Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Jorge Eduardo Ruiz Sánchez

Asesor

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2025

Resumen

La información es el recurso más valioso para las empresas en la actualidad. Su manejo y resguardo son fundamentales, ya que se comparte no solo de manera física y en dispositivos de almacenamiento, sino también a través de correos electrónicos, redes sociales, plataformas en la nube y otros medios digitales. Esta variedad de formas de transmisión y almacenamiento expone la información a diversas vulnerabilidades y riesgos, especialmente a ataques cibernéticos. Un hackeo, la filtración o la pérdida de información pueden provocar serias complicaciones, no solo para las empresas, sino también para los gobiernos, comprometiendo la economía, la reputación y la seguridad de las instituciones.

Los especialistas en ciberseguridad son profesionales altamente capacitados, que cuentan con habilidades y conocimientos específicos para mitigar estos riesgos. Su trabajo se enfoca en el análisis detallado de redes y sistemas de información, empleando herramientas avanzadas para llevar a cabo pruebas de penetración, gestión de incidentes e identificación de amenazas. Estos profesionales son esenciales para implementar protocolos de seguridad que resguarden la integridad de la información y reduzcan el efecto de posibles ataques.

Dentro del campo de la ciberseguridad, hay equipos especializados conocidos como Red Team y Blue Team, que juegan un papel fundamental en la protección de las organizaciones frente a ciberataques sofisticados. Los equipos Red Team se enfocan en simular ataques., intentando superar las defensas de la organización para descubrir posibles vulnerabilidades. Su enfoque proactivo ayuda a las empresas a reconocer sus debilidades y a reforzar sus sistemas. En contraste, los equipos Blue Team se enfocan en mantener y optimizar las defensas existentes, implementando medidas de seguridad y vigilando continuamente las redes para identificar y reaccionar ante cualquier amenaza en tiempo real.

La colaboración entre estos dos equipos es esencial para crear un entorno seguro. Mientras que el Red Team desafía las defensas, el Blue Team trabaja para reforzarlas, generando un ciclo de mejora continua en la seguridad de la información. Esta dinámica es vital en un mundo donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes.

Palabras clave: Amenazas, Blue team, Información, Red Team, Riesgos, Vulnerabilidades

Abstract

Information is the most valuable resource for companies today. Its management and protection are fundamental, as it is shared not only physically and on storage devices but also through emails, social media, cloud platforms, and other digital means. This variety of transmission and storage methods exposes information to various vulnerabilities and risks, especially from cyberattacks. A hack, data breach, or loss of information can lead to serious complications, not only for companies but also for governments, compromising the economy, reputation, and security of institutions.

Cybersecurity specialists are highly trained professionals with specific skills and knowledge to mitigate these risks. Their work focuses on the detailed analysis of networks and information systems, employing advanced tools to conduct penetration testing, incident management, and threat identification. These professionals are essential for implementing security protocols that safeguard information integrity and reduce the impact of potential attacks.

Within the field of cybersecurity, there are specialized teams known as Red Team and Blue Team, which play a fundamental role in protecting organizations against sophisticated cyberattacks. Red Team members focus on simulating attacks, attempting to breach the organization's defenses to uncover potential vulnerabilities. Their proactive approach helps companies recognize their weaknesses and strengthen their systems. In contrast, Blue Team members focus on maintaining and optimizing existing defenses, implementing security measures, and continuously monitoring networks to identify and respond to any threats in real-time.

Collaboration between these two teams is essential for creating a secure environment. While the Red Team challenges the defenses, the Blue Team works to reinforce them, generating a cycle of continuous improvement in information security. This dynamic is vital in a world where cyber threats are becoming increasingly sophisticated and frequent.

Keywords: Blue Team, Information, Red Team, Risks, Threats, Vulnerabilities.

Tabla de Contenido

Lista de figuras

Lista de tablas

Lista de Apendices

Introducción

Para las organizaciones es de suma importancia proteger sus datos, y evitar que puedan ser alterados, robados, secuestrados, o estar expuestos a muchas otras incidencias que traigan consecuencias irreparables para los objetivos del negocio. De ahí proviene la necesidad de disponer de personal calificado, normas y procedimientos que faciliten la creación de un Sistema de Gestión de Seguridad de la Información (SGSI) robusto, alineado con los fundamentos de la seguridad informática, tales como la confidencialidad, la integridad y la disponibilidad de la información.

Las tecnologías de la información se encuentran en constante evolución, y actualmente se comparten grandes cantidades de información a través de los distintos medios y herramientas que esta nos ofrece. Al estar compartida a través de redes como el internet, la información está expuesta a ataques informáticos, ejecutados por parte de ciberdelincuentes, quienes estudian y aprovechan las vulnerabilidades de las organizaciones.

Los profesionales de ciberseguridad, además de su conocimiento, cuentan con una serie de herramientas de hardware y software en las que se pueden apoyar para minimizar riesgos, y proteger de forma efectiva los activos tecnológicos. También existen una serie de pruebas como las de intrusión o pentesting, que permiten poner a prueba los sistemas de seguridad implementados por las empresas, evidenciar vulnerabilidades, y ejecutar las correcciones que se consideren pertinentes. A estos grupos de especialistas expertos en realizar este tipo de pruebas se les conoce como “Red Team” y “Blue Team”.

En el presente documento analizaremos los estándares, metodologías, estrategias, y herramientas utilizadas por estos equipos especializados, así como los principales ataques y

vulnerabilidades a las que hacen frente, y los beneficios que representa para las organizaciones contar con ellos.

Planteamiento del Problema

La tecnología avanza a un ritmo vertiginoso, transformando continuamente la forma en que las entidades implementan sus procesos. Este progreso ha permitido optimizar numerosas tareas que anteriormente se realizaban de forma manual, resultando en mejoras significativas en eficiencia y productividad. Sin embargo, este mismo avance ha dado lugar a un entorno donde se comparten enormes volúmenes de información a través de Internet y redes internas.

Aunque existen herramientas creadas para asegurar la privacidad, integridad y disponibilidad de la información, hay muchas aplicaciones que promueven el hurto o la modificación de dicha información, lo cual puede generar graves problemas a las entidades impactadas. En Colombia, aunque el panorama ha mostrado avances positivos durante los utimos años, la situación sigue siendo precaria. Muchas empresas y entidades gubernamentales han incorporado profesionales en ciberseguridad, pero este campo aún se encuentra descuidado en numerosas organizaciones.

La falta de políticas de seguridad claramente definidas y de Sistemas de Gestión de Seguridad de la Información (SGSI) eficientes, junto con la ausencia de grupos de expertos en ciberseguridad debidamente organizados, dificulta la capacidad para abordar las amenazas de manera efectiva. Esta desconsideración hacia la seguridad informática podría tener un impacto negativo en la estructura organizacional y en el cumplimiento de los objetivos empresariales.

En Colombia, varias entidades han sido víctimas de ciberataques. Un ejemplo notable es el ataque cibernético que sufrió la Universidad de los Andes en 2021, donde un caso de ransomware afectó su sistema de gestión académica, obligándola a suspender actividades académicas y enfrentarse a pérdidas económicas significativas. Asimismo, en noviembre de 2022, la EPS Sanitas fue víctima de un ciberataque perpetrado por la banda de hackers conocida

como Ransomhouse, que comprometió el sistema de Keralty, contratado por la empresa para almacenar datos digitales, incluyendo información confidencial de colaboradores y proveedores, así como historias clínicas de pacientes.

Estos ejemplos evidencian la urgente necesidad de contar con equipos especializados dedicados a monitorear y responder a amenazas cibernéticas, cuyas prácticas podrían haber prevenido la materialización de estos ataques. La colaboración entre los equipos Red Team y Blue Team es esencial para minimizar riesgos y reforzar la seguridad de la información.

Formulación del Problema

¿Cómo pueden los equipos de seguridad Red Team y Blue Team colaborar para proteger de manera efectiva los sistemas y datos críticos de una organización, y cuál es su impacto en la defensa contra amenazas cibernéticas?

Justificación

Colombia sobresale como uno de los países con mayor progreso tecnológico en Latinoamérica; sin embargo, a nivel global, su posición sigue siendo inferior en comparación con naciones líderes en la industria, como Estados Unidos y varios países europeos. Esta situación es especialmente crítica en el ámbito de la ciberseguridad, donde el país enfrenta retos significativos que requieren atención inmediata.

A lo largo de los cambios de gobierno, la ciberseguridad ha sido descuidada, ya que se ha priorizado la atención a problemas económicos y sociales que demandan un enfoque más inmediato por parte del Estado. Sin embargo, esta falta de atención puede acarrear consecuencias graves tanto para las organizaciones del sector público como para las del sector privado. En 2022, 34 compañías en Colombia, incluyendo entidades relevantes como EPM, Sanitas, la Fiscalía General, Viva Air y la Universidad Javeriana, sufrieron ciberataques. Estos incidentes no solo afectaron negativamente la reputación de las organizaciones, sino que también provocaron serias repercusiones para miles de usuarios de los servicios que estas ofrecen.

egún FortiGuard Labs, en 2023, Colombia tuvo 12.000 millones de intentos de ciberataques, menos que los 20.000 millones de 2022. Sin embargo, la situación empeoró en 2024, cuando el país sufrió 36.000 millones de intentos de ataque, según un informe de Fortinet. Estas cifras muestran que la actividad de ciberseguridad en Colombia varía mucho. Aunque la baja en 2023 puede parecer positiva, el gran aumento en 2024 muestra que las amenazas cibernéticas son más complejas y específicas, lo que resalta la necesidad de que las organizaciones estén alertas y se adapten a los cambios en el panorama de amenazas. Este aumento preocupante se debe, en gran parte, a la falta de personal capacitado en ciberseguridad, lo que hace que muchos equipos estén sobrecargados de trabajo y bajo mucha presión.

Expertos en seguridad informática han advertido sobre la urgente necesidad de robustecer el sistema nacional de defensa cibernética del país y sus principales entidades. A pesar de que este tema ha sido abordado a nivel político, muchas iniciativas han quedado en meras declaraciones sin una implementación efectiva. La ausencia de un marco robusto de ciberseguridad ha llevado a incidentes que han comprometido información sensible de empresas y usuarios, lo que resalta la necesidad de una reaccion coordinada y eficaz para mejorar las estrategias y controles.

La situación actual resalta la importancia de elaborar estrategias específicas y duraderas que enfrenten los riesgos vinculados a la ciberseguridad. Esto abarca el establecimiento de políticas sólidas, la inversión en tecnologías de seguridad innovadoras, y la formación constante profesionales en el área. Solo así se podrá construir un entorno digital más seguro y resiliente, capaz de enfrentar amenazas cibernéticas en constante evolución.

Es crucial que el gobierno y las empresas trabajen conjuntamente para establecer un marco de ciberseguridad que no solo proteja datos y sistemas críticos, sino que también fomente la confianza en la implementación de la tecnología en todos los ámbitos de la sociedad. La creación de equipos expertos en ciberseguridad, tales como Red Team y Blue Team, facilitará a las entidades colombianas una mejor preparación para afrontar ataques informáticos avanzados.

Por lo tanto, la ciberseguridad en Colombia debe ser priorizada y fortalecida mediante estrategias concretas y colaborativas. Gracias a ejercicios simulados y exitosos ejecutados por el Red Team, el Blue Team podrá ajustar las políticas de seguridad y controles para cerrar las brechas identificadas. Este enfoque proactivo es fundamental porque fomentará un ciclo de mejora continua en la seguridad. dado que las amenazas cibernéticas evolucionan rápidamente y requieren respuestas ágiles. Solo a través de una visión integral que incluya la formación de

equipos especializados y la puesta en marcha de políticas sólidas, se podrá construir un entorno digital seguro y resiliente que proteja tanto a las instituciones públicas como al sector privado.

Objetivos

Objetivo General

Analizar el papel de los equipos de seguridad Red Team y Blue Team, así como su impacto en la protección de las organizaciones contra las amenazas cibernéticas

Objetivos Específicos

Revisar la normatividad y los estándares de seguridad vigentes en la protección contra ciberdelitos, entendiendo cómo estas prácticas pueden fortalecer la necesidad de implementar equipos de seguridad Red Team y Blue Team en las organizaciones.

Investigar la integración de metodologías y herramientas empleadas por los equipos de seguridad Red Team y Blue Team para evaluar la seguridad de los sistemas de información y la efectividad de los controles de seguridad establecidos.

