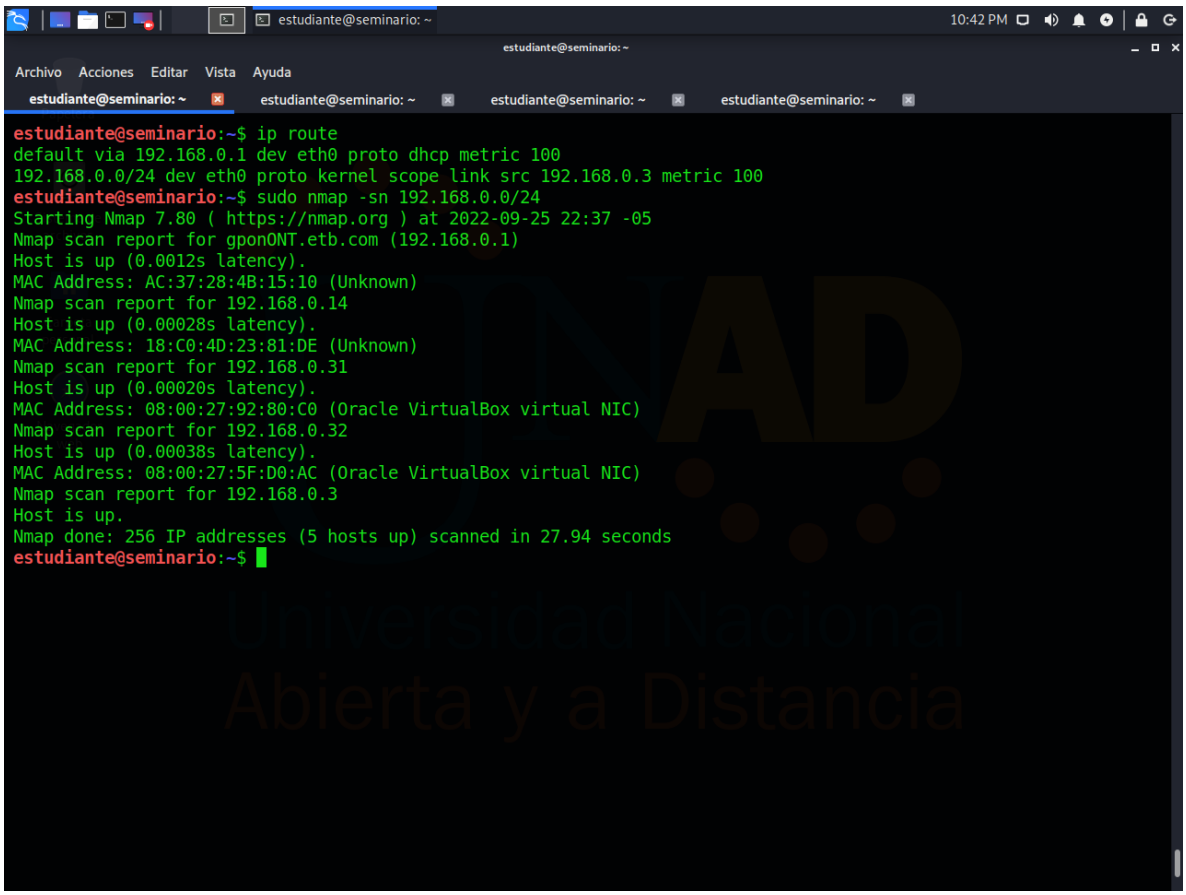
2.3 ESTRATEGIAS RED TEAM

Se plantea un escenario de prueba, en el que se deben identificar vulnerabilidades de un sistema con dos máquinas, lograr la extracción de datos y reportar los hallazgos. El proceso empezó con el uso de Nmap para identificar las máquinas objetivo disponibles en la red de la máquina atacante, Kali. Se utilizó el comando ip route para identificar los datos de red en los que se ubica la máquina y posteriormente se usó el comando nmap -sn 192.168.0.0/24 para escanear todas

[6] HERNÁNDEZ, Mikel. ¿Cuál Son La 5 Fases Del Pentesting? - Ciberseguridad. Bidaidea: líderes en Ciberseguridad & Inteligencia [página web]. (21, marzo, 2022). [Consultado el 4, septiembre, 2022]. Disponible en Internet: <https://ciberseguridadbidaidea.com/fases-del-pentesting/>.

las máquinas disponibles en el segmento de red compartido con Kali, esto permitió identificar las máquinas con Windows 7.

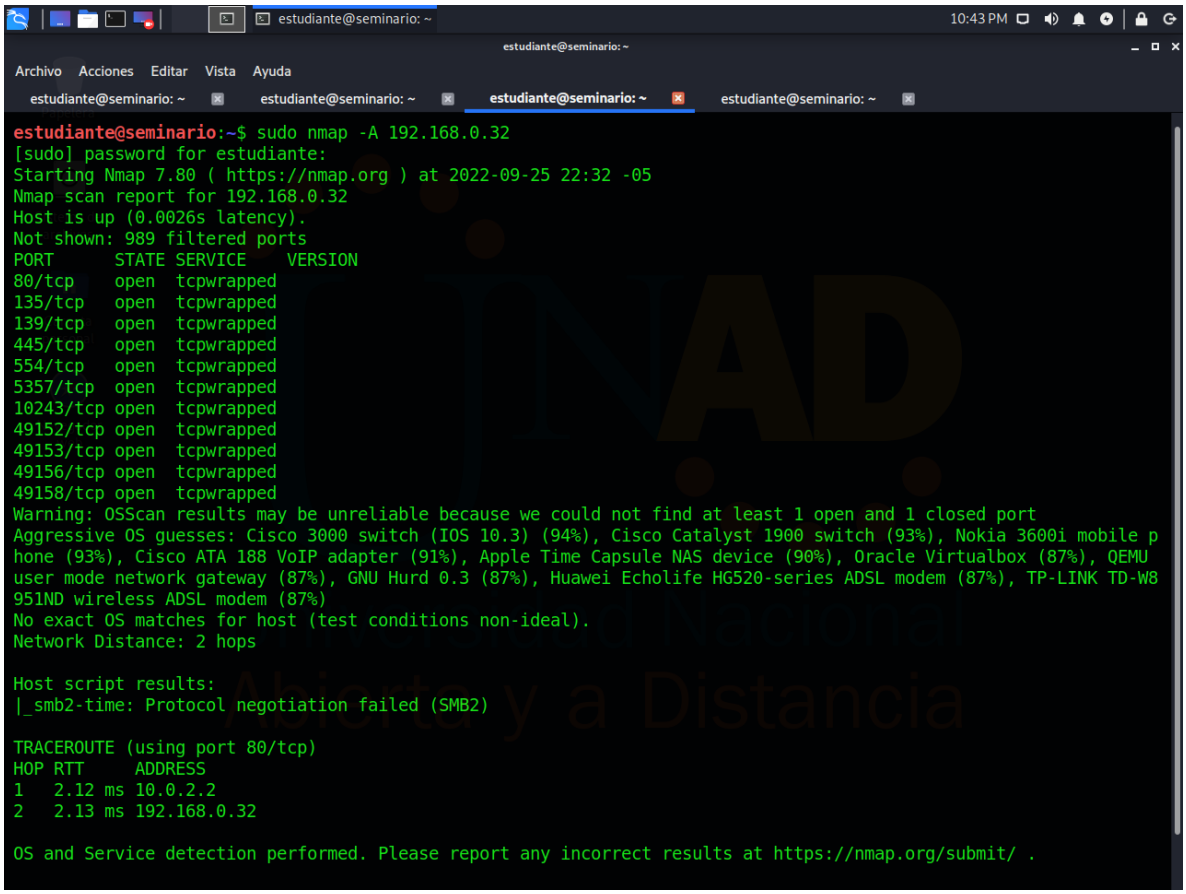
Figura 1. Escaneo con Nmap



Fuente: elaboración propia.