Identificar las vulnerabilidades y los tipos de ataques informáticos más frecuentes, así como el papel que desempeñan los equipos de seguridad Red Team y Blue Team en su mitigación

Demostrar los beneficios que obtienen las organizaciones al incorporar equipos de seguridad Red Team y Blue Team en sus estrategias de ciberseguridad, y cómo estos equipos pueden fortalecer la protección de sus sistemas y datos esenciales

Conceptos Equipos de Seguridad

Equipos Blue Team

El Blue Team es el equipo encargado de proteger a las organizaciones contra posibles ataques de manera activa y preventiva. Su principal tarea es analizar las amenazas que podrían afectar a la empresa y tomar medidas para reducir los riesgos. Esto incluye la vigilancia constante de la red, los sistemas, las aplicaciones y otros recursos tecnológicos, además de proponer planes de acción para fortalecer la seguridad.

Cuando ocurre un incidente, el Blue Team se encarga de responder rápidamente para minimizar los daños. Esto implica varias actividades, como:

- Investigar lo sucedido a través de análisis forenses en las máquinas o sistemas afectados para entender cómo ocurrió el ataque.
- Identificar el camino del ataque para determinar los pasos que siguió el atacante para acceder a los sistemas (trazabilidad del ataque).
- Proponer estrategias y soluciones para reparar los daños y evitar que algo similar vuelva a suceder.
- Implementar medidas para identificar futuros ataques de manera más rápida y eficiente.

Principales Funciones de Blue Team:

- Realizar un inventario de los activos que requieren protección para llevar a cabo una evaluación de riesgo.
- Organizar campañas de concientización para el personal involucrado, fomentando una cultura de seguridad.
- Ejecutar revisiones periódicas de los sistemas y la infraestructura de red.
- Evaluar riesgos y desarrollar planes y estrategias para su mitigación.
- Realizar auditorías del DNS para prevenir ataques de phishing y reducir amenazas tanto al DNS como a la web.
- Instalar y mantener actualizado el software de seguridad en todos los equipos informáticos y dispositivos.
- Establecer controles rigurosos de acceso a los recursos y equipos tecnológicos.
- Desplegar software de detección y prevención de intrusiones (IDS e IPS), así como herramientas de exploración de vulnerabilidades.
- Implementar soluciones de gestión de eventos e información de seguridad (SIEM) para registrar y analizar la actividad de la red.
- Analizar los registros y la memoria del sistema para identificar actividades inusuales y detectar ataques a tiempo.
- Verificar la configuración de la red para asegurar su correcto funcionamiento.
- Proteger los sistemas informáticos mediante la instalación de software antivirus o antimalware.

Etapas de las Operaciones del Blue Team

El Blue Team, responsable de la defensa activa y reactiva de los sistemas de información de una organización, tiene como objetivo principal proteger, detectar y responder a las amenazas cibernéticas que pueden poner en riesgo la seguridad de la infraestructura tecnológica. A diferencia del Red Team, que simula ataques para identificar vulnerabilidades, el Blue Team opera en tiempo real para prevenir intrusiones, reducir riesgos y asegurar la continuidad de las operaciones.

El trabajo del Blue Team se basa en la implementación de estrategias, herramientas y marcos tecnológicos que permiten monitorear, analizar y responder a incidentes. Este enfoque defensivo es esencial para cualquier organización que busque protegerse contra la creciente sofisticación de los ataques cibernéticos.

Este equipo sigue un conjunto de pasos clave para garantizar la seguridad de la organización:

Monitoreo Continuo. Utiliza herramientas como sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS) y plataformas de gestión de eventos e información de seguridad (SIEM) para supervisar continuamente las actividades en la red. Por ejemplo, herramientas como Splunk o IBM QRadar permiten identificar patrones anómalos que podrían indicar un ataque.

Identificación de Amenazas. Una vez detectadas actividades sospechosas, el equipo analiza los datos recopilados para identificar posibles amenazas. Esto incluye el análisis de logs, tráfico de red y comportamientos inusuales. Por ejemplo, un incremento inesperado en los intentos de acceso podría señalar un ataque de fuerza bruta.

Respuesta a Incidentes. El Blue Team pone en marcha estrategias de reacción que abarcan el control del ataque, la reducción de sus impactos y la restauración del sistema. Un ejemplo reciente es el ataque de ransomware a la empresa Kaseya en 2021, donde las respuestas rápidas de los equipos defensivos ayudaron a minimizar el impacto.

Fortalecimiento de la Seguridad. Después de un incidente, el Blue Team realiza un estudio post-mortem para identificar las razones del ataque y robustecer las defensas.. Esto puede abarcar la actualización de firewalls, la adopción de políticas de contraseñas más rigurosas o la formación de los empleados en ciberseguridad.

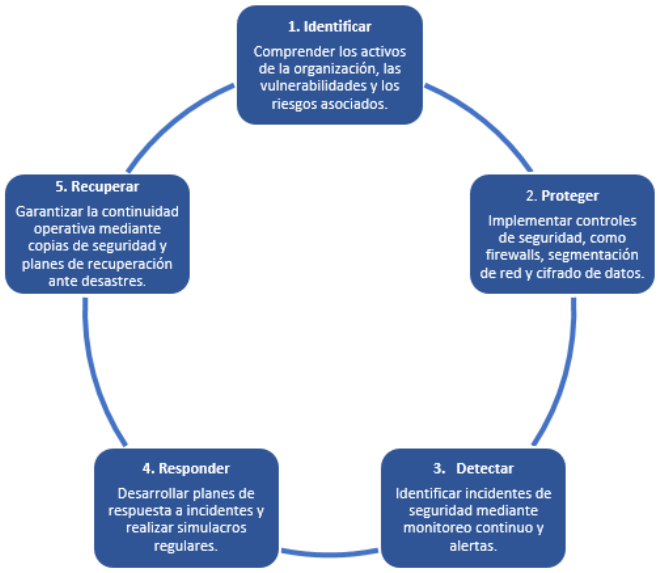
Colaboración con el Red Team. En ejercicios de Purple Teaming, el Blue Team trabaja junto con el Red Team para identificar y remediar vulnerabilidades de manera proactiva. Este enfoque colaborativo permite mejorar las defensas antes de que los atacantes puedan aprovecharlas.

Algunos Frameworks Utilizados por el Equipo Blue Team

NIST Cybersecurity Framework. Es un marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) que ofrece una estrategia organizada para identificar, salvaguardar, identificar, reaccionar y recuperar sistemas frente a ataques informáticos. Este framework se utiliza extensamente por los Blue Teams para asegurar la capacidad de resistencia de las organizaciones ante amenazas, y comprende las siguientes etapas:

Figura 1

Etapas del framework NIST

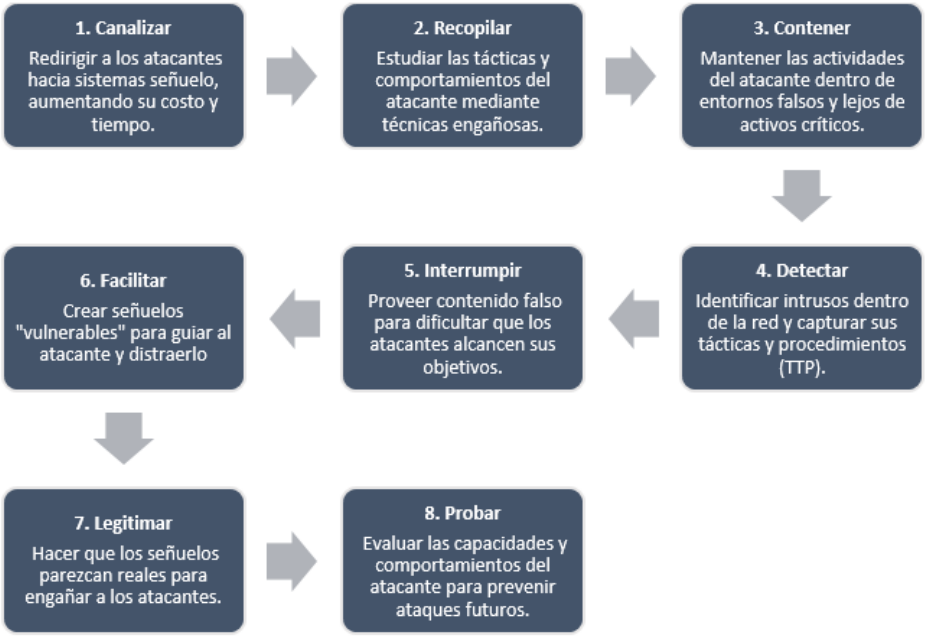


Nota. Elaboración propia.

MITRE Shield. Complementa al framework ATT&CK y se enfoca en las tácticas defensivas que puede implementar el Blue Team para contrarrestar las técnicas utilizadas por los atacantes. Este marco incluye estrategias como el engaño, la segmentación de redes y el monitoreo avanzado.

Figura 2

Tácticas del MITRE Shield



Nota. Elaboración propia.

Equipos Red Team

Los Red Teams se encargan de simular el comportamiento de los atacantes reales, utilizando herramientas y técnicas similares a las que ellos emplearían. Su meta es identificar y utilizar las vulnerabilidades presentes en los sistemas, aplicaciones o redes de una entidad. Esto incluye el uso de métodos como los exploits (para aprovechar fallos de seguridad) y el pivoting (que consiste en moverse de una máquina comprometida a otras dentro de la red). De esta forma, el Red Team recrea escenarios de ataque realistas para evaluar la capacidad de la organización de enfrentar amenazas.

El propósito principal del Red Team es analizar la seguridad desde la perspectiva de un atacante, ayudando al equipo de seguridad interno, conocido como Blue Team, a mejorar sus

defensas. Este proceso se realiza de manera controlada y constructiva, permitiendo a la organización prepararse mejor frente a ataques reales.

Principales Funciones de Red Team

- Definir qué activos se utilizarán para realizar pruebas y establecer las técnicas de ataque a emplear.
- Identificar los activos más expuestos en función de los objetivos de la evaluación, detectando posibles vulnerabilidades que faciliten una intrusión.
- Localizar vulnerabilidades críticas que permitan el acceso no autorizado a los sistemas.
- Una vez identificado el activo más vulnerable, se debe organizar el ingreso a la red interna, un procedimiento que puede variar en tiempo de ejecución dependiendo del grado de protección de la compañía.
- Planificar rutas de acceso secundarias para los ataques, en caso de que el Blue Team detecte y contenga la intrusión.
- Con acceso completo a la organización, evaluar cuáles activos podrían resultar más perjudicados ante un ataque.

La implementación de una estrategia combinada entre los equipos Red y Blue permite a las organizaciones beneficiarse de enfoques y habilidades complementarias. Esta cooperación crea un clima de rivalidad sana que potencia el desempeño de ambos equipos. Aunque el Red Team es útil para detectar vulnerabilidades y destacar la condición actual del sistema, el Blue Team es

crucial para proporcionar protección a largo plazo, garantizando que las defensas se conserven sólidas mediante una vigilancia continua.

Dentro de los ejercicios realizados por el Red Team se incluyen:

Pruebas de Penetración. Las pruebas de penetración consisten en simular un ataque para intentar acceder a un sistema, generalmente utilizando diversas herramientas de software. Un ejemplo es John the Ripper, un programa diseñado para descifrar contraseñas, que permite identificar el tipo de cifrado utilizado y tratar de eludirlo.

Phishin. La suplantación de identidad, o phishing, hace referencia al envío de emails que parecen ser auténticos, con la intención de engañar a los empleados para que realicen acciones como ingresar sus credenciales en un sitio web controlado por el atacante.

Herramientas de Interceptación de Comunicaciones. Existen herramientas como rastreadores de paquetes y analizadores de protocolos que pueden ser empleadas para mapear redes o leer mensajes transmitidos, obteniendo información sobre el sistema. Si un atacante determina que un servidor opera con un sistema operativo de Microsoft, dirigirá sus esfuerzos hacia la explotación de las vulnerabilidades específicas de esa plataforma.

Clonación de Tarjetas de Seguridad. Esta técnica se emplea para acceder a áreas restringidas, como salas de servidores.

Etapas de las Operaciones del Red Team

El Red Teaming es una estrategia avanzada de ciberseguridad implementada por las organizaciones, para evaluar la efectividad de sus estrategias de defensa mediante simulaciones realistas de ataques cibernéticos. Este enfoque se basa en la emulación de tácticas, técnicas y procedimientos utilizados por ciberdelincuentes, con el objetivo de identificar vulnerabilidades y fortalecer la postura de seguridad de una organización. La metodología del Red Teaming sigue un conjunto de etapas bien definidas que se apoyan en frameworks reconocidos internacionalmente, como MITRE ATT&CK y Cyber Kill Chain, los cuales proporcionan un marco estructurado para analizar y simular ciberataques.

El proceso de simulación llevado a cabo por el Red Team puede dividirse en varias fases

Establecimiento de un Objetivo. Consiste en definir un objetivo claro para la simulación. Por ejemplo, el objetivo podría ser exponer información sensible de la empresa, comprometer sistemas críticos o evaluar la eficacia de las acciones de respuesta ante incidentes.