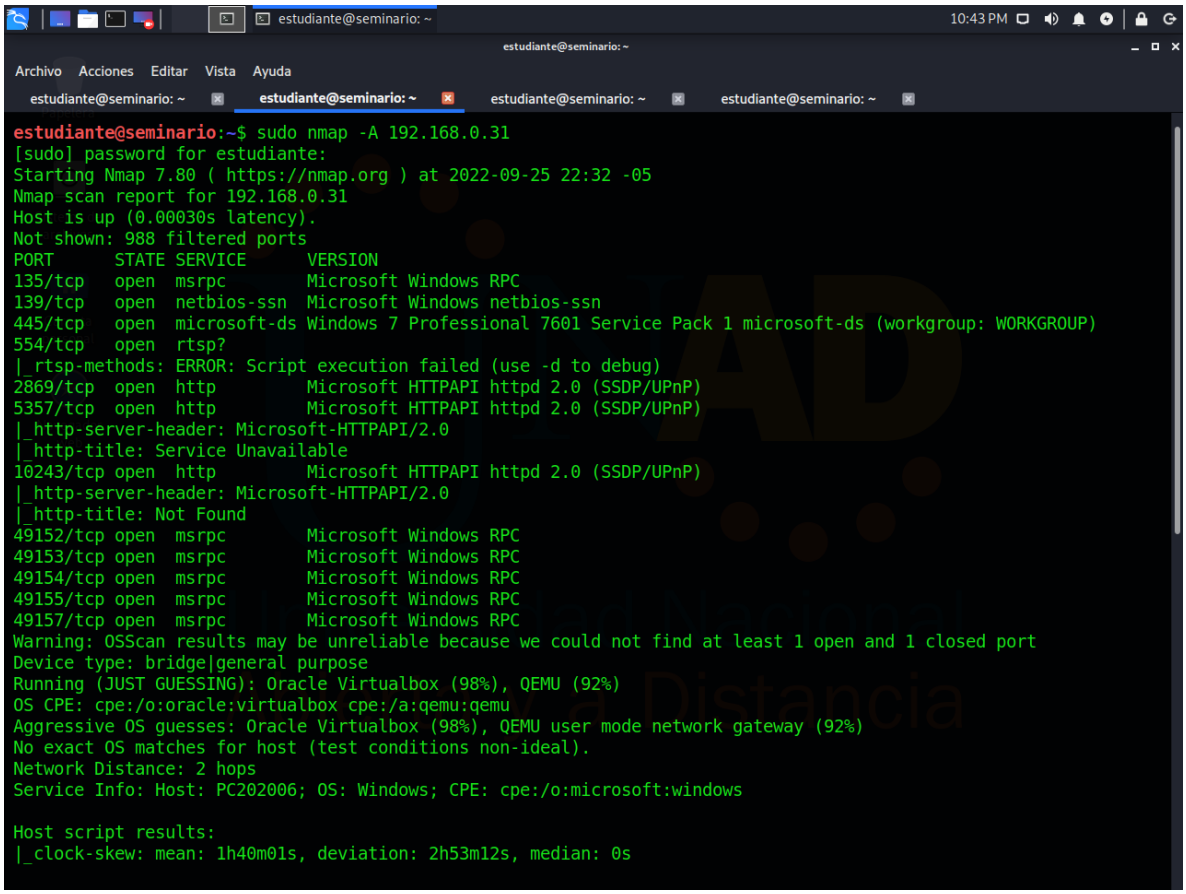
Una vez realizado el reconocimiento de los recursos disponibles, se realizó un análisis de vulnerabilidades preliminar con Nmap, usando el comando nmap -A 192.168.0.xx, con el que se ordenó un escaneo completo de puertos a las dos máquinas Windows 7, para identificar brechas de seguridad en sus configuraciones. Este proceso arrojó múltiples brechas de seguridad en las máquinas Windows 192.168.0.31, donde se identificaron puertos abiertos y protocolos vulnerables.

Figura 2. Escaneo Nmap máquina 32



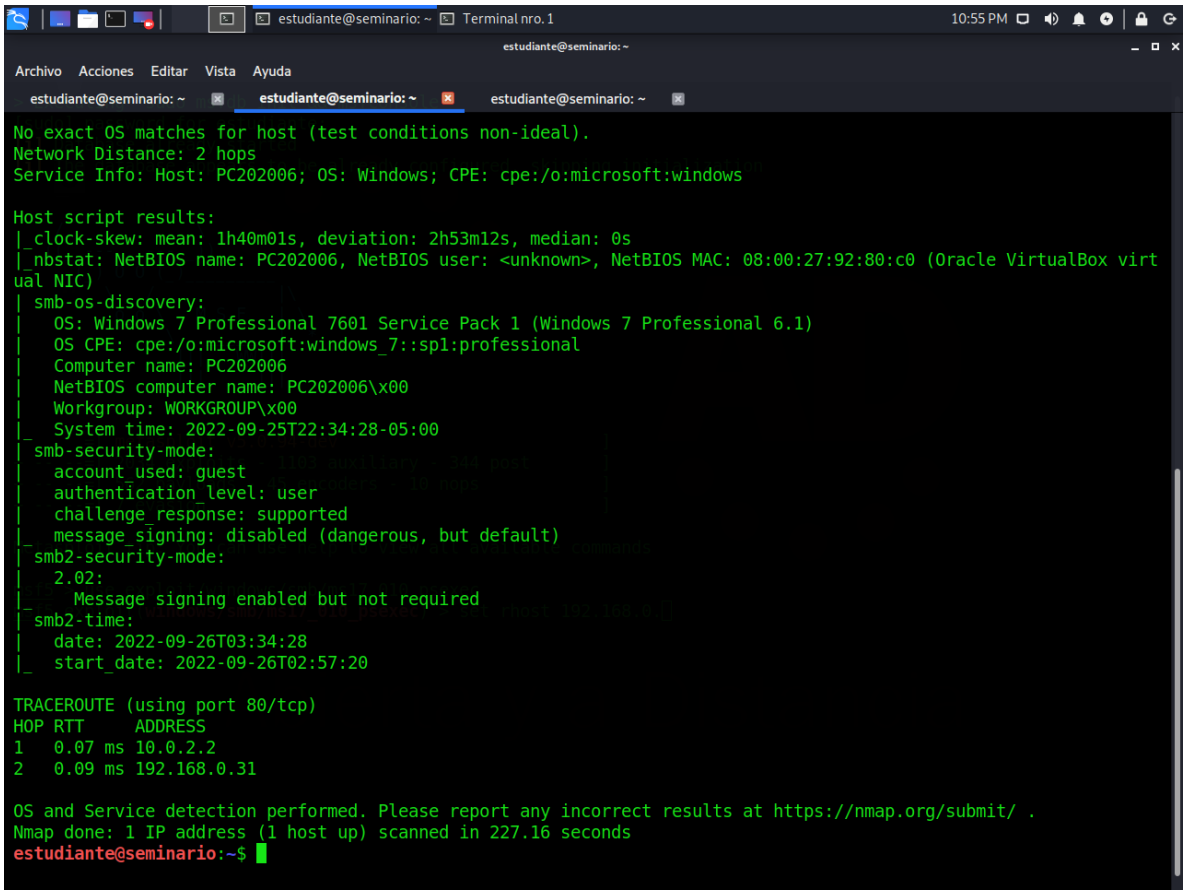
Fuente: elaboración propia.

Figura 3. Escaneo Nmap máquina 31



Fuente: elaboración propia.

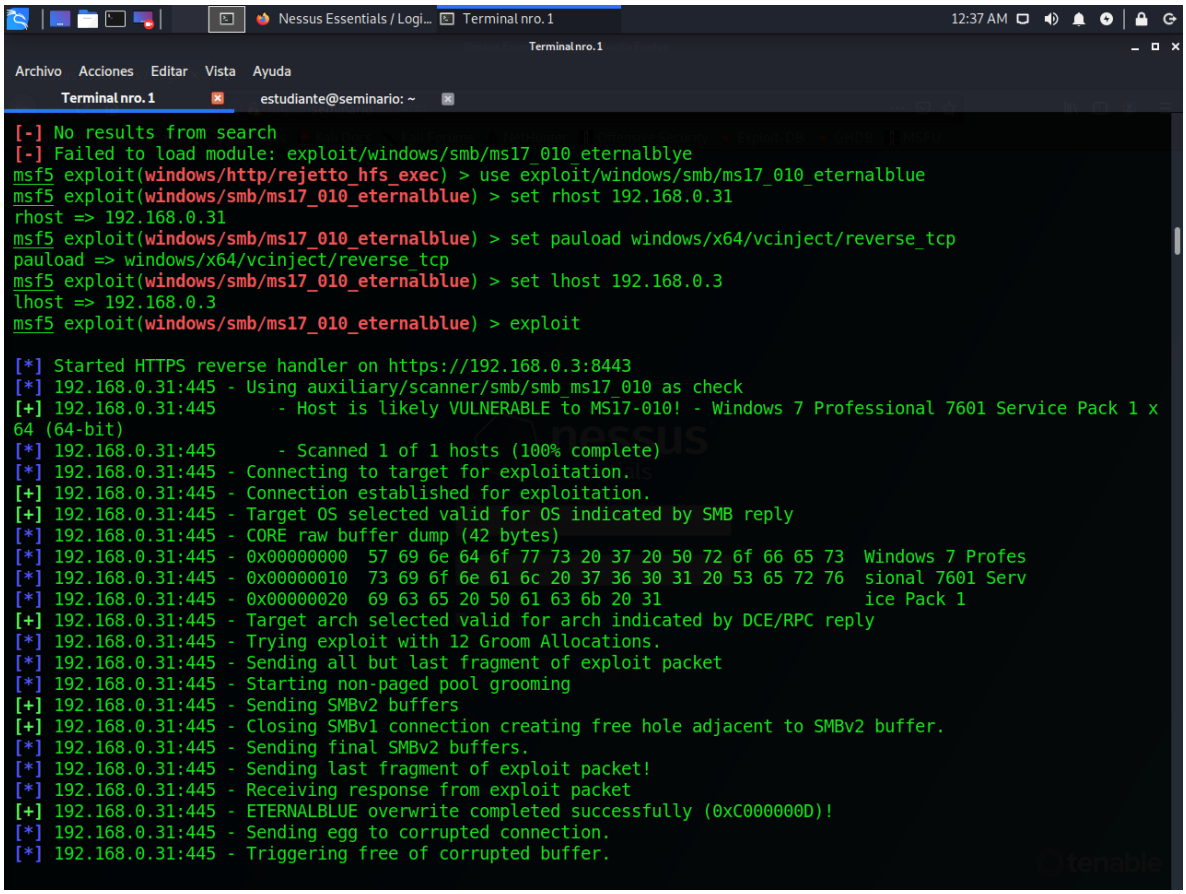
Figura 4. Vulnerabilidades identificadas con Nmap en máquina 31



Fuente: elaboración propia.