Reconocimiento del Objetivo. En esta fase, el equipo recolecta datos acerca de la entidad, que incluyen aplicaciones, trabajadores, redes e infraestructuras físicas. Este factor es vital, dado que una vigilancia insuficiente de la seguridad física puede convertirse en un sitio de entrada para ataques cibernéticos. Por ejemplo, un intruso podría acceder a las instalaciones, entrar a servidores o estaciones de trabajo, extraer información sensible o instalar malware. El 20% de los ataques cibernéticos exitosos se inician con el acceso físico no autorizado.

Explotación de Vulnerabilidades. El equipo utiliza diversos vectores de ataque, como el phishing, contraseñas débiles o credenciales comprometidas, para obtener acceso inicial al sistema. Por ejemplo, en 2022, un ataque a través de phishing permitió a un grupo de hackers acceder a los sistemas de una gran empresa de tecnología, comprometiendo datos de clientes y empleados.

Escalada de Privilegios. Una vez dentro del sistema, el Red Team intenta escalar privilegios, explorando vulnerabilidades adicionales para obtener acceso a recursos más críticos, como servidores o bases de datos.

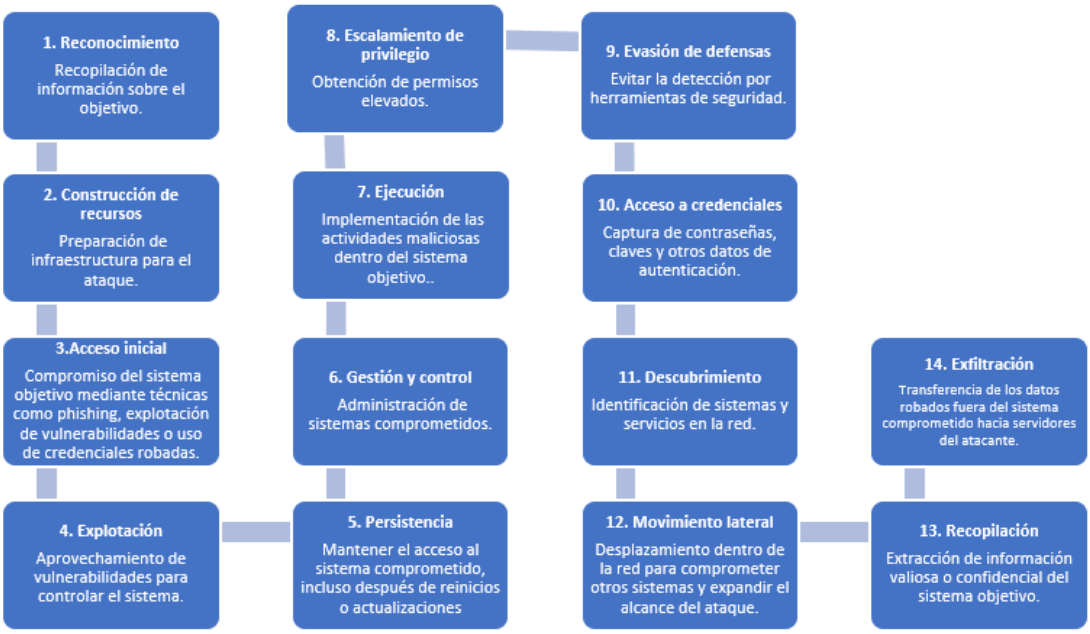
Informe y Remediación. Después de finalizar la simulación, el equipo registra las debilidades identificadas y ofrece recomendaciones concretas para su mitigación. Este informe es crucial para que la organización pueda llevar a cabo mejoras en sus medidas de seguridad.

Algunos Frameworks Utilizados por el Equipo Red Team

MITRE ATT&CK. El framework MITRE ATT&CK clasifica las estrategias y métodos empleados por los oponentes en ciberataques. Este modelo es ampliamente utilizado por los equipos de Red Team para estructurar sus simulaciones y garantizar que abarcan todas las posibles fases del ataque.

Figura 3

Tácticas del MITRE ATT&CK



Nota. Elaboración propia.

CYBER KILL CHAIN. El modelo Cyber Kill Chain, desarrollado por Lockheed Martin, proporciona otro enfoque para analizar ciberataques. Este framework se centra en las etapas de un ataque desde el reconocimiento hasta las acciones finales sobre el objetivo, destacando la importancia de interrumpir el ataque en las primeras fases.

Figura 4

Etapas del modelo Cyber Kill Chain

Nota. Elaboración propia.

Pruebas de Penetración

Las pruebas de intrusion son un proceso ordenado para identificar falencias en programas informáticos y redes digitales. Este tipo de estudio de seguridad informática analiza la protección de un sistema o red a través de la simulación de un ataque virtual, con el objetivo de detectar potenciales vulnerabilidades antes de que sean utilizadas por atacantes reales.

Se llevan a cabo con el consentimiento de la entidad y su objetivo primordial es detectar deficiencias en sistemas, software y redes. Asimismo, permiten analizar las repercusiones que podría acarrear una vulnerabilidad si se aprovecha, establecer las medidas correctivas necesarias

para reducir los riesgos, fortalecer la seguridad y garantizar la adherencia a normas y regulaciones de protección.

Por otra parte, estas evaluaciones son valiosas para comprobar la conformidad con políticas de seguridad internas, evaluar el grado de sensibilización de los empleados respecto a dichas políticas e identificar la capacidad de la entidad para reaccionar ante incidentes de seguridad.

Delito Informático

Se refiere a cualquier acción ilegal realizada a través de sistemas de computación, redes o datos digitales, que impacta en la privacidad, integridad y disponibilidad de la información. Estos crímenes abarcan diversas actividades delictivas, como el acceso indebido a sistemas, el hurto de información y el fraude en línea, entre otros. Dado que estos actos pueden realizarse de forma rápida y fácil, frecuentemente se ejecutan en tan solo unos segundos, utilizando únicamente un dispositivo informático y sin requerir la presencia física en el lugar del crimen. Además, el incremento y progreso continuo de los delitos informáticos dificultan aún más su detección y seguimiento, lo que convierte la ciberseguridad en un desafío constante para las organizaciones y las personas, quienes deben estar siempre alertas y preparadas para enfrentar estas amenazas en evolución.

Vulnerabilidades

Son fallas, debilidades o errores presentes en sistemas, programas, redes o recursos tecnológicos que pueden ser utilizados por ciberdelincuentes para provocar daños. Estas vulnerabilidades funcionan como puertas abiertas que facilitan a los intrusos accesos no autorizados, el robo de datos, la afectacion de servicios, o la toma de control de un sistema.

Dentro de las principales causas de vulnerabilidades se encuentran errores de configuración, falta de actualizaciones, fallas en el diseño, y errores humanos.

Ingeniería Social

La ingeniería social es una técnica que se basa en manipular a las personas utilizando estrategias psicológicas para influir en sus decisiones o acciones. En el ámbito de la seguridad informática, esto significa aprovechar los errores o descuidos humanos para convencer a las víctimas de que hagan algo que va en contra de sus propios intereses, muchas veces sin que lo noten.

En esencia, se trata de engañar a las personas para que compartan información confidencial, como contraseñas, datos bancarios o cualquier otro tipo de dato sensible. Los ciberdelincuentes utilizan esta información para cometer fraudes, acceder a sistemas restringidos o realizar actividades ilegales.

Lo que hace a la ingeniería social tan peligrosa es que no depende de fallos en la tecnología, sino de la capacidad de los atacantes para ganarse la confianza de las personas, aprovechar su desconocimiento o incluso su distracción. En otras palabras, el punto débil que explotan no es el sistema, sino el factor humano.

Amenazas Informáticas

Una amenaza informática son acciones, intenciones o eventos que buscan aprovechar vulnerabilidades en sistemas tecnológicos con el objetivo de dañarlos, invadirlos o comprometer

su funcionamiento. Estas amenazas pueden poner en riesgo la integridad, confidencialidad y disponibilidad de la información, afectando tanto a individuos como a empresas.

En el caso de las organizaciones, las amenazas informáticas provienen principalmente de ataques externos, como los realizados por ciberdelincuentes que buscan obtener acceso no autorizado, robar información sensible, interrumpir operaciones o extorsionar a las víctimas mediante técnicas como el ransomware o el phishing. Sin embargo, no todas las amenazas vienen desde afuera. También existen riesgos internos, que pueden ser igual de peligrosos. Estos incluyen el robo de información por parte de empleados, el uso indebido de los sistemas, errores humanos o incluso descuidos que dejan expuestos los datos y sistemas críticos.

Tipos de Amenazas Informáticas

Account Breach (Cuenta Comprometida). Es un acceso no autorizado a una cuenta de usuario o administrador dentro de un dominio, se da cuando un atacante obtiene y utiliza las credenciales de inicio de sesión de manera fraudulenta. Este tipo de amenaza informática compromete la seguridad de la cuenta afectada, permitiendo al atacante acceder a recursos, sistemas o datos sensibles asociados al dominio.

Cuando una cuenta es comprometida, el atacante puede realizar diversas acciones maliciosas, como robar información, modificar configuraciones, instalar malware o incluso utilizar la cuenta como punto de partida para expandir el ataque a otros sistemas dentro de la red. Este tipo de brechas representa un riesgo significativo, ya que los atacantes suelen hacerse pasar por el usuario legítimo, dificultando la detección del incidente.

Data Deletion (Eliminación de Datos). Es la eliminación deliberada de datos críticos, delicados o valiosos de un sistema, dispositivo o red. Este procedimiento puede ser realizado por ciberdelincuentes, trabajadores insatisfechos, o incluso a través de ataques automatizados por medio de malware, creado específicamente para eliminar datos. Lo que hace que esta amenaza sea importante es que en muchas ocasiones la información suprimida es difícil o imposible de recuperarse, especialmente si no se disponen de copias de seguridad.

La eliminación de datos puede estar impulsada por múltiples razones, tales como sabotaje, extorsión, venganza o simplemente el propósito de perjudicar algo.

Data Exfiltration (Filtración Externa de datos). Es el acceso, copia, transferencia o extracción no autorizada de información sensible desde un sistema, red o dominio hacia ubicaciones externas controladas por un atacante. Este tipo de amenaza pone en riesgo la privacidad de los datos y puede generar graves repercusiones para entidades e individuos, dado que los datos sustraídos frecuentemente se emplean para propósitos malintencionados, tales como espionaje, extorsión, y estafa.

La filtración de información puede realizarse de varias maneras, ya sea de forma manual por un trabajador inapropiado o a través de herramientas automatizadas, como malware creado específicamente para obtener datos sin ser identificado.

Data Leaks. Exposición o transferencia no permitida de datos delicados o confidenciales fuera de un ambiente seguro, ya sea de forma deliberada o accidental. Estas pérdidas de información se pueden dar a través de varios medios, tales como correos electrónicos, servicios de

mensajería, grupos de trabajo, aplicaciones en la nube o dispositivos móviles, y constituyen un peligro considerable para la privacidad y la seguridad de las entidades e individuos.

Elevation of Privilege (Elevación de Privilegios). Es una modalidad en la que los atacantes, después de poner en riesgo una o varias cuentas con privilegios restringidos en un dominio, buscan incrementar su nivel de acceso para conseguir privilegios superiores, como los de administrador global. Este tipo de amenaza es especialmente riesgosa, dado que posibilita que el atacante adquiera un control más extenso sobre los recursos, sistemas y datos del dominio, lo que podría tener serias repercusiones para la seguridad de la organización.

Malicious Insider (Usuario Interno Malintencionado). Se trata de un usuario o administrador con acceso legítimo a los sistemas, datos o recursos de una entidad que emplea este acceso de forma deliberada para poner en riesgo la seguridad, difundir información delicada o provocar perjuicios a la compañía. Este tipo de riesgo puede surgir de empleados presentes, ex empleados, contratistas, asociados de negocios o cualquier empleado con privilegios de acceso en la organización.

Malware (Software Malicioso). Es un software diseñado específicamente para llevar a cabo acciones malintencionadas o no permitidas en sistemas de computación, redes o dispositivos. Su objetivo va desde provocar perjuicios, sustraer datos íntimos, espiar acciones del usuario, hasta asumir el control absoluto de un sistema. Dentro de los tipos más habituales de malware se encuentran virus, troyanos, ransomware, spyware, gusanos y otras aplicaciones malintencionadas.

Password Cracking. Es el procedimiento en el que un atacante emplea herramientas especializadas y equipos de cómputo de gran capacidad para adquirir contraseñas sin autorización. Este proceso implica examinar una amplia variedad de combinaciones posibles en un breve lapso de tiempo hasta hallar la contraseña correcta, lo que le posibilita ingresar a datos sensibles, sistemas o recursos protegidos.

Phishing/Whaling (Suplantación de Identidad/Whaling). Es el envío masivo de emails, mensajes de texto o comunicaciones digitales que parecen originarse de empresas, entidades financieras, servicios en línea u organizaciones legítimas. La finalidad de estos mensajes es engañar a los usuarios para que divulguen datos privados, tales como contraseñas, números de cuenta bancaria, información de tarjetas de crédito o cualquier otra información delicada. En ciertas situaciones, los atacantes también intentan conseguir el acceso completo a las cuentas de los usuarios o infectar sus dispositivos con software malicioso.

Ransomware. Es una de las amenazas cibernéticas más temida y devastadora para las compañías en el presente. Este tipo de malware funciona cifrando información vital de una entidad, impidiendo el acceso a sus datos y sistemas fundamentales. Los atacantes demandan una compensación económica, para otorgar la clave de descifrado que les permita la recuperación de los archivos y la restauración de las operaciones.

Normatividad Sobre Delitos Informáticos

En la actualidad, muchas personas llevan a cabo acciones fraudulentas utilizando internet. Estas actividades, cuyo número aumenta a la par de los avances tecnológicos, suelen ser perpetradas por individuos con conocimientos informáticos. Algunos de los delitos más comunes incluyen el secuestro de información, extorsiones, estafas, ciberacoso, robo de identidad y fraudes relacionados con cuentas bancarias o tarjetas de crédito, entre otros.

Estos actos ilegales, cometidos a través de herramientas informáticas e internet, suelen ser difíciles o incluso imposibles de rastrear, ya que se ejecutan de manera rápida y sin dejar rastro evidente. A pesar de ello, existen leyes diseñadas para proteger a las víctimas de estos delitos. A continuación, profundizaremos en algunas de estas normativas.

Ley 527 de 1999

Establece que “la firma electrónica es un conjunto de datos en forma electrónica que se adjunta o se asocia a un documento electrónico y que permite identificar al firmante y manifestar su consentimiento” (MINTIC, 1999). Esta ley busca facilitar el uso de medios electrónicos en las transacciones comerciales, garantizando la autenticidad y la integridad de los documentos electrónicos.

Mediante esta se determina que la firma digital posee la misma validez legal que una firma tradicional hecha en papel, mientras cumpla con ciertos requisitos que garantizan la identidad del individuo que firma y la integridad del documento.

Su objetivo principal es facilitar las transacciones electrónicas, permitiendo que las personas y las empresas realicen trámites de manera más rápida y segura a través de Internet. Además, la ley define las responsabilidades de las entidades que ofrecen servicios de certificación para garantizar que las firmas electrónicas sean confiables.

Ley 1266 de 2008

Define reglas en relación a la administración de la información financiera de los ciudadanos. Según esta ley, “la información contenida en las bases de datos debe ser veraz, completa, actualizada y comprensible” (Congreso de la República de Colombia, 2008). Esto implica que las entidades que manejan datos personales deben asegurarse que la información que poseen sea precisa y esté actualizada, protegiendo así los derechos de los consumidores.

La ley garantiza que las personas tengan el derecho a conocer, actualizar y corregir su información. Exige que los datos sean verídicos y actualizados, y requiere el consentimiento previo para su recolección y uso. Además, establece medidas para proteger la confidencialidad y seguridad de esta información, con el fin de evitar accesos no autorizados.

Ley 1273 de 2009

A través de esta ley, se creó una nueva categoría legal llamada "protección de la información y los datos" (Congreso de la República de Colombia, 2009). Su objetivo es sancionar a las personas que cometan delitos relacionados con la información, las tecnologías y las comunicaciones en Colombia.

La ley establece un marco legal para la protección de datos personales y la prevención de delitos informáticos, garantizando que la información personal sea manejada de manera segura y responsable. Tipifica conductas delictivas como el ingreso no permitido a sistemas informaticos y la interceptación de información. Además, otorga a los ciudadanos derechos sobre su información, como el acceso, la actualización y la rectificación de sus datos, y responsabiliza a las entidades que manejan esta información por su protección y el cumplimiento de la ley.

Esta ley contempla los siguientes artículos y delitos:

Artículo 269A. Acceso Abusivo a un Sistema Informático

Cualquier individuo que acceda y permanezca en un sistema informático, ya sea con o sin medidas de seguridad, y sin la autorización del administrador, podrá enfrentar una pena de prisión de 4 a 8 años, además de una multa que varía entre 100 y 1000 SMMLV.

Artículo 269B. Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación

Si una persona, sin autorización, bloquea o interfiere en el funcionamiento de un sistema informático, los datos que contiene o una red de telecomunicaciones, puede ser condenada a prisión de 4 a 8 años y a una multa de hasta 1.000 SMMLV, siempre que no sea un delito más grave con una pena mayor.

Artículo 269C. Interceptación de Datos Informáticos

Acceder o controlar datos en un sistema informático y transmitirlos sin autorización judicial puede llevar a una pena de prisión de 3 a 6 años.

Artículo 269D. Daño Informático

Cualquiera que, sin permiso, destruya, dañe, modifique o elimine datos o sistemas informáticos enfrentará una pena de prisión de 4 a 8 años y una multa que oscila entre 100 y 1.000 SMMLV.

Artículo 269E. Uso de Software Malicioso

La creación, venta, distribución o uso de programas dañinos (como virus) sin autorización puede resultar en una condena de 4 a 8 años de cárcel y una multa de 100 a 1.000 SMMLV.

Artículo 269F. Violación de Datos Personales

El uso, venta, compartición o robo de datos personales sin autorización puede conllevar una pena de prisión de 4 a 8 años y una multa de 100 a 1.000 SMMLV.

Artículo 269. Suplantación de Sitios Web para Capturar Datos Personales.

Si alguien crea, vende o utiliza páginas web falsas, enlaces o ventanas emergentes sin autorización, puede ser condenado a prisión de 4 a 8 años y a una multa de 100 a 1.000 SMMLV. Esto también se aplica a quienes alteren la dirección IP de un sitio web para engañar a usuarios haciéndoles creer que están accediendo a su banco u otro sitio confiable.

Artículo 269H. Circunstancias de Agravación Punitiva.

Este artículo aborda las circunstancias que pueden agravar las penas impuestas por los delitos mencionados anteriormente:

- En sistemas informáticos o redes del sector público, oficial o financiero.
- Cuando el responsable es un funcionario público que no cumple sus deberes.
- Si se aprovecha la confianza de alguien con quien se tiene una relación contractual.
- Cuando se filtran o distribuyen contenidos que dañan a terceros.
- Si el delito busca un beneficio propio o para otra persona.
- Si se usa con fines terroristas o amenaza la seguridad nacional.
- Si se engaña a personas inocentes para que participen sin saberlo.
- Si el responsable administra o controla la información, además puede perder su derecho a ejercer profesiones relacionadas con sistemas informáticos por hasta 3 años.

Ley 1341 de 2009

Según el Congreso de la República de Colombia (2009), se definen principios y conceptos fundamentales relacionados con la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC).

Esta ley asegura que las personas puedan utilizar tecnologías de manera libre, siguiendo reglas internacionales que promueven una competencia justa. Además, protege el derecho a comunicarse y garantiza que los servicios básicos de tecnología, como Internet, estén disponibles para todos. También se enfoca en mejorar la infraestructura tecnológica y facilitar el acceso a estas herramientas, con el fin de que un mayor número de personas pueda beneficiarse de ellas.

Ley 1581 de 2012

Conocida como la Ley de Protección de Datos Personales, la Ley 1581 de 2012 establece que “el tratamiento de datos personales debe sujetarse a los siguientes principios: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad” (Congreso de la República de Colombia, 2012). Esta legislación busca garantizar que los individuos tengan el derecho de conocer, actualizar y corregir la información que han proporcionado a entidades públicas o privadas. Así, se asegura que los datos sean gestionados de manera adecuada, respetando siempre los derechos de quienes los suministran y promoviendo un manejo responsable y ético de la información personal.

Tabla 1

Relacion de la normatividad con las funciones de los equipos Red Team y Blue Team

Normativa	Descripción	Relación con Red Team	Relación con Blue Team
Ley 527 de 1999	Regula el uso de mensajes digitales y el comercio electrónico.	Simulación de ataques para evaluar la autenticidad e integridad.	Establecimiento de estrategias y controles de seguridad para salvaguardar los datos.
Ley 1266 de 2008	Manejo de información personal en bases de datos.	Evaluación de vulnerabilidades relacionadas con la gestión de datos personales.	Protección de la información y permisos de acceso, actualización y corrección.
Ley 1273 de 2009	Protección de la información y los datos, tipifica delitos informáticos.	Simulación de ataques para identificar accesos abusivos y dañinos.	Respuesta ante incidentes y mitigación de daños informáticos.
Ley 1341 de 2009	Uso de tecnologías y comunicación, y promoción de la competencia justa.	Evaluación del cumplimiento de normativas en sistemas.	Garantizar acceso y disponibilidad de servicios tecnológicos.
Ley 1581 de 2012	Protección de datos personales, asegurando su manejo adecuado.	Análisis de riesgos en la gestión de datos personales.	Implementación de políticas de privacidad y protección de datos.

Nota. Elaboración propia.

Actuación Ética y Legal

La actuación ética y legal de los especialistas en ciberseguridad es fundamental para garantizar la integridad y seguridad de los datos en un entorno cada vez más digitalizado. De acuerdo con el código ético del COPNIA, todos los ingenieros, sin importar su campo de trabajo, deben comportarse con integridad, responsabilidad y en pro del bienestar social.

Importancia de la Ética Profesional

Los especialistas en ciberseguridad tienen la responsabilidad de proteger la seguridad y el bienestar del público. Esto implica no solo cumplir con las leyes, sino también adherirse a principios éticos que guíen su práctica profesional.

Antes de aceptar ofertas laborales atractivas en términos de salario y beneficios, es crucial evaluar si la empresa fomenta prácticas legales y confiables. Trabajar en un entorno que no respete estos principios puede comprometer la integridad profesional y personal.

Complicidad en Actividades Ilegales

Colaborar con empresas que no cumplen con las normativas legales puede implicar ser cómplice de actividades ilegales, lo cual es inaceptable desde un punto de vista ético. Esto no solo afecta la reputación del profesional, sino que también puede conllevar consecuencias legales severas, incluyendo multas y penas de prisión bajo leyes como la Ley 1273.

Acceso a Información Sensible

Durante auditorías y evaluaciones de seguridad, es común que las empresas de ciberseguridad necesiten acceder a información sensible. Este acceso debe ser controlado y limitado a lo estrictamente necesario.

Es vital establecer contratos y acuerdos de confidencialidad que especifiquen claramente qué información puede ser consultada, quién tiene acceso a ella y el propósito de su uso. Estos acuerdos deben incluir medidas de protección para el cliente, como la obligación de informar sobre accesos no autorizados.

Estrategias para Promover la Ética y Legalidad

Políticas y Procedimientos. Las empresas deben establecer políticas claras sobre el uso de herramientas forenses, especificando sus fines y limitaciones.

Control de Acceso. Implementar sistemas de control de acceso y autenticación multifactorial para garantizar que solo personal autorizado pueda utilizar herramientas sensibles.

Monitoreo de Actividades. Utilizar software de monitoreo para registrar todas las acciones realizadas con herramientas forenses, facilitando auditorías y la identificación de conductas sospechosas.

Capacitación Continua. Ofrecer capacitación constante sobre ética profesional y regulaciones legales para generar conciencia sobre el uso responsable de herramientas y procedimientos.

Canales de Denuncia. Establecer mecanismos anónimos para denunciar conductas inapropiadas sin temor a represalias.

Manejo de Incidentes de Ciberseguridad

- En caso de incidentes como el ciberespionaje, es crucial investigar a fondo, identificar a los responsables y tomar acciones legales si es necesario.

- Suspender o cancelar contratos con empresas involucradas hasta resolver el problema es esencial para evitar futuras complicaciones.
- Mantener informados a todos los interesados sobre las medidas adoptadas y realizar una evaluación de riesgos para fortalecer la seguridad interna y las políticas de contratación.

Metodologías y Herramientas Utilizadas por los Equipos Especializados Blue Team y Red Team

Blue Team y Red Team son grupos compuestos por expertos en ciberseguridad, cuyo enfoque es analizar y garantizar el correcto funcionamiento de los sistemas informáticos de las empresas, asegurando la integridad, confidencialidad y disponibilidad de la información.

Responsabilidades y Metodología de Blue Team

El Blue Team está integrado por personal de seguridad que tiene una perspectiva interna de la empresa. Su función es proteger todo el entorno de tecnología de la información frente a diversas ciberamenazas. Los miembros del Blue Team están familiarizados con los planes comerciales y las estrategias de seguridad de la organización, por lo que su labor consiste en reforzar la seguridad para evitar que los atacantes comprometan los recursos de TI.