Con la identificación de múltiples vulnerabilidades y puertos expuestos, sumados a la información suministrada en el anexo, se procede a seleccionar Metasploit como herramienta para la explotación de vulnerabilidades. El exploit seleccionado fue EternalBlue, un exploit desarrollado por la NSA, que aprovecha el protocolo SMB y la vulnerabilidad CVE-2017-0144, de Windows.

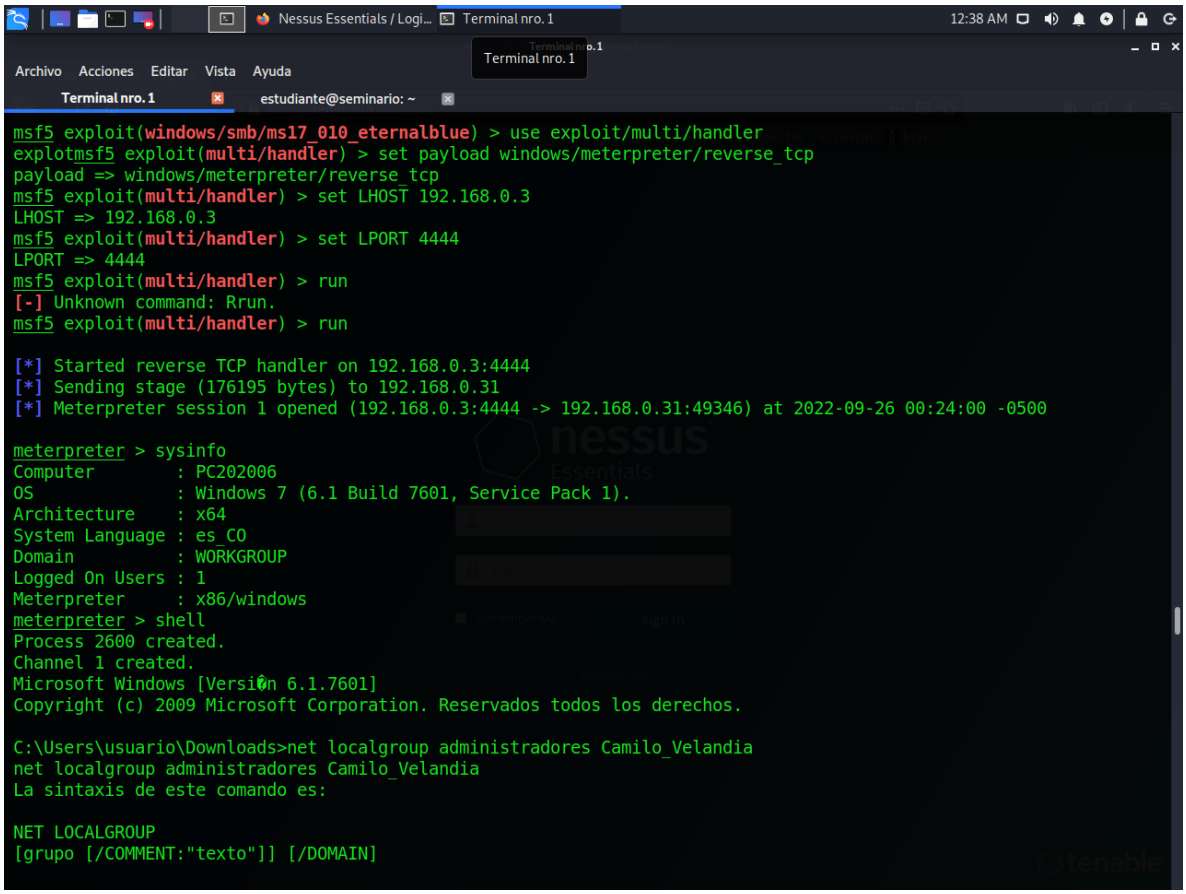
Figura 5. Ejecución EternalBlue



Fuente: elaboración propia.

El uso dado al exploit, fue generar una carga con Meterpreter, un troyano que permite controlar de forma remota las máquinas. Para forzar su ejecución, se estableció un servidor Apache en la máquina Kali, a la vez que se monitoreó el tráfico de red de la máquina objetivo, para forzar el acceso al troyano seleccionado.

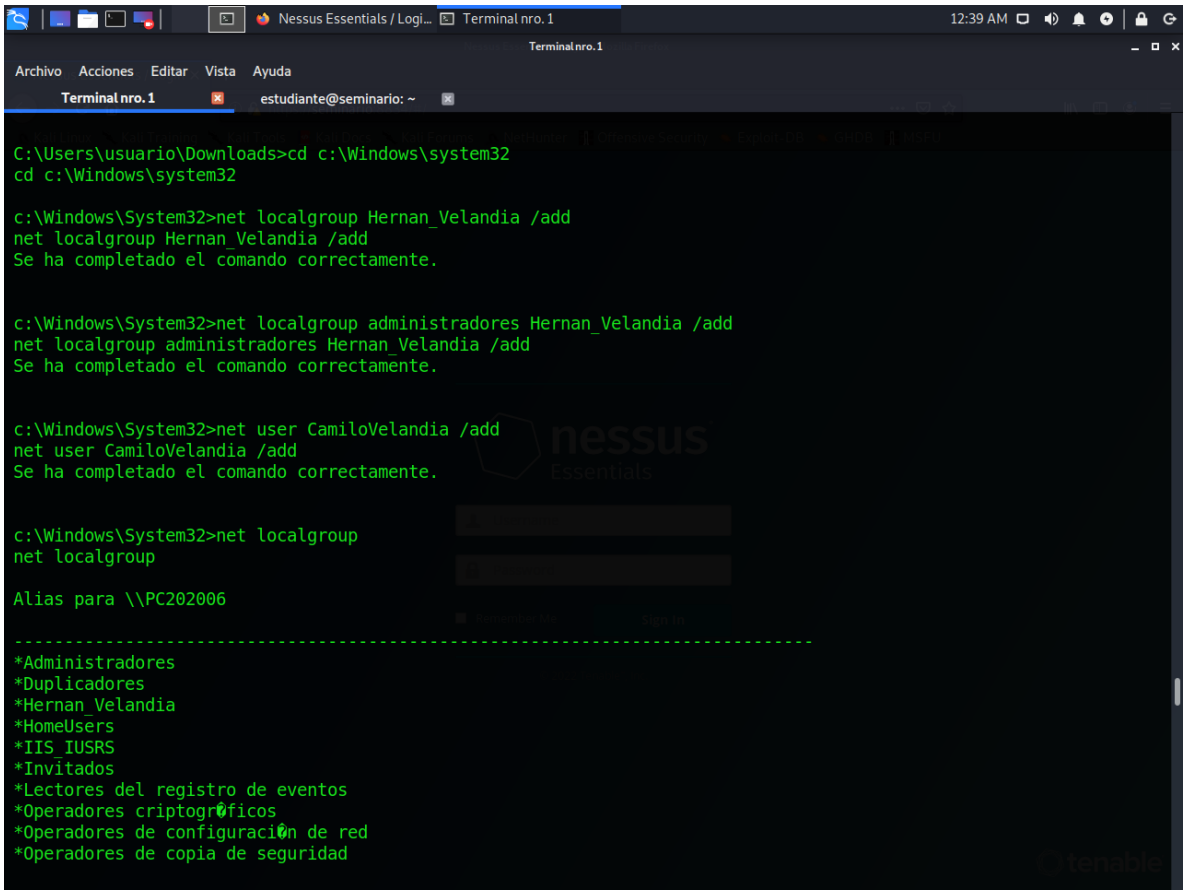
Figura 6. Configuración de Meterpreter



Fuente: elaboración propia.