El primer paso para el equipo azul es recopilar datos para documentar exactamente lo que con mayor prioridad debería protegerse, para esto hacen una evaluación de riesgos. El primer paso es identificar los activos clave, documentar cuál es su nivel de importancia, y que valor representan para el negocio, además del impacto que podría tener para la empresa no contar con estos activos.

Estos especialistas suelen utilizar varias herramientas de monitoreo que les permiten identificar y registrar información relacionada con el acceso al sistema, y sobre actividades inusuales que en estos se presenten. Estos equipos también hacen verificaciones periódicas del sistema y del DNS, validan las vulnerabilidades de la red interna y externa, y recopilarán muestras de tráfico de la red para su posterior análisis.

Otra de sus funciones es implementar medidas de seguridad alrededor de los recursos tecnologicos más importantes de la empresa, al evaluar y priorizar los riesgos, el Red Team puede desarrollar un plan para ejecutar soluciones que pueden reducir el daño o la vulnerabilidad de los activos TI.

En este proceso es fundamental contar participación de los gerentes, ya que desde el gobierno corporativo se puede decidir si se acepta un riesgo, o facilitan los recursos necesarios para implementar los controles requeridos para mitigarlos. Por lo general realizan un análisis costo-beneficio, para garantizar que los controles de seguridad brinden beneficios al negocio con una mínima inversión.

Blue Team apoya activamente acciones preventivas que permitan el adecuado cumplimiento de las políticas de ciberseguridad, lo que significa fortalecer a la empresa para enfrentar amenazas informáticas.

Principales Estrategias de Estos Equipos

Correcta Gobernanza de la Práctica de Seguridad. Blue Team lleva a cabo operaciones de seguridad de datos bajo la dirección del Director de Seguridad de la Información y en cumplimiento de las normas empresariales.

Detectar y Responder Ante Amenazas. Blue Team realiza tareas de detección con herramientas de monitoreo, analizando sistemas de amenazas avanzados e interrumpiendo proactivamente los ataques antes de que los ciberdelincuentes alcancen sus objetivos.

Detectar y Corregir Vulnerabilidades. Es responsable de abordar las debilidades y vulnerabilidades, una acción importante para resolver problemas antes de que sean explotados, y de mejorar continuamente la postura de seguridad para proteger a la organización de nuevas amenazas.

Diseñar, Implantar y Operar Cualquier Medida Orientada la Prevención de Riesgos. Blue Team utiliza toda la información que tiene, y las lecciones aprendidas para que situaciones de peligro no vuelvan a ocurrir. Esto tiene como objetivo que la organización se anticipe a este tipo de situaciones, reforzando las medidas preventivas necesarias para evitar que se produzcan incidentes.

Formación y Concienciación en Materia de Seguridad. Es bien sabido que los trabajadores de una entidad suelen ser el elemento más vulnerable de la cadena de seguridad. Formarlos y compartir con ellos conocimientos de seguridad es fundamental para evitar el éxito de un gran número de ataques.

La capacitación y la concientización es una función de seguridad clave, porque no solo permite a los empleados resistir los ataques, sino también trabajar de manera segura en su vida diaria, lo que representa un componente crucial de la habilidad de la empresa para identificar amenazas.

Herramientas Utilizadas por Blue Team

Las herramientas que usualmente emplean los equipos Blue Team, se categorizan de acuerdo al contexto del sistema donde se utilizan. Los sistemas informáticos se componen de

varios elementos que suponen distintos riesgos, por lo que las estrategias de seguridad varían para cada uno de estos escenarios.

Protección de Redes

Firewalls. Son dispositivos físicos o de software instalados en diferentes niveles del sistema para administrar el tráfico hacia y desde el dispositivo. Sin embargo, los cortafuegos pueden detectar anomalías y evitar que entren amenazas o que escape información confidencial del sistema.

IDS/IPS. Son dispositivos físicos o de software que se pueden instalar en la red o directamente en los dispositivos conectados a ella. Las técnicas de detección/prevención de intrusiones le permiten monitorear, detectar y prevenir amenazas cibernéticas de la red.

Los IDS permiten detectar accesos no autorizados a un sistema o red, para en base a estos generar alertas o log, que puedan ser analizados posteriormente por administradores del sistema o especialistas. A diferencia del IPS este no actúa ante los ataques, solo alerta de ellos.

Extensive Detection and Response (XDR). Estas herramientas funcionan no solo en la red, sino en todo el sistema. Además, te permiten centralizar y organizar la información obtenida por diferentes productos de ciberseguridad. Recopila y agrega datos a través de múltiples niveles de seguridad, incluidos endpoints, correo electrónico, servidores, múltiples servicios en la nube, y la red en general.

Protección de Dispositivos

Endpoint Detection and Response (EDR). Este es un tipo de software que se instala directamente en los dispositivos conectados a Internet. Los EDR analizan los sistemas informáticos en busca de amenazas que los programas antivirus hayan pasado por alto. Para hacer esto, los EDR se basan en firmas y patrones de aprendizaje automático. Por tanto, permiten la detección de amenazas conocidas y de día cero.

Antivirus. Son software diseñados para escanear datos como páginas web, archivos, programas y aplicaciones, con el objetivo de encontrar y eliminar malware lo más rápido posible. La gran mayoría ofrece protección en tiempo real para ayudar a proteger sus dispositivos de amenazas futuras. Trabajan escaneando regularmente los equipos de cómputo en busca de amenazas conocidas, y brindando actualizaciones automáticas, que permiten detectar, bloquear y eliminar códigos y software maliciosos.

Protección de Aplicaciones

SAST (Static Application Security Testing). Utilizada para la seguridad de aplicaciones estáticas, esta verifica el código fuente de la herramienta para encontrar vulnerabilidades conocidas.

DAST (Dynamic Application Security Testing). Permite verificar y analizar aplicaciones activas en busca de un comportamiento inusual que indique posibles vulnerabilidades.

RASP (Runtime Application Self-protection). Son herramientas de autoprotección que se integran en las aplicaciones durante su ejecución, para que pueda monitorearse a sí misma y evitar ataques en tiempo real.

SCA (Software composition analysis). Estas herramientas ayudan a evaluar y monitorear todos los componentes de una aplicación para detectar vulnerabilidades que hayan podido ser introducidas a lo largo de la cadena de desarrollo y producción del software.

Protección de Datos. Muchas de las herramientas comunes del Blue Team están relacionadas con la criptografía. Esta rama de las matemáticas ha permitido el desarrollo de algoritmos, cuya función es la de encriptar y desencriptar información de manera segura.

Algunas aplicaciones que se pueden usar para encriptar datos son:

VeraCrypt. Es un software de código abierto multiplataforma utilizado para cifrar archivos, carpetas, unidades USB extraíbles, discos duros completos, e incluso aquellos donde se encuentra instalado el sistema operativo.

GNU Privacy Guard. Permite crear e intercambiar claves públicas que están codificadas en ASCII, y por lo tanto, pueden enviarse de manera segura por cualquier medio que no se considere confiable.

Algunos Ejemplos de Herramiemtas de Contención Open Source

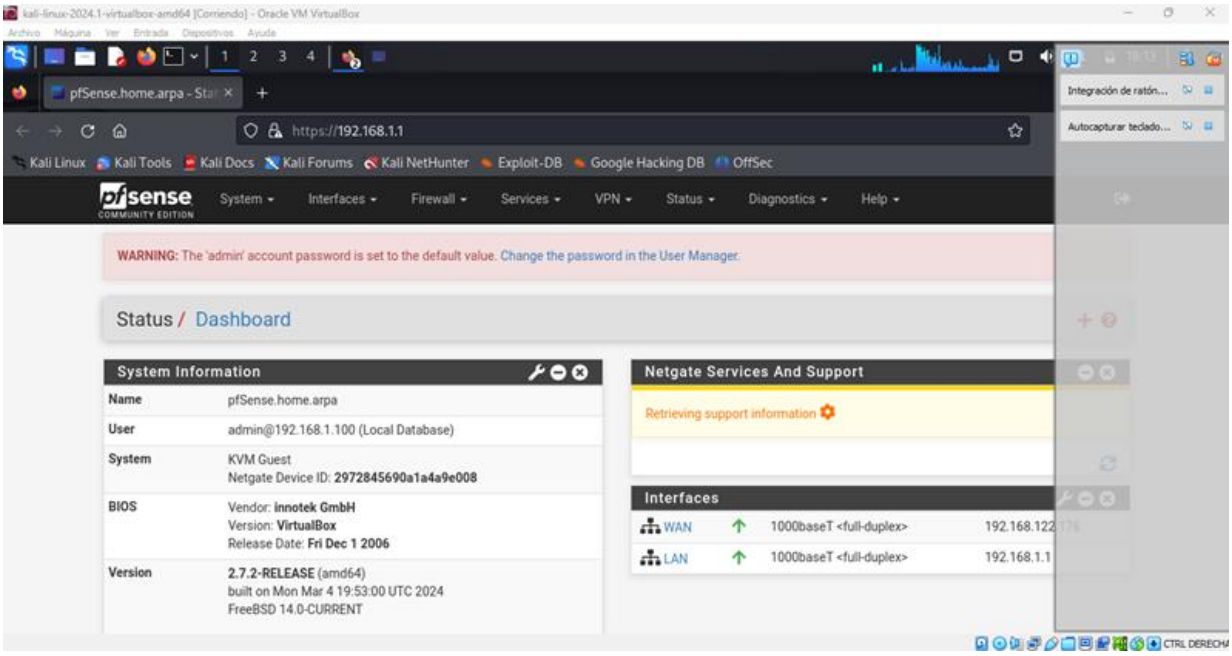
PfSense. Es un sistema operativo de firewall y router basado en FreeBSD. Ofrece una interfaz web fácil de usar y es altamente configurable. Proporciona soporte para VPN, filtrado de paquetes y monitoreo de tráfico.

Caracteristicas:

- Es de código abierto, motivo por el cual no hay costos de licencia.
- Permite configuraciones personalizadas para diferentes necesidades de red.
- Posee una interfaz web intuitiva que facilita la administración.
- Soporta VPN, balanceo de carga y filtrado de contenido.
- Cuenta con una comunicad activa, que ofrece amplio soporte y documentación.
- Cuenta con actualizaciones de seguridad y funcionalidad frecuentes.

Figura 5

Ventana principal Dashboard PfSense



Nota. Elaboración propia.

Snort. es un sistema de detección y prevención de intrusiones (IDS/IPS) que permite la inspección de tráfico en tiempo ofreciendo detección de ataques en tiempo real, soporte para reglas personalizadas, y registro de eventos y alertas.

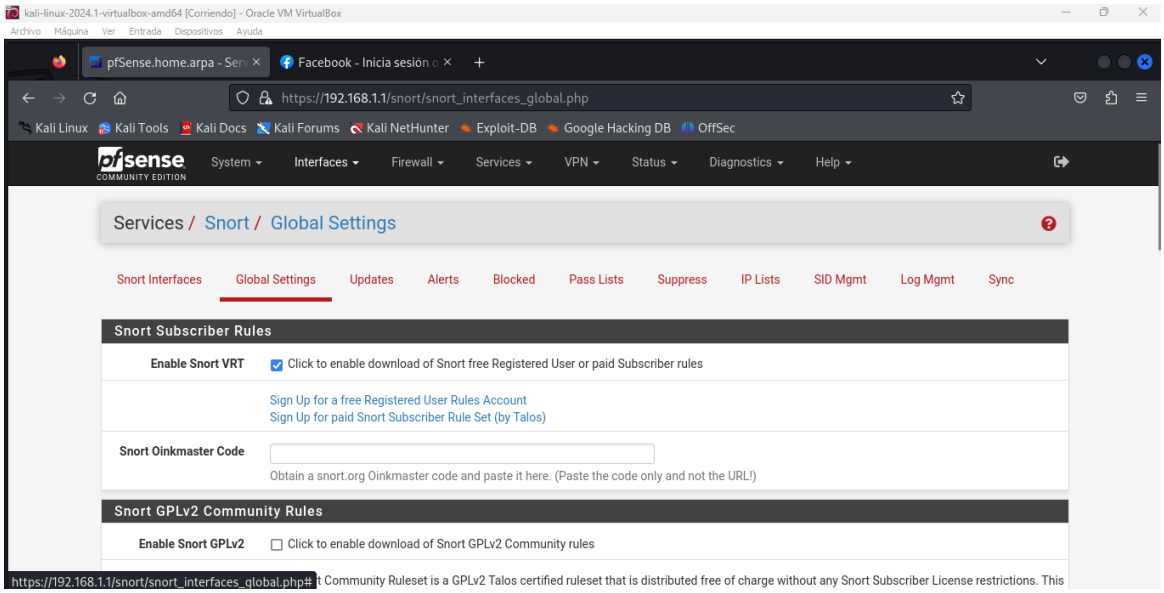
Caracteristicas:

- Es de código abierto, sin costos de licencia, lo que lo hace accesible para muchas organizaciones.
- Tiene capacidad para identificar y prevenir ataques en tiempo real.
- Permite crear y modificar reglas según las necesidades específicas.
- Se puede integrar fácilmente con otras herramientas de seguridad.

- Se adapta a diferentes entornos y requisitos de seguridad.
- Amplio soporte comunitario y recursos disponibles.

Figura 6

Vista pestana Global Settings Snort



Nota. Elaboración propia.

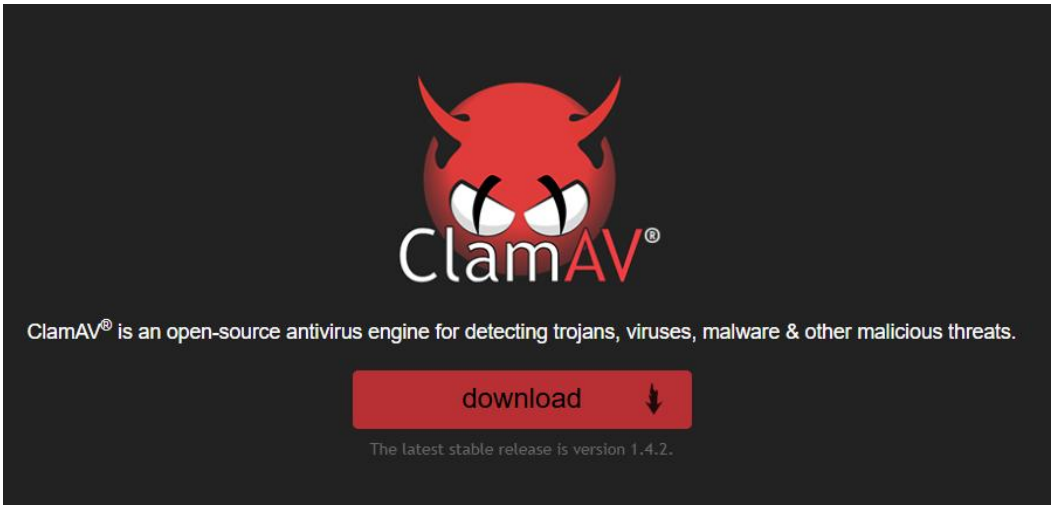
ClamAV. Es un antivirus de código abierto diseñado para detectar malware y virus en archivos y correos electrónicos. Ofrece Escaneo de archivos en tiempo real, actualizaciones frecuentes de la base de datos de virus, y soporte para múltiples plataformas.

Caracteristicas:

- Es de código abierto lo que la hace ideal para organizaciones con presupuestos limitados.
- Permite ajustar configuraciones y definir políticas de escaneo.
- Funciona en múltiples plataformas, incluyendo Linux y Windows.
- Cuenta con una base de datos de virus actualizada regularmente.
- Permite programar escaneos automáticos.

Figura 7

ClamAV antivirus



Nota. Tomado de https://www.clamav.net/

Responsabilidades y Metodología de Red Team

El objetivo principal del equipo Red Team es asegurar el potencial de reacción del equipo Blue Team, para comprobar si las estrategias y herramientas de seguridad utilizadas por este son efectivas, y así poder detectar intrusiones y aplicar las correcciones pertinentes en el menor tiempo

posible. A este equipo solo se le facilita el nombre de la empresa, con el objetivo de que se realicen pruebas con escenarios similares al de un ataque real.

Su trabajo consiste en adoptar la perspectiva de un intruso para evaluar la eficacia de los controles de seguridad implementados por una organización. Estos grupos emplean metodologías específicas y diversas herramientas para llevar a cabo sus tareas.

Ciclo del Red Team

Definición y Planificación. En esta fase se determina qué tipos de vectores u objetos específicos se emplearán y de qué manera serán atacados. Una vez que se han infiltrado oportunamente, se procede a la fase de planificación de las acciones que respaldarán este ataque.

Reconocimiento Externo. Se trata de crear todas las acciones posibles para encontrar los recursos que se liberan en el área examinada, luego continuar examinando cada parte y, por lo tanto, averiguar si la intervención es inadecuada.

Compromiso Inicial. Si la amenaza se considera lo suficientemente significativa como para abrir una vía de acceso, se pueden llevar a cabo desde intentos de intrusión por fuerza bruta contra los usuarios, hasta la transferencia de archivos que faciliten el acceso a la red interna.

Acceso a la Red Interna. Si el equipo original está comprometido, se deben encontrar los medios para acceder a la red interna. Este proceso puede variar dependiendo de la seguridad de la empresa, y puede tardar varios minutos o días.

Elevación de Privilegios. En esta fase se pretende establecer rutas de acceso alternativas en caso de que el equipo de seguridad del Blue Team identifique y neutralice el ataque principal. Al contar con otras opciones, se podrá proseguir con la operación, incluso si el equipo de seguridad está ocupado investigando el primer ataque.

Reconocimiento Interno. Una vez que obtiene acceso total a la organización, lleva a cabo un análisis interno de todos los recursos para identificar cuáles ataques podrían ser los más severos y cuáles activos podrían verse más comprometidos.

Análisis y Reporte. Con el registro de todas las vulnerabilidades encontradas, métodos utilizados y datos accesibles, se crea un informe detallado de los resultados, riesgos y recomendaciones para mejorar la seguridad.

Podemos concebir los vectores como las rutas disponibles para la intrusión. En el contexto del Red Team, existen vectores de Acceso y de Ataque, los cuales pueden variar, aunque generalmente hay ciertos tipos que se mantienen constantes en todas las organizaciones que implementan red teaming.

Vectores de Acceso Red Team

Son formas de intrusión que pueden ser utilizadas para comprometer sistemas o redes. Existen muchos vectores de ataque y acceso diferentes que los equipos de Red Team pueden emplear, pero, en general, hay ciertos tipos que se repiten en la mayoría de las organizaciones que trabajan con este enfoque.

Ingeniería Social. Es la manipulación psicológica empleada para adquirir datos privados, tales como contraseñas, accesos o informacion sensible, aprovechando la confianza o el desconocimiento de las personas

Ataques a Redes Wi-Fi. Se comprometen redes inalámbricas mediante técnicas como Evil Twin (redes falsas) o crackeo de contraseñas WPA/WPA2.

Explotación de Vulnerabilidades. Se utilizan fallas conocidas en aplicaciones, sistemas operativos o servicios para obtener acceso inicial.

Ataques a APIs. Se explotan configuraciones inseguras o vulnerabilidades en APIs para acceder a datos o servicios protegidos.

Ataques de Intermediario (MITM). Es la interceptación de comunicaciones entre dos partes, con el objetivo de capturar información sensible como credenciales o datos.

Uso de USB Malicioso. Se utilizan dispositivos USB infectados con malware, que al ser conectados a un sistema, pueden instalar programas maliciosos o robar información.

Ataques a Sistemas en la Nube. Se explotan configuraciones incorrectas en plataformas como AWS, Azure o Google Cloud para obtener acceso a recursos o datos.

Clonación de Tarjetas RFID/NFC. Uso de dispositivos para copiar credenciales de acceso físico a través de tarjetas o dispositivos de autenticación.

Reconocimiento Pasivo (OSINT). Recolección de información pública sobre la organización objetivo, como correos electrónicos, dominios, infraestructura, etc., para planificar el acceso inicial.

Vectores de ataque Red Team

Una vez que el acceso inicial se logra, los vectores de ataque son utilizados para comprometer sistemas, escalar privilegios, moverse lateralmente y extraer datos.

SQL Injection. Se trata de introducir código malintencionado en aplicaciones web con el objetivo de modificar bases de datos y sustraer datos.

Cross-Site Scripting (XSS). Se da con la inyección de scripts dañinos en páginas web, para robar datos de usuarios o realizar acciones sin su autorización.

Cross-Site Request Forgery (CSRF). Un usuario es obligado, sin que lo sepa, a realizar acciones no deseadas en una aplicación web.

Ataques de Fuerza Bruta. Son intentos automáticos de adivinar contraseñas en servicios como correos, aplicaciones o accesos remotos.

Escalamiento de Privilegios. Se encuentran fallas en un sistema para obtener permisos de administrador y mayor control sobre el.

Movimientos Laterales (Lateral Movement). Otros sistemas dentro de la red son explorados, una vez que se tiene acceso inicial.

Pass-the-Hash. Es el uso de contraseñas cifradas (hashes), para acceder a sistemas sin necesidad de conocer las contraseñas reales.

Ataques a Directorio Activo. Se intenta controlar redes que usan Active Directory, para robar credenciales o permisos de administrador.

Malware Personalizado. Consiste en la creación de virus o programas diseñados para evitar ser detectados por antivirus y mantener acceso al sistema.

Ataques a Dispositivos IoT. Se comprometen dispositivos conectados (como cámaras o sensores) aprovechando configuraciones débiles o falta de actualizaciones.

Ataques de Intermediario (MITM). Se interceptan comunicaciones en una red para robar información o modificar datos.

Ataques a Sistemas SCADA/ICS. Es el compromiso de sistemas industriales y de infraestructura crítica, como fábricas o plantas de energía.

Exfiltración de Datos. Método utilizado para robar información sensible de una organización sin ser detectado.

Ataques a Sistemas de Virtualización. Aprovechamiento de fallas en entornos virtuales (como VMware o Hyper-V) para comprometer sistemas.

Ataques con Ransomware Simulado. Uso controlado de ransomware para probar cómo responde una organización ante este tipo de ataques.

Ataques a Redes DNS. Manipulación del tráfico de internet (DNS) para redirigir usuarios o robar información.

Uso de Scripts Maliciosos. Ejecución de comandos dañinos con herramientas como PowerShell, Bash o Python para controlar sistemas o robar datos.

Herramientas Utilizadas por Red Team

Herramientas de Reconocimiento

- *RustScan.* Se caracteriza por contar con un escaneo de puertos rápido y preciso, permitiendo identificar posibles puntos de entrada a la red.
- *Amass.* Se trata de un potente rastreador de red capaz de identificar subdominios vinculados a una organización.
- *CloudEnum*. Es una herramienta que ayuda a listar los recursos en la nube, lo que facilita saber cómo una organización utiliza los servicios en línea.

- *Recon-NG.* Es un conjunto de herramientas para reunir información en internet, que permite a los usuarios crear y personalizar sus propios módulos para hacer investigaciones.
- *AttackSurfaceMapper.* Esta herramienta recopila datos sobre un objetivo y muestra visualmente las áreas donde podría ser atacado.
- *DNSDumpster.* Es un buscador que encuentra registros DNS y también ayuda a trazar mapas de dominios.
- *SprayingToolKit***.** Este conjunto de herramientas se utiliza para realizar ataques de "spraying de contraseñas", que intentan acceder a cuentas usando contraseñas comunes.
- *o365Recon.* Esta herramienta es útil para obtener información sobre los usuarios de Office 365 en una organización.
- *GadgetToJScript.* Convierte componentes de .NET en scripts de JScript, permitiendo que se ejecuten en entornos controlados.
- *ThreatCheck.* Ayuda a determinar si una organización es susceptible a un tipo específico de ataque.
- *Freeze.* Esta herramienta sirve para bloquear cuentas de usuario, evitando que se bloqueen durante un ataque de fuerza bruta.

Herramientas de Entrega. Después de obtener el acceso inicial, el siguiente paso es implementar una carga útil o un exploit, para lo cual son útiles las siguientes herramientas:

- *o365AttackToolKit.* Es un kit de herramientas se utiliza para lanzar diversos ataques contra Office 365.
- *EvilGinx2.* Poderoso framework de phishing y bypass de autenticación de dos factores.
- *GoPhish.* Una plataforma de phishing de código abierto que permite a los usuarios crear y realizar campañas de phishing simuladas.
- *PwnAuth.* Utilizado para ataques de robo de tokens de autenticación web.
- *Modlishka.* Servidor proxy de phishing inverso que puede ayudar a realizar ataques automatizados de phishing y suplantación de identidad.

Herramientas de Comando y Control. Permiten a los atacantes controlar los sistemas o redes que han infiltrado.

- *PoshC2.* Marco de servidor de comando y control versátil y poderoso.
- *Sliver.* Marco de generación de payloads con un conjunto de características para la evasión.
- *Silenttrinity.* Marco de post-explotación que utiliza la ejecución de IronPython para la ejecución lateral en la red.
- *Empire.* Marco post-explotación que permite el control total de la máquina objetivo.