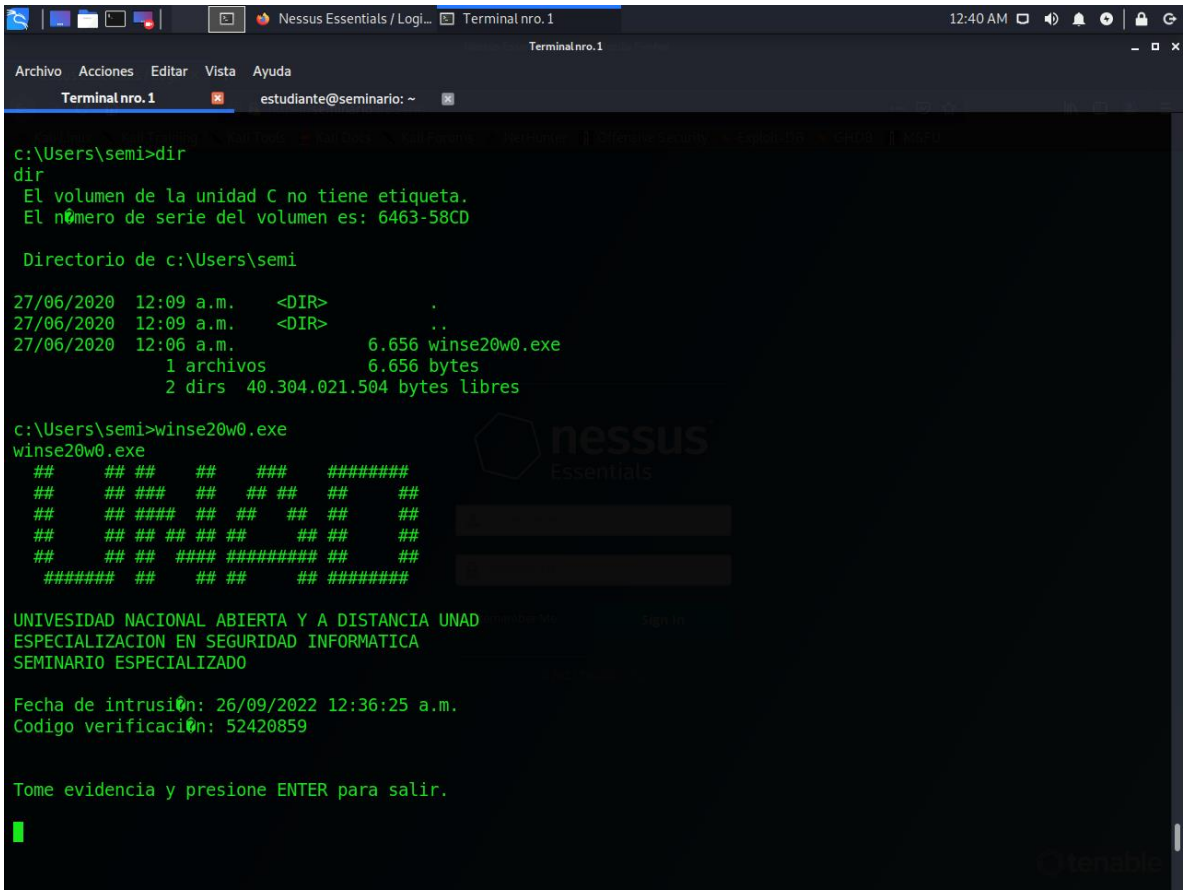
Una vez explotada la vulnerabilidad, se procede a una fase de post explotación, en la que se busca ampliar la superficie comprometida del sistema. Para ello, se realizaron dos tareas, la creación de un usuario administrador en la máquina y el acceso a un archivo almacenado en el equipo. En ambas tareas se utilizaron comandos Shell nativos de Windows, ejecutados desde Kali a través de Meterpreter. En primer lugar, se realizó la creación de un nuevo usuario con privilegios de administrador. Posteriormente, se localizó el archivo winse20w0.exe, mencionado en el anexo, y se ejecutó para evidenciar el acceso remoto a la máquina.

Figura 7. Configuración y validación de nuevo usuario



Fuente: elaboración propia.

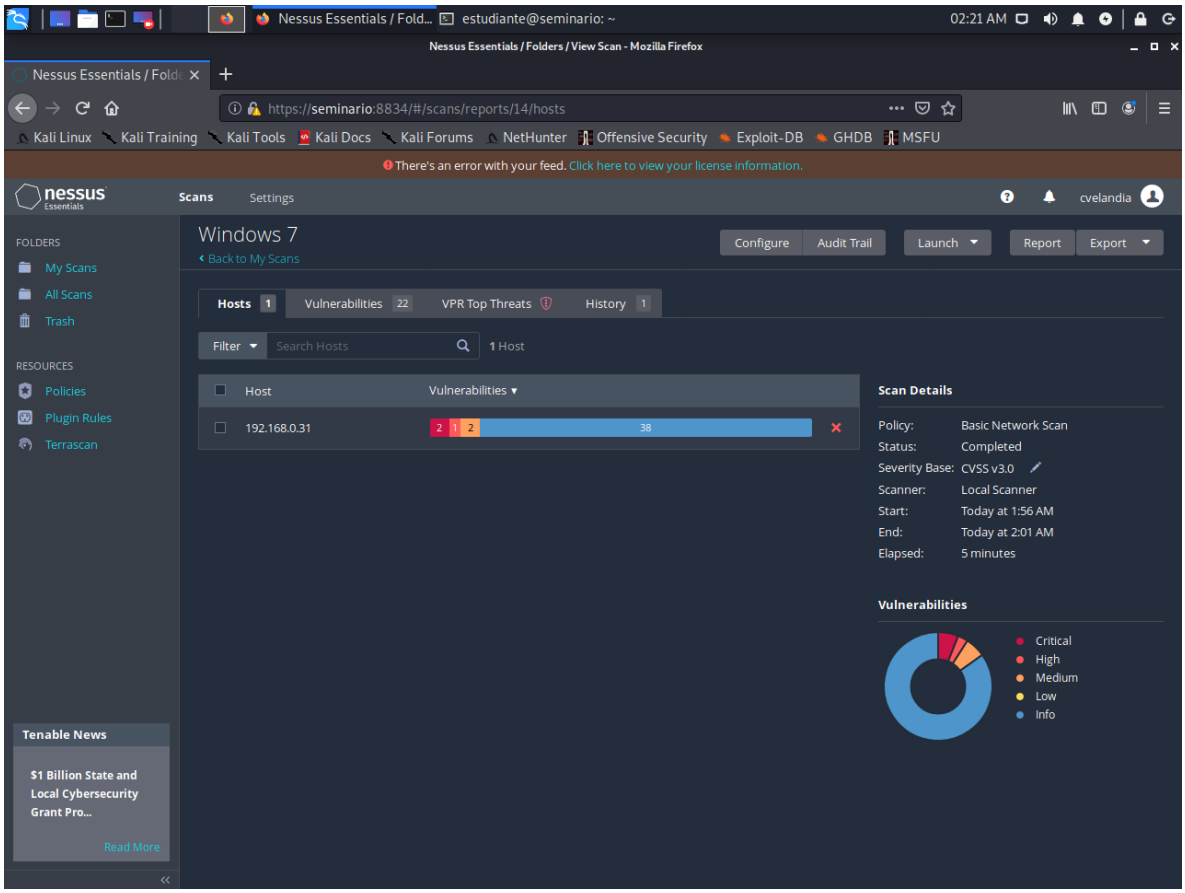
Figura 8. Búsqueda y ejecución del archivo winse20w0.exe



Fuente: elaboración propia.

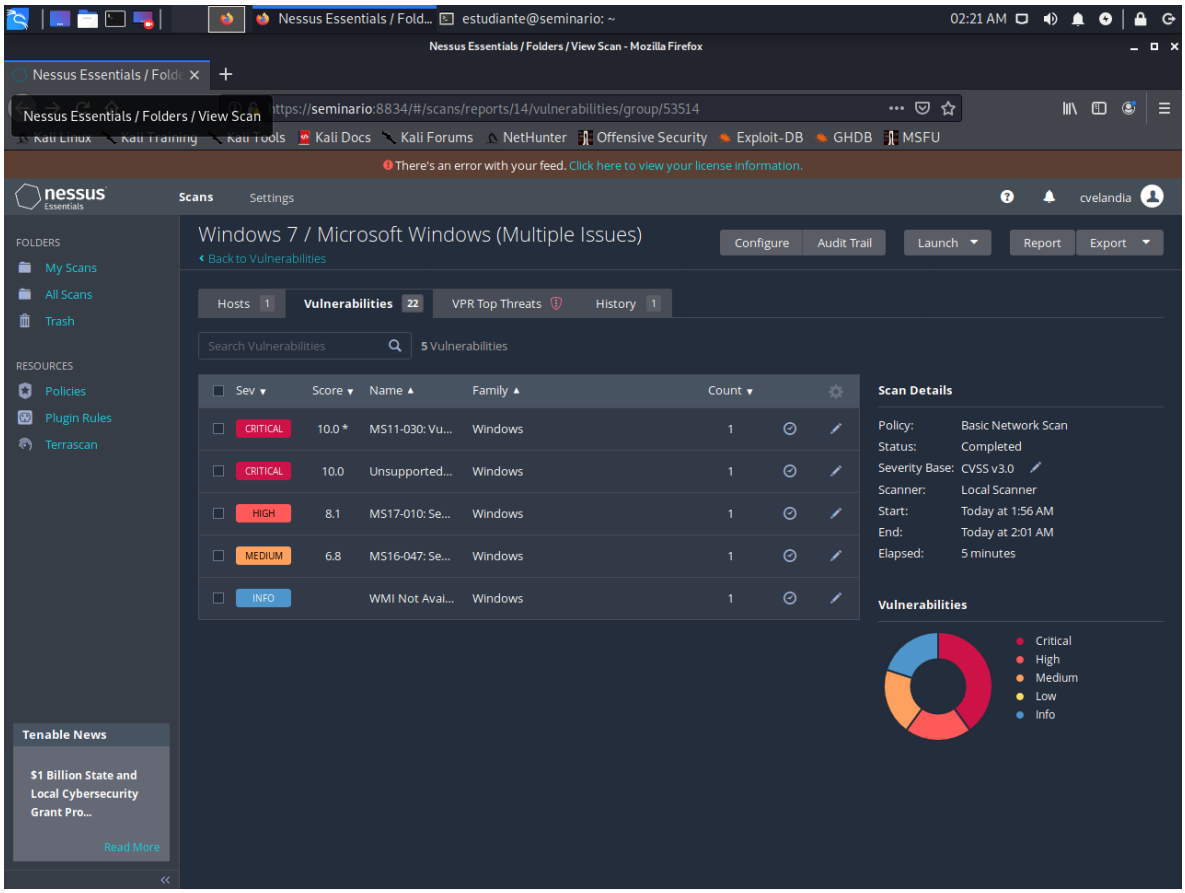
Para finalizar el proceso, se generó un análisis de vulnerabilidades de la máquina objetivo, utilizando la herramienta Nessus. A través de este servicio, se generó un reporte ampliamente documentado de todas las vulnerabilidades del recurso, no solo las explotadas en esta actividad. Nessus realiza un amplio escaneo de vulnerabilidades y presenta reportes consolidados y detallados del grado de exposición de la máquina, las vulnerabilidades presentes y los puntos críticos del recurso. Su interfaz gráfica permite comprender en un primer vistazo la criticidad del informe, además de ofrecer amplia información sobre el detalle de los hallazgos.