- *AzureC2Relay*. Proyecto que extiende las capacidades de PoshC2 para usarlo con Azure Functions.

Herramientas de Volcado de Credenciales. Pueden ser utilizadas para obtener credenciales de los sistemas infiltrados.

- *MimiKatz.* Famosa para extraer contraseñas en texto plano, hashes, PIN y tickets kerberos de la memoria.
- *HekaTomb.* Poderoso volcador de credenciales que utiliza una variedad de técnicas.
- *SharpLAPS.* Permite extraer contraseñas almacenadas en las propiedades de LAPS (Local Administrator Password Solution).
- *Net-GPPPassword.* Herramienta extrae contraseñas almacenadas en Group Policy Preferences.
- *PyPyKatz.* Extractor de contraseñas y otros secretos de la memoria de Windows**.**

Herramientas para Escalada de Privilegios. Cuando obtener un simple acceso no es suficiente, se necesita adquirir mayores privilegios para cumplir objetivos más avanzados. Estas herramientas ayudan con esa tarea:

- *SharpUp.* Herramienta de código abierto puede ser utilizada para buscar potenciales vectores de escalada de privilegios en sistemas Windows.

- *MultiPotato.* Se centra en explotar la confianza en el servicio NBNS (NetBIOS Name Service) para elevar los privilegios.
- *PEASS (Privilege Escalation Awesome Scripts Suite).* Es una recopilación de scripts y binarios que pueden ser útiles durante el proceso de escalada de privilegios.
- *Watson.* Herramienta que se utiliza para enumerar vulnerabilidades de software de Windows que podrían ser explotadas para escalar privilegios.

Herramientas para Evasión de Defensas. Una vez dentro, mantenerse bajo el radar es esencial, para evadir las defensas existentes.

- *EDRSandBlast.* Detector y desactivador de soluciones EDR (Endpoint Detection and Response) y SandBlast Agent.
- *SPAWN*. Generador de shellcode para el evasion de EDR.
- *NetLoader*. Cargador de red para la evasión de soluciones de seguridad.
- *KillDefenderBOF*. Herramienta que puede ser utilizada para deshabilitar Windows Defender.
- *SharPyShell*. Shell obfuscado y altamente personalizable que es útil para mantener la persistencia.
- *SharpStay*. Permite la persistencia a través de la creación de tareas programadas.
- *SharpEventPersist.* Script que se utiliza para la persistencia a través de la suscripción a eventos de Windows.

Herramientas para Movimiento Lateral. Técnicas que los ciberdelincuentes utilizan para moverse a través de una red en busca de activos clave y de datos para explotar.

- *SCShell.* Herramienta de código abierto que utiliza la funcionalidad incorporada de los sistemas Windows para moverse lateralmente en la red.
- *MoveKit.* Diseñado para la infiltración en redes de grandes corporaciones, facilita la replicación a través de conexiones legítimas.
- *ImPacket.* Suite de herramientas se utiliza para trabajar con protocolos de red. Con Impacket, se puede construir versiones personalizadas de ataques y explotaciones.

Herramientas para Exfiltración. Después de infiltrarse en la red y localizar los datos útiles, se deben extraer o exfiltrar.

- *SharpExfiltrate.* Herramienta que permite la exfiltración de datos a través de canales encubiertos, evitando la detección.
- *DNSExfiltrator.* Utiliza consultas y respuestas DNS para exfiltrar datos.
- *Egress-Assess.* Se utiliza para probar la seguridad de las soluciones de prevención de pérdida de datos (DLP) en un entorno de red.

Tabla 2

Relación de las herramientas con los ataques y controles que permiten gestionar

Tipo de ataque	Tipo de control/prevención	Herramienta	Descripción
Ingeniería Social	Concienciación y Formación	N/A	Capacitación para evitar la manipulación psicológica.
Ataques a Redes	Protección de Redes	Firewalls	Controlan el tráfico y bloquean amenazas en redes.
		IDS/IPS	Monitorean y previenen intrusiones en la red.
Explotación de Vulnerabilidades	Protección de Aplicaciones	SAST	Verifica el código fuente en busca de vulnerabilidades.
		DAST	Analiza aplicaciones activas en busca de comportamientos inusuales.
SQL Injection	Protección de Aplicaciones	RASP	Monitorea aplicaciones en tiempo real para evitar ataques.
Phishing	Conciencia y Formación	GoPhish	Plataforma para crear campañas de phishing simuladas.
		EvilGinx2	Framework de phishing y bypass de autenticación de dos factores.
Escalada de Privilegios	Escalación de Privilegios	SharpUp	Busca vectores de escalada de privilegios en sistemas Windows.
		PEASS	Conjunto de scripts útiles para la escalada de privilegios.
Movimiento Lateral	Protección de Redes	SCShell	Utiliza funcionalidades de Windows para moverse lateralmente en la red.
		Impacket	Herramienta para trabajar con protocolos de red y realizar ataques.
Exfiltración de Datos	Protección de Datos	SharpExfiltrate	Permite la exfiltración de datos a través de canales encubiertos.
		DNSExfiltrator	Utiliza consultas DNS para exfiltrar datos.

Nota. Elaboracion propia.

Herramientas de Gestión de Seguridad: SIEM y CIS

Security Information and Event Management (SIEM)

Es una herramienta fundamental en la ciberseguridad que permite a las organizaciones gestionar y analizar la información de seguridad de manera efectiva. Los SIEM no solo detectan amenazas, sino que también es un componente fundamental en la gestión de la respuesta a incidentes, permitiendo a las organizaciones actuar rápidamente y aprender de ellos para fortalecer su seguridad en el futuro.

Funciones principales:

- *El SIEM se encarga de recopilar información de diferentes fuentes, como servidores, bases de datos, equipos de red y aplicaciones. Esto le permite tener una visión completa de lo que está sucediendo en el entorno de seguridad.*
- *Agrupa eventos y registros en tiempo real, lo que facilita que los analistas puedan ver todo en un solo lugar y hacer un análisis más efectivo.*
- *Convierte los datos recopilados en un formato común. Esto hace que sea más sencillo analizar y encontrar conexiones entre los datos.*
- *Examina los eventos en busca de patrones o comportamientos inusuales que podrían señalar una amenaza. Esto ayuda a detectar problemas antes de que se conviertan en incidentes graves.*
- *Permite reconocer incidentes de seguridad que quizás no sean evidentes si solo se observa un evento aislado. Así, se puede tener una mejor perspectiva de la situación.*
- *Proporciona análisis en tiempo real, permitiendo detectar y reaccionar rápidamente ante cualquier incidente de seguridad que surja.*

- *Facilita la identificación de amenazas emergentes, permitiendo a los equipos de seguridad estar siempre un paso adelante.*
- *Genera alertas automáticamente basadas en reglas preestablecidas o en comportamientos detectados, asegurando que nada pase desapercibido.*
- *Notifica a los equipos de seguridad sobre posibles incidentes, para que puedan actuar de inmediato.*
- *Genera informes detallados sobre las actividades de seguridad, lo que ayuda a cumplir con normativas y auditorías, y a demostrar que se están tomando las medidas adecuadas.*
- *Ayuda a las organizaciones a demostrar su postura de seguridad ante reguladores y partes interesadas.*
- *Ofrece herramientas que permiten a los analistas investigar incidentes de seguridad, rastrear actividades y entender el alcance de un ataque.*
- *Permite una respuesta rápida y efectiva a los incidentes, minimizando el daño potencial.*
- *Muchos SIEM pueden automatizar acciones de respuesta, como el aislamiento de un dispositivo comprometido o la ejecución de scripts para mitigar amenazas.*
- *Recopilan y almacenan datos de logs que son esenciales para el análisis forense post-incidente. Esto ayuda a entender cómo ocurrió un ataque y qué vulnerabilidades fueron explotadas.*
- *Permiten correlacionar eventos de diferentes fuentes, facilitando la identificación de patrones de ataque y la evaluación de su impacto.*

Características principales:

- *Ofrecen dashboards que permiten a los usuarios seguir la seguridad de manera clara y efectiva, haciendo que la información sea fácil de entender y de usar.*
- *Se integra sin problemas con otros recursos de seguridad, tales como cortafuegos, antivirus y sistemas de alerta ante intrusiones.*
- *Pueden integrarse con otras herramientas de seguridad, facilitando una respuesta coordinada y eficiente a incidentes*
- *Puede ajustarse a medida que la organización crece, lo que asegura que siempre cumpla con sus necesidades.*
- *Permite automatizar tareas repetitivas, como responder a incidentes y generar informes. Esto libera tiempo para que el equipo se enfoque en tareas más estratégicas.*
- *Incluye datos sobre amenazas externas, lo que mejora la capacidad de identificar y reaccionar de forma más eficaz ante incidentes de seguridad.*
- *Al ofrecer análisis de incidentes anteriores, las organizaciones pueden ajustar sus políticas y controles de seguridad, mejorando su postura general.*

Ejemplos de herramientas SIEM open source:

ELK Stack (Elasticsearch, Logstash y Kibana). Es una herramienta SIEM de código abierto que integra 3 componentes:

- *Elasticsearch. Es un sistema que facilita la búsqueda y el estudio de grandes volúmenes de información.*

- *Logstash. Es un recurso que recoge, transforma y transmite información a Elasticsearch.*
- *Kibana. Es un panel que permite visualizar y examinar la información que se encuentra almacenada en Elasticsearch.*

ELK Stack se caracteriza por ofrecer:

- *Análisis en tiempo real para monitorear eventos y detectar anomalías.*
- *Dashboards personalizables para mostrar información relevante.*
- *Integración con otras herramientas y sistemas para una mayor funcionalidad.*
- *Permite la recolección y centralización de logs de múltiples fuentes, lo que facilita el acceso a información crítica durante un incidente.*
- *Elasticsearch permite realizar búsquedas y análisis en tiempo real, lo que ayuda a los analistas a identificar rápidamente la naturaleza y el alcance de un incidente.*
- *Kibana ofrece dashboards que permiten visualizar datos de seguridad en tiempo real, facilitando la identificación de patrones y anomalías que podrían indicar un incidente.*
- *Las visualizaciones pueden incluir alertas que se activan ante ciertos umbrales, permitiendo una respuesta rápida.*

Wazuh. Es una plataforma de seguridad de código abierto que proporciona capacidades de monitoreo, detección de intrusiones y análisis de seguridad. Está diseñada para ayudar a las organizaciones a gestionar la seguridad de sus sistemas y aplicaciones.

Wazuh se caracteriza por:

- *Recopilar y analizar datos de seguridad en tiempo real desde diferentes fuentes, como servidores, aplicaciones y dispositivos de red,*
- *Utiliza reglas predefinidas y personalizables para detectar actividades sospechosas.*
- *Permite la recopilación y análisis de logs de diferentes fuentes, facilitando la identificación de incidentes de seguridad.*
- *Asiste a las entidades con regulaciones y criterios de seguridad mediante auditorías y reportes.*
- *Se puede integrar fácilmente con Elasticsearch, Logstash y Kibana para visualización y análisis avanzado de datos.*
- *Complementa ELK al proporcionar capacidades de detección de intrusiones y respuesta automatizada. Puede ejecutar scripts o acciones específicas en respuesta a eventos detectados.*
- *Permite definir reglas que desencadenan respuestas automáticas, como el bloqueo de IPs o la notificación a los administradores.*
- *La capacidad de ELK para almacenar grandes volúmenes de datos permite a los equipos de seguridad realizar análisis forenses exhaustivos después de un incidente.*
- *Facilita la correlación de eventos y la identificación de la cadena de eventos que llevaron a un incidente, lo que es esencial para entender y mitigar futuros riesgos.*
- *Genera informes que ayudan a las organizaciones a aprender de los incidentes, ajustando sus políticas y procedimientos de seguridad.*

- *Sus registros centralizados y las capacidades de análisis proporcionan una base sólida para auditorías y cumplimiento normativo.*

CIS "Center For Internet Security"

Son un conjunto de prácticas recomendadas para mejorar la ciberseguridad en organizaciones, y acumplir con regulaciones de seguridad.

Estan compustos por:

- *CIS Controls.* Son un conjunto de 18 controles de seguridad que proporcionan un marco para protegerse contra las amenazas más comunes. Estos controles están diseñados para ser implementados de manera prioritaria y pueden adaptarse a diferentes tipos de organizaciones.
- *CIS Benchmarks.* Son guías de configuración segura que se ofrecen para diversos sistemas operativos, aplicaciones y dispositivos. Estas guías permiten evaluar la configuración actual de los sistemas y realizar mejoras, facilitando así el cumplimiento de los estándares de seguridad recomendados.