Figura 9. Resumen de vulnerabilidades Nessus



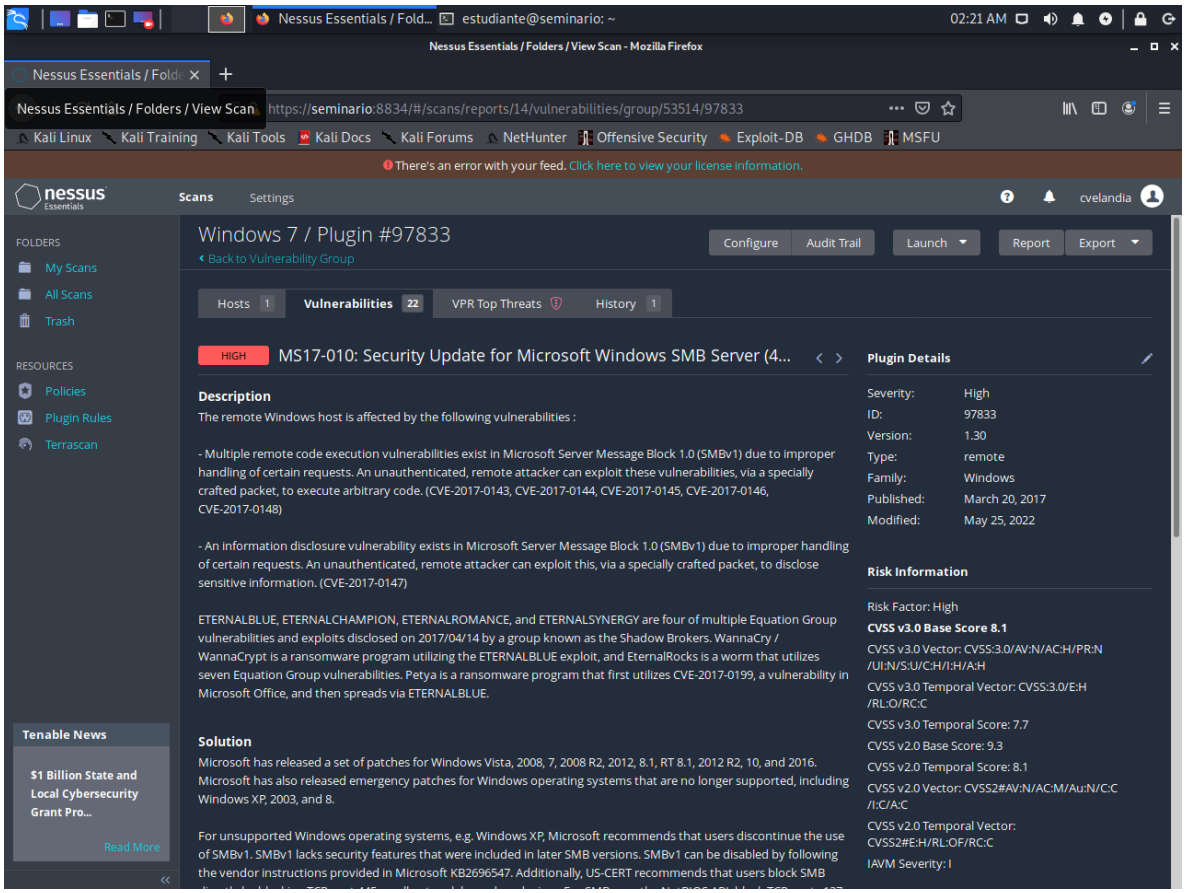
Fuente: elaboración propia.

Figura 10. Reporte de vulnerabilidades por categoría



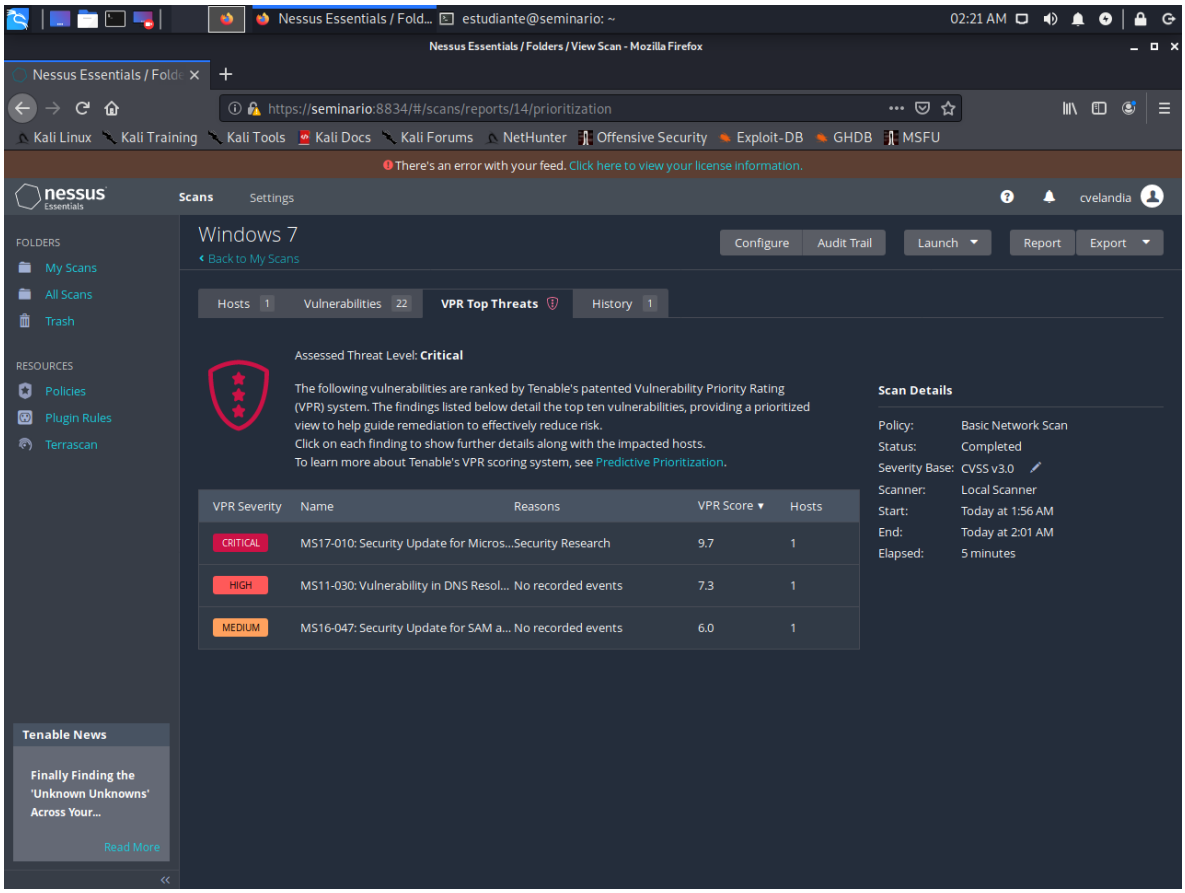
Fuente: elaboración propia.

Figura 11. Reporte detallado de vulnerabilidad



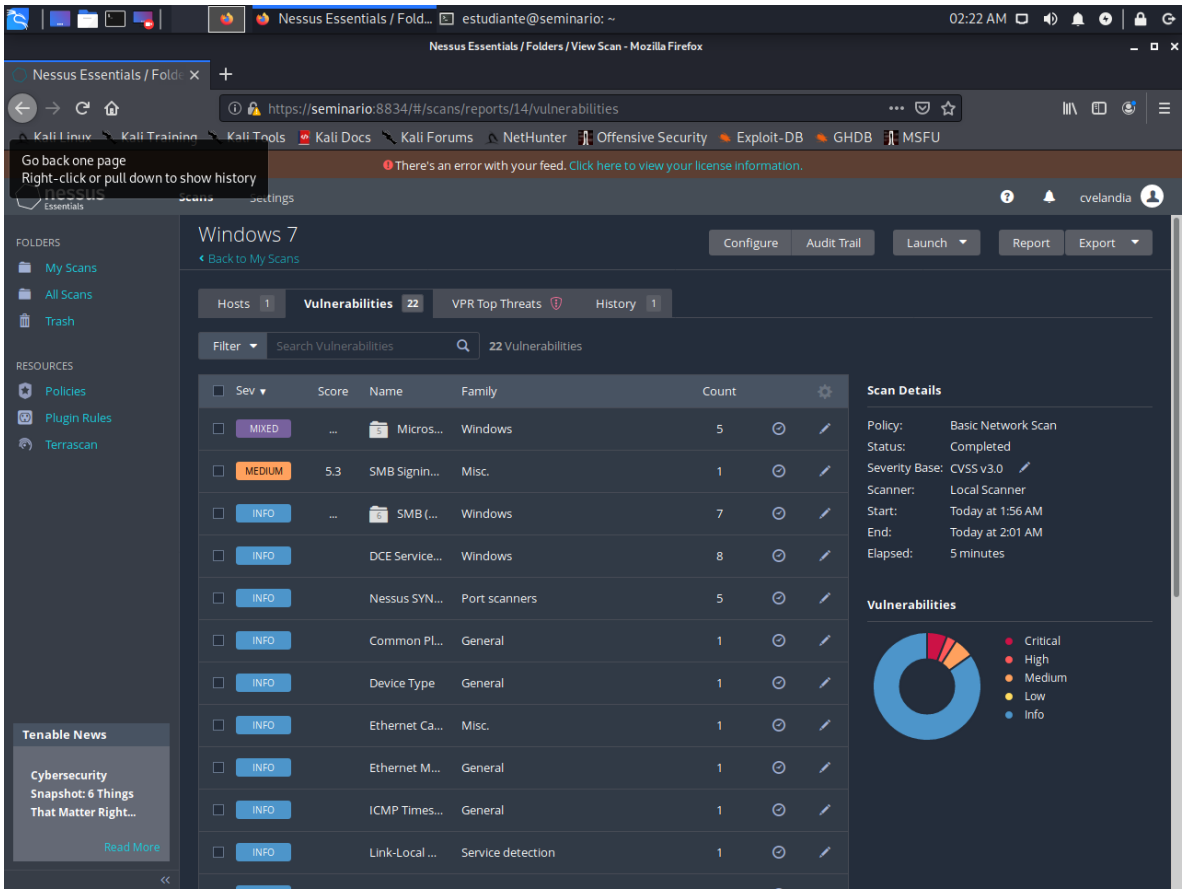
Fuente: elaboración propia.

Figura 12. Vulnerabilidades críticas



Fuente: elaboración propia.

Figura 13. Reporte total de vulnerabilidades agrupado por categorías



Fuente: elaboración propia.

Sobre la información suministrada para realizar la práctica, el primer elemento que llamó la atención en el análisis del anexo fue la mención al protocolo SMB versión 1. El protocolo es antiguo y ofrece una funcionalidad de comunicación y control entre máquinas, que permite el intercambio de información entre sistemas en una misma red, puede ser explotado para realizar ataques de DoS[7] y es la base del ransomware Wannacry[8]. El protocolo ha sido actualizado en múltiples ocasiones, buscando fortalecer los aspectos de seguridad que lo convierten en una vulnerabilidad explotable.

[7] Know How. "SMB (Server Message Block): definición, funciones y áreas de aplicación". IONOS Digital Guide. https://www.ionos.es/digitalguide/servidores/know-how/server-message-block-smb/ (accedido el 26 de septiembre de 2022).

[8] S. A. Tovar Balderas, R. A. González Ponce y D. García. "WannaCry: ataque mundial y consideraciones sobre ciberseguridad | Revista .Seguridad". Revista .Seguridad |. https://revista.seguridad.unam.mx/numero29/wannacry (accedido el 26 de septiembre de 2022).

En segundo lugar, llama la atención la fecha de actualización del sistema operativo, ya que la última actualización se realizó en febrero de 2017 y el ataque mundial del ransomware Wannacry se realizó en mayo de 2017[9], por lo que, las actualizaciones liberadas por Microsoft para contrarrestar este canal de ataque no se encuentran aplicadas a la máquina, esto marca el patrón de ataque para usar herramientas relacionadas con Wannacry. Esta información se relaciona con lo mencionado, respecto a la vulnerabilidad CVE-2017-0144 y la actualización de seguridad MS17-010[10], ambas relacionadas con el vector de ataque de Wannacry a través del protocolo SMBv1, con herramientas como EternalBlue[11].

La información obtenida permitió establecer que al menos una de las máquinas suministradas, sería vulnerable a ataques contra el protocolo SMBv1, que permitiría infectarla con otro tipo de amenazas capaces de realizar exfiltración de información, control de la máquina, suplantación, secuestro de datos o equipos, entre otros. La vulnerabilidad CVE-2017-0144 se constituye en una puerta trasera con capacidad de poner en riesgo no solo el equipo objetivo, sino toda la red en la que se encuentre y tenga visibilidad.

El recurso principal para identificar los fallos asociados al recurso fue Nmap, que en un escaneo sencillo ofreció amplia información sobre protocolos y puertos expuestos en la máquina. Si bien esta información no es suficiente para determinar un vector de ataque, si permite identificar que el recurso presenta múltiples puertas disponibles, por lo que basta con complementar el análisis con una herramienta que permita el escaneo de vulnerabilidades a profundidad. Para este efecto, se realizó un análisis posterior con Nessus, que permitió confirmar la información de los recursos expuestos, las vulnerabilidades asociadas, además de ofrecer información adicional sobre los exploits más comunes para su uso.

Para el caso del recurso, el protocolo SMBv1 era el vector de ataque más interesante para su explotación. El puerto expuesto para este protocolo es el 445/tcp, el cual se identificó tanto con Nmap como con Nessus. La vulnerabilidad identificada es una puerta trasera fácilmente explotable en un sistema sin las actualizaciones de seguridad requeridas ni una correcta configuración de puertos. El riesgo asociado a esta vulnerabilidad es la capacidad que tiene un atacante de utilizar este recurso para contagiar la máquina con otros exploits.

El uso más conocido dado a esta vulnerabilidad fue el ataque conocido como Wannacry y otros ataques derivados de la misma metodología, en los que, el

[9] Kaspersky. "¿Qué es el ransomware WannaCry?" www.kaspersky.es. https://www.kaspersky.es/resource-center/threats/ransomware-wannacry (accedido el 26 de septiembre de 2022).
[10] MITRE. "CVE -CVE-2017-0144". CVE -CVE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144 (accedido el 26 de septiembre de 2022).
[11] CSIRT-EPN. "MS17-010 EternalBlue SMB Remote Windows". CSIRT-EPN. https://www.csirt-epn.edu.ec/servicios/vulnerabilidades/58-ms17-010 (accedido el 27 de septiembre de 2022).

atacante obtenía control de la máquina objetivo, contagiaba a todos los recursos disponibles desde la máquina víctima y, posteriormente, realizaba la encriptación de todos los archivos de la máquina atacada. Este secuestro de recursos, conocido como Ransomware, iba acompañado de un mensaje de extorsión a la víctima, en la que se solicitaba un monto para entregar la contraseña que permitiera desencriptar los archivos.

El problema con este tipo de ataques, es que el atacante ha logrado tomar control total al menos del equipo víctima, por lo que puede exfiltrar información almacenada en la máquina, también tomar control de los recursos de la máquina para espiar a la víctima, secuestrar su información, convertir el equipo en un zombie para operaciones de minado o ataques DDoS, entre otros, sin contar con el riesgo al que expone al resto de recursos en la misma red.

2.4 ESTRATEGIAS BLUE TEAM

Ante el escenario de presenciar un ataque en tiempo real, la reacción instintiva sería apagar los sistemas o servidores que se encuentren bajo ataque, sin embargo, no es conveniente tomar este camino, ya que se eliminaría toda la evidencia en memoria, dificultando o incluso impidiendo determinar el grado de exposición de los activos de información de la compañía. En su lugar, se deben organizar los equipos y esfuerzos en tres grandes frentes o fases: Un frente de detección de amenazas, un frente de contención o limpieza y un frente de remediación.

El frente de detección debe realizar un análisis forense para identificar el vector de ataque utilizado, esto incluye análisis de puertos y tráfico de red con herramientas como Nmap o herramientas de firewall de la organización, el objetivo es poder identificar los puertos utilizados por el atacante y tráfico inusual en la red, ya que es posible que el atacante siga conectado a los sistemas. Una vez identificado el vector de ataque, se debe proceder a realizar un análisis de detección de malware para establecer los exploits utilizados, lo que permitirá entender el objetivo del atacante. Este análisis debe únicamente identificar la amenaza y aislarla al ponerla en cuarentena, no eliminarla, ya que esto podría destruir evidencias necesarias para posteriores acciones legales.

En esta fase se debe recolectar toda la información que sea posible para análisis inmediatos y futuros. El objetivo final de esta fase debe ser poder entender elementos como las vulnerabilidades que fueron utilizadas para realizar el ataque, el rol que jugaron actores de la organización y que permitieron que se realizara el ataque, si el ataque fue dirigido y especializado hacia la compañía o si hace parte de un ataque masivo, a qué recursos logró tener acceso el atacante, que elementos

como usuarios, contraseñas, atribuciones, etc., fueron comprometidos y deben ser cambiados, etc[12].

Una vez se han identificado las amenazas, se debe iniciar una fase de contención o limpieza, que requiere eliminar todo el software malicioso, así como todos los elementos que el atacante haya podido dejar en el sistema. También se deben aislar todos los elementos que hayan sido comprometidos, desconectándolos de la red, filtrando o redirigiendo su tráfico, desactivando accesos remotos y cambiando contraseñas comprometidas. El objetivo es poder contener la amenaza para evitar que se siga propagando, de forma tal que las próximas tareas se puedan enfocar en remover los elementos indeseados de los recursos comprometidos.

Toda la información que se pueda obtener, debe ser almacenada en medios extraíbles que posteriormente puedan ser utilizados en ambientes controlados y aislados, para poder analizarla y obtener datos importantes sobre el ataque que permitan robustecer la infraestructura de seguridad de la organización, así como obtener evidencias forenses que puedan ayudar a identificar al atacante y demostrar su relación con el evento. No se deben usar medios de almacenamiento conectados a la red de la organización, ya que pueden poner en riesgo los recursos a los que puedan tener acceso.

El protocolo de limpieza debe ser estricto y detallado, no debe quedar ningún recurso comprometido ni elementos introducidos al sistema por el atacante, ya que podrían continuar con la propagación. Para este fin pueden usarse herramientas como antivirus y antimalware, los elementos identificados y puestos en cuarentena deben ser transferidos a almacenamientos aislados y controlados para poder usarlos posteriormente en análisis. Todos los recursos de datos que fueron expuestos deben ser aislados, para poder analizarlos y recuperarlos con backups en la fase posterior, no se deben ejecutar procesos de restauración sin haber contenido y eliminado previamente la amenaza, ya que podría poner en riesgo todas las copias y respaldos de la organización.

Finalmente, se debe realizar una fase de recuperación y remediación del incidente. Con la amenaza controlada y eliminada, debe procederse a restaurar la información que pudo ser comprometida en su integridad, haciendo uso de los backups de la organización. De igual forma, aprovechando la información obtenida en las fases previas, se deben cambiar las contraseñas que puedan haber estado expuestas, también revisar los permisos asociados a las cuentas para identificar y corregir cualquier modificación no autorizada, como elevaciones de privilegios para usarlos como nuevos vectores de ataque futuros.

---

[12] A. Koshy. "How to Respond to a Cyber Attack?" How to Respond to a Cyber Attack? https://beaglesecurity.com/blog/article/how-to-respond-to-a-cyber-attack.html (accedido el 29 de septiembre de 2022).

Con la información obtenida, se deben identificar las vulnerabilidades de la organización, para poder aplicar las actualizaciones, parches y controles necesarios que cierren estas brechas. La prioridad en esta fase es cerrar todos los frentes para impedir ataques similares en el futuro. También debe ofrecer información para implementar controles de detección temprana, como herramientas para monitoreo de tráfico, alertas de acciones inusuales, agentes de descubrimiento, etc., que permitan hacer frente a la amenaza desde el primer momento, para minimizar el área de ataque y mitigar el impacto del ataque.

Se deben informar a las autoridades competentes acerca del ataque recibido, la información comprometida y las medidas tomadas para remediarlo, también se debe compartir toda la información obtenida de los procesos de identificación y contención, para el análisis forense de las autoridades. También es recomendable comunicar a los clientes acerca del ataque recibido, las medidas usadas para contenerlo y las soluciones implementadas para evitar su repetición, se debe poder transmitir un mensaje de confianza que evite incidentes de pánico futuros[13].

Una vez la organización se ha podido recuperar del incidente, se deben realizar análisis exhaustivos de la información recogida, con el fin de comprender las vulnerabilidades adicionales de la organización y definir planes de remediación para ellas. Esto puede comprender desde cambios en la arquitectura de la organización, adquisición de nuevas herramientas y controles de seguridad, medidas contra funcionarios comprometidos en caso de ataques internos, programas de formación en prevención y ciber seguridad para los funcionarios, etc. Con estas medidas posteriores, se pretender fortalecer la organización desde su cultura, sus equipos y su infraestructura para prevenir ataques futuros similares o de otro tipo.

Para mitigar la ocurrencia de estos eventos, se sugiere realizar procesos de hardenización sobre la infraestructura organizacional. El proceso de hardenización debe enfocarse en dificultar el actuar del atacante, no es posible generar un sistema invulnerable, pero si uno difícil de vulnerar, que demore al atacante, haciendo que el defensor gane tiempo valioso para detectar y controlar la amenaza. En el sistema presentado en el ejercicio de Red Team, se identificaron múltiples vulnerabilidades que pudieron ser explotadas para que el atacante lograra acceder al sistema, un proceso de hardenización puede cerrar esas brechas, dificultando el acceso para el enemigo.

Dentro de las medidas básicas a aplicar al sistema, está la instalación de actualizaciones y parches de sistemas operativos y software. En el ejercicio de Red Team se evidenció que vulnerabilidades por falta de actualizaciones pueden

[13] S. Bocceta. "Responding to Cyberattacks: 6 Top Tips". MSP Backup and IT Management Software Simplified. https://www.msp360.com/resources/blog/how-to-respond-to-cyberattacks/ (accedido el 29 de septiembre de 2022).

exponer al sistema a ataques de nivel de criticidad tan altos como el del ransomware Wannacry; la instalación de las actualizaciones de Windows habría actualizado la versión del protocolo SMBv1 a una versión más reciente, que no contenga la vulnerabilidad explotada por EternalBlue.

Otra medida importante es deshabilitar todos los servicios que no sean requeridos por el sistema, así como cerrar todos los puertos que no estén en uso. El proceso de hardenización debe llevar a la configuración de un sistema con funciones específicas y restricciones a todo lo que no sea requerido, este principio de confianza cero permite tener un monitoreo focalizado y estricto para detectar amenazas con facilidad, en lugar de un sistema con funciones y accesos no requeridos pero disponibles, que demanden un monitoreo amplio y costoso[14].

La configuración del firewall es una medida fundamental para prevenir ataques como el realizado en el ejercicio de Red Team. Una correcta configuración del firewall para regular la visibilidad entre los equipos, permitiría generar alertas ante el escaneo de puertos realizado con herramientas como NMap, así como habría bloqueado los intentos de acceso a la máquina por el puerto 445, usado en el ataque. Esta configuración se puede llevar hasta el punto de impedir que las máquinas sean visibles entre sí en la red de la organización, si esto no es requerido para la correcta ejecución de sus funciones.

Una correcta gestión de privilegios de administrador y la implementación de directorios activos de red, sumado al bloqueo de creación de usuarios locales, podría mitigar el riesgo de que un atacante cree usuarios con tales privilegios en la máquina, para saltar los controles establecidos.

Todo lo anterior puede acompañarse con la inversión en herramientas de seguridad que fortalezcan el sistema, como SIEM, DLP, antivirus, antimalware, etc. Estas herramientas permiten monitorear el sistema y generar alertas tempranas ante la ejecución de código malicioso, la extracción de datos o la generación de tráfico de red inusual. Todas estas alertas deben ser gestionadas para identificar las amenazas, notificar a los equipos de respuesta y permitir que actúen a tiempo para mitigar el impacto del ataque.

En el ejercicio de Red Team, se forzó el ataque mediante un payload con un troyano, ejecutado desde la máquina víctima. Este riesgo puede ser mitigado mediante la formación del personal de la organización en elementos de ciber seguridad y concientización ante amenazas. Una correcta formación de los equipos, puede ayudar a que identifiquen a tiempo este tipo de ataques y los reporte a los equipos de ciber seguridad, que podrán analizarlo en ambientes seguros y aislados, sin comprometer los recursos de la organización.

[14] CISET. "Hardening informático ¿Qué es?" CISET - Informática para empresas. https://www.ciset.es/publicaciones/blog/746-hardening (accedido el 29 de septiembre de 2022).

Una guía útil para el proceso de hardenización de la organización, así como para la implementación de buenas prácticas en materia de ciber seguridad es la guía de CIS. El Center for Internet Security CIS es una organización internacional sin ánimo de lucro, dedicada al diseño y promoción de mejores prácticas en lo referente al manejo de amenazas de ciber seguridad. La organización provee un marco de trabajo enfocado en las mejores prácticas en tres categorías diferentes: básicas, fundamentales y organizacionales. A su vez, el marco de trabajo se enfoca en tres categorías de tipo de empresa, en función de su tamaño y su nivel de madurez, definiendo marcos para categorías IG1, IG2 e IG3. La última versión de los controles recomendados por CIS es la 8 e incluye 153 medidas de seguridad[15].

El uso principal de las recomendaciones del CIS es aplicar mejores prácticas en la organización en materia de ciber seguridad. El alcance de IG1 son medidas básicas para la protección de cualquier empresa, sin importar su tamaño o nivel de madurez, esta sería la base de un proceso de hardenización y protección para la organización. Las medidas del grupo IG2 están enfocadas a compañías con capacidades económicas intermedias y activos de información expuestos, los controles ayudan a los equipos de seguridad a administrar los sistemas de control y proteger la información de la organización, son medidas útiles a la hora de estructurar un esquema de SOC para la organización y las políticas que lo rijan. Finalmente, el grupo IG3 están enfocadas a organizaciones de gran tamaño y gran capacidad de recursos económicos, que requieren proteger activos de información altamente sensibles y con un alto nivel de exposición, las medidas requieren la implementación de lo definido en IG1 e IG2 y fortalece el esquema con medidas adicionales enfocadas en la protección ante amenazas de alto nivel, como ataques dirigidos y atacantes de alto perfil.

El inventario de controles generales recogidos en el CIS, permiten comprender el enfoque y uso de las medidas recomendadas para su aplicación. En su orden, los controles incluyen el inventario y control de activos de hardware, inventario y control de activos de software, la gestión continua de vulnerabilidades, el control de privilegios de administrador, la configuración de hardware y software para todos los equipos, el monitoreo y análisis de logs de auditoría, la protección de recursos expuestos a internet como correos electrónicos o navegación web, la defensa contra malware, el control de puertos, protocolos y servicios, las funciones de recuperación de datos, la configuración de dispositivos de red, el uso de medidas de protección perimetral, la protección de datos, el control de accesos por necesidad, el control de acceso inalámbrico, el monitoreo de cuentas de usuario, la capacitación y concientización en temas de seguridad a los usuarios, la seguridad de aplicaciones,

[15] ManageEngine. "¿Qué son y cómo implementar los Controles de CIS (CIS Controls)?" ManageEngine - IT Operations and Service Management Software. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html (accedido el 29 de septiembre de 2022).

los planes de respuesta a incidentes y el desarrollo de pruebas de penetración. El enfoque de estos controles es construir una política de seguridad robusta, alineada con la implementación de controles de seguridad y la formación de los equipos.

3. VIDEO

En el link https://youtu.be/YVOWij5CVoc se puede acceder a la sustentación en video de la actividad.

4. CONCLUSIONES

Debido al amplio número de amenazas que se presentan en los entornos digitales, la legislación nacional e internacional ha establecido un marco jurídico para determinar la legalidad de las acciones cometidas por actores propios y ajenos y las sanciones correspondientes. Este marco jurídico determina las acciones que pueden realizar las organizaciones para medir la efectividad de sus sistemas y contrarrestar ataques, lo cual es utilizado por los equipos Red Team para poder establecer vulnerabilidades e identificar la superficie de exposición de los activos de información ante un posible ataque. A su vez, los equipos Blue Team utilizan esta información y toda la que puedan recolectar en sus acciones de monitoreo y análisis para establecer medidas de remediación de vulnerabilidades.

Las acciones de los equipos Red Team y Blue Team son fundamentales para proteger la integridad de los sistemas de las organizaciones, pues combinan la detección de vulnerabilidades y amenazas, con la aplicación de medidas de protección proactivas, para mitigar el riesgo ante posibles ataques informáticos. Toda organización o persona que interactúe en el ciber espacio es susceptible a ser el objetivo de un atacante, por lo que, deben contemplarse todas las medidas que puedan aplicarse para hacer su entorno más seguro.

5. RECOMENDACIONES

Todas las organizaciones, sin importar su naturaleza o tamaño, deben contar con una política de ciber seguridad, que les permita establecer los controles mínimos a implementar para su protección. Elementos básicos como la actualización de sistemas operativos, el uso de software legal actualizado y la implementación de un antivirus y un firewall (incluyendo los nativos del sistema operativo), pueden ser fundamentales a la hora de impedir un ataque informático a la infraestructura a proteger.

Organizaciones de mayor tamaño y con activos informáticos que puedan considerarse de mayor valor, cuentan con una superficie de ataque más amplia, por lo que, es su obligación implementar mayores controles, desarrollar políticas más robustas e incorporar a su cultura y procesos buenas prácticas en materia de ciber seguridad. El uso de marcos de trabajo y guías es un buen punto de inicio para el camino a recorrer.

Las organizaciones que tengan las capacidades, deben evaluar la posibilidad de incorporar equipos Blue Team y Red Team a sus protocolos de ciber seguridad, esto otorgará capacidades de diagnóstico preventivo, ejecución de pruebas de pentesting y construcción de planes de remediación preventivos. El objetivo de incorporar estos equipos es fortalecer la estrategia de seguridad desde la prevención y no desde la contención.

BIBLIOGRAFÍA

Superintendencia de Industria y Comercio [página web]. [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

LEY 1581 de 2012 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#:~:text=La%20presente%20ley%20tiene%20por,el%20artículo%2015%20de%20la>.

COLOMBIA SE adhiere al Convenio de Budapest contra la ciberdelincuencia | Cancillería [Anónimo]. Cancillería | Ministerio de Relaciones Exteriores de Colombia [página web]. [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia#:~:text=Colombia%20se%20adhiere%20al%20Convenio%20de%20Budapest%20contra%20la%20ciberdelincuencia,-2020-03-17&text=Estrasburgo%20(mar.,la%20lucha%20contra%20la%20ciberdelincuencia>.

COUNCIL OF EUROPE. Convenio sobre la ciberdelincuencia. (23, noviembre, 2001). [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.oas.org/juridico/english/cyb_pry_convenio.pdf>.

EC-COUNCIL. Understanding the Five Phases of the Penetration Testing Process. Cybersecurity Exchange [página web]. [Consultado el 3, septiembre, 2022]. Disponible en Internet: <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/>.

HERNÁNDEZ, Mikel. ¿Cuál Son La 5 Fases Del Pentesting? - Ciberseguridad. Bidaidea: líderes en Ciberseguridad & Inteligencia [página web]. (21, marzo, 2022). [Consultado el 4, septiembre, 2022]. Disponible en Internet: <https://ciberseguridadbidaidea.com/fases-del-pentesting/>.

Know How. "SMB (Server Message Block): definición, funciones y áreas de aplicación". IONOS Digital Guide. https://www.ionos.es/digitalguide/servidores/know-how/server-message-block-smb/ (accedido el 26 de septiembre de 2022).

S. A. Tovar Balderas, R. A. González Ponce y D. García. "WannaCry: ataque mundial y consideraciones sobre ciberseguridad | Revista .Seguridad". Revista

.Seguridad |. https://revista.seguridad.unam.mx/numero29/wannacry (accedido el 26 de septiembre de 2022).

Kaspersky. "¿Qué es el ransomware WannaCry?" www.kaspersky.es. https://www.kaspersky.es/resource-center/threats/ransomware-wannacry (accedido el 26 de septiembre de 2022).

MITRE. "CVE -CVE-2017-0144". CVE -CVE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144 (accedido el 26 de septiembre de 2022).

CSIRT-EPN. "MS17-010 EternalBlue SMB Remote Windows". CSIRT-EPN. https://www.csirt-epn.edu.ec/servicios/vulnerabilidades/58-ms17-010 (accedido el 27 de septiembre de 2022).

A. Koshy. "How to Respond to a Cyber Attack?" How to Respond to a Cyber Attack? https://beaglesecurity.com/blog/article/how-to-respond-to-a-cyber-attack.html (accedido el 29 de septiembre de 2022).

S. Bocceta. "Responding to Cyberattacks: 6 Top Tips". MSP Backup and IT Management Software Simplified. https://www.msp360.com/resources/blog/how-to-respond-to-cyberattacks/ (accedido el 29 de septiembre de 2022).

CISET. "Hardening informático ¿Qué es?" CISET - Informática para empresas. https://www.ciset.es/publicaciones/blog/746-hardening (accedido el 29 de septiembre de 2022).

ManageEngine. "¿Qué son y cómo implementar los Controles de CIS (CIS Controls)?" ManageEngine - IT Operations and Service Management Software. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html (accedido el 29 de septiembre de 2022).