Laboratorio de Pentesting Red Team

La identificación y mitigación de vulnerabilidades son cruciales para proteger la información en las organizaciones, especialmente en un contexto donde los datos son un activo valioso. Durante el desarrollo de este laboratorio, asumiremos el rol de miembros de un equipo Red Team, encargándonos de investigar una posible fuga de información en un equipo que opera con Windows 7, y que podría tener fallas de seguridad. Se llevará a cabo una práctica controlada para evaluar la seguridad de la máquina objetivo mediante la identificación y explotación de

vulnerabilidades, con el fin de entender el impacto potencial que estas pueden tener en la integridad del sistema.

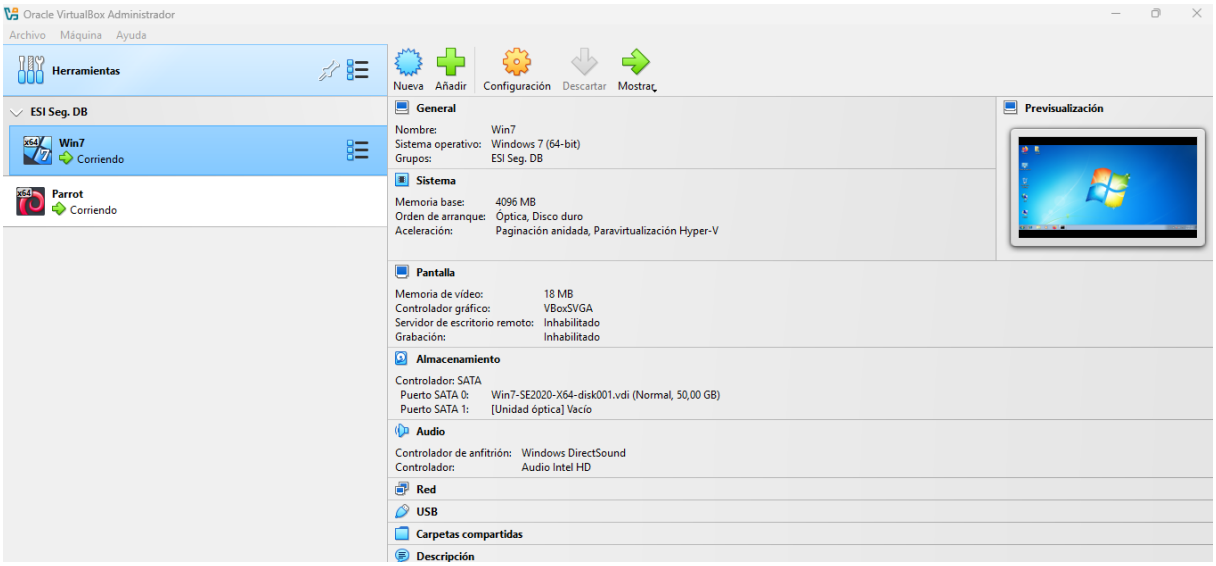
Se utilizarán herramientas de pruebas de penetración como Nmap y Metasploit para recopilar información y explotar vulnerabilidades. Los resultados ofrecerán una visión clara de la seguridad de la máquina y ayudarán a desarrollar estrategias para prevenir futuros ataques.

Preparación del Ambiente Controlado

Se realiza la descarga de las máquinas virtuales suministradas previamente por la Directora del curso, una de las cuales será objeto de análisis y explotación de vulnerabilidades.

Figura 8

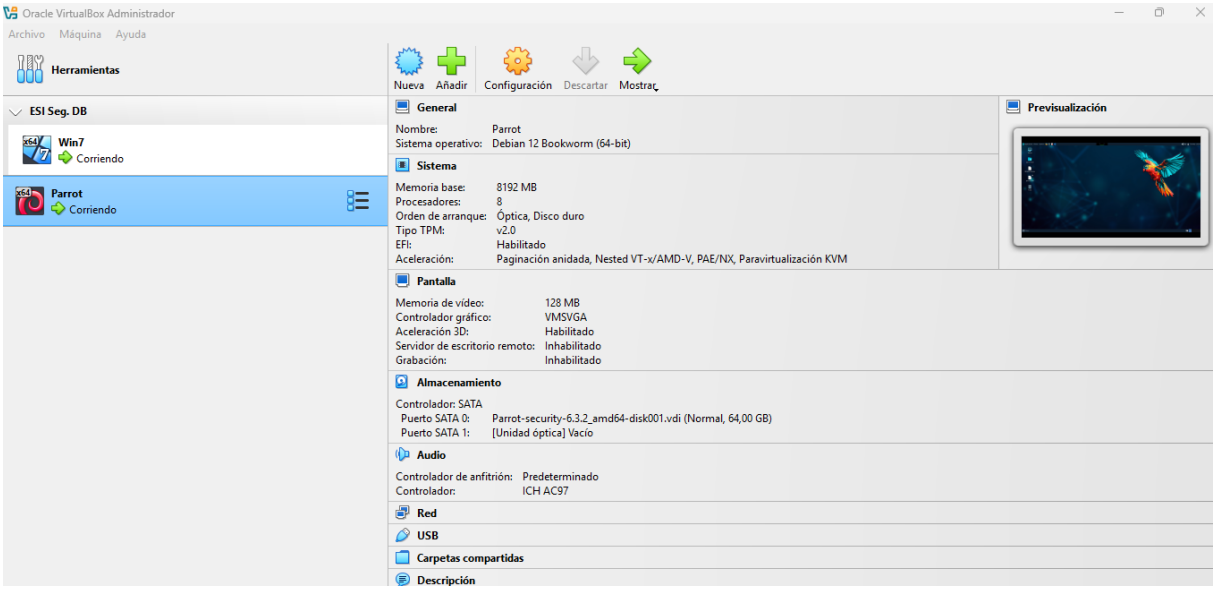
Máquina virtual Windows 7 importada



Nota. Elaboracion propia.

Figura 9

Máquina virtual Parrot importada



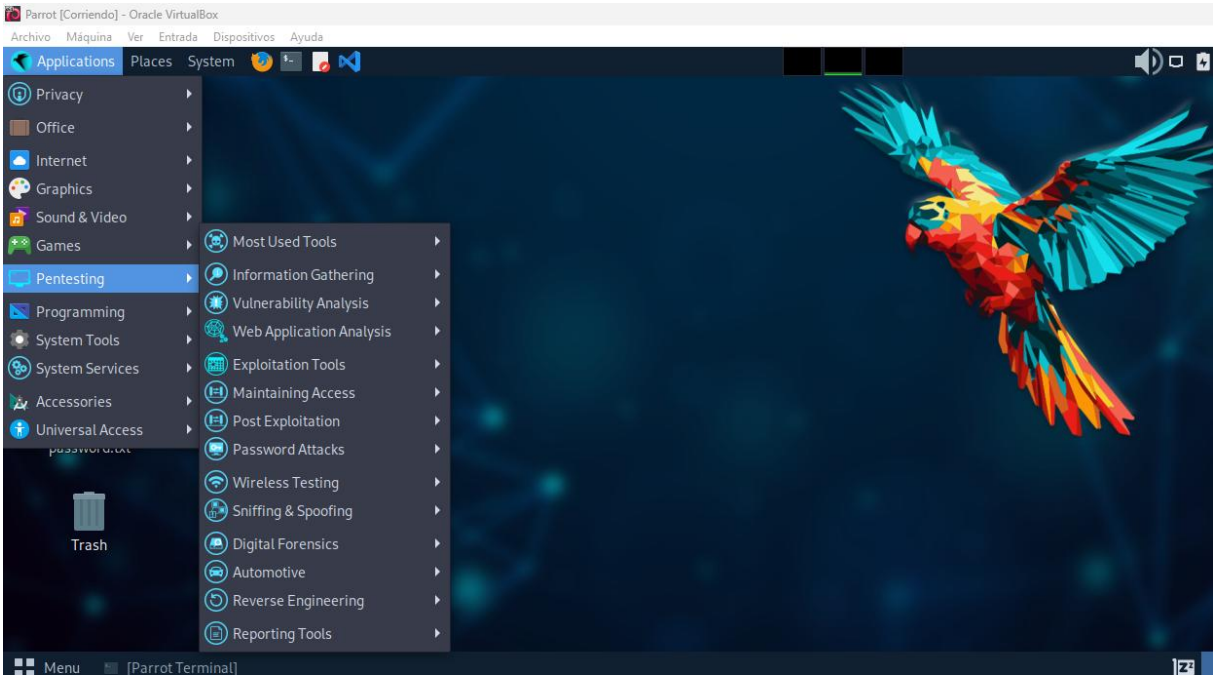
Nota. Elaboracion propia.

Se importan las maquinas virtuales con Windows 7 y Parrot en vittualbox, y se configuran los adaptadores de red como Adaptador puente, para que estas tomen direccionamiento por DHCP de la red local.

De acuerdo a la información suministrada en el anexo 4 – escenario 3 nuestra maquina objetivo será la que cuenta con sistema operativo Windows 7, y la maquina atacante que utilizaremos será la Parrot, que cuenta con herramientas de pentesting precargadas.

Figura 10

Herramientas de pentesting maquina atacante Parrot



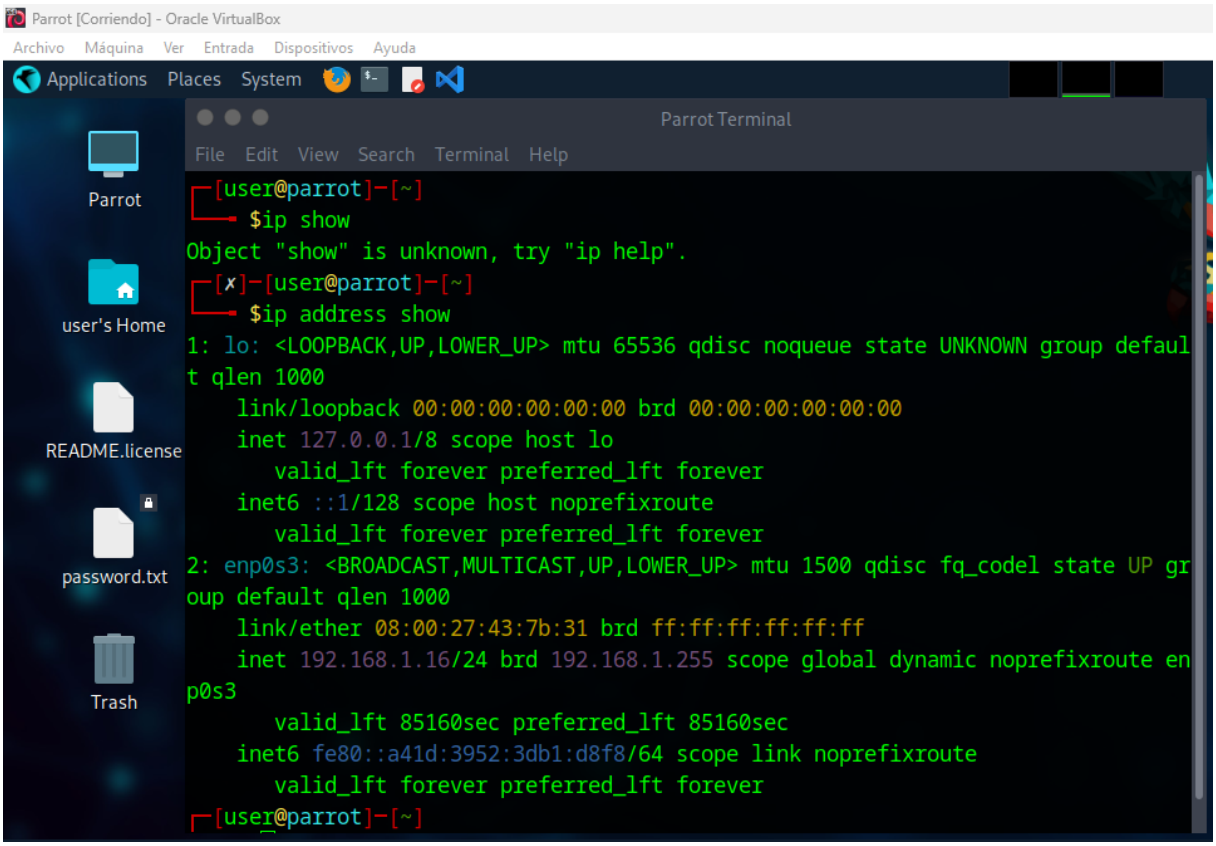
Nota. Elaboracion propia.

Reconocimiento

Procederemos a identificar la dirección IP de la maquina atacante, para esto abrimos un terminal de comandos en la máquina Parrot y ejecutamos el comando: ip address show, lo que nos proporcionará el siguiente resultado:

Figura 11

Validación direccionamiento IP MV Parrot



Nota. Elaboracion propia.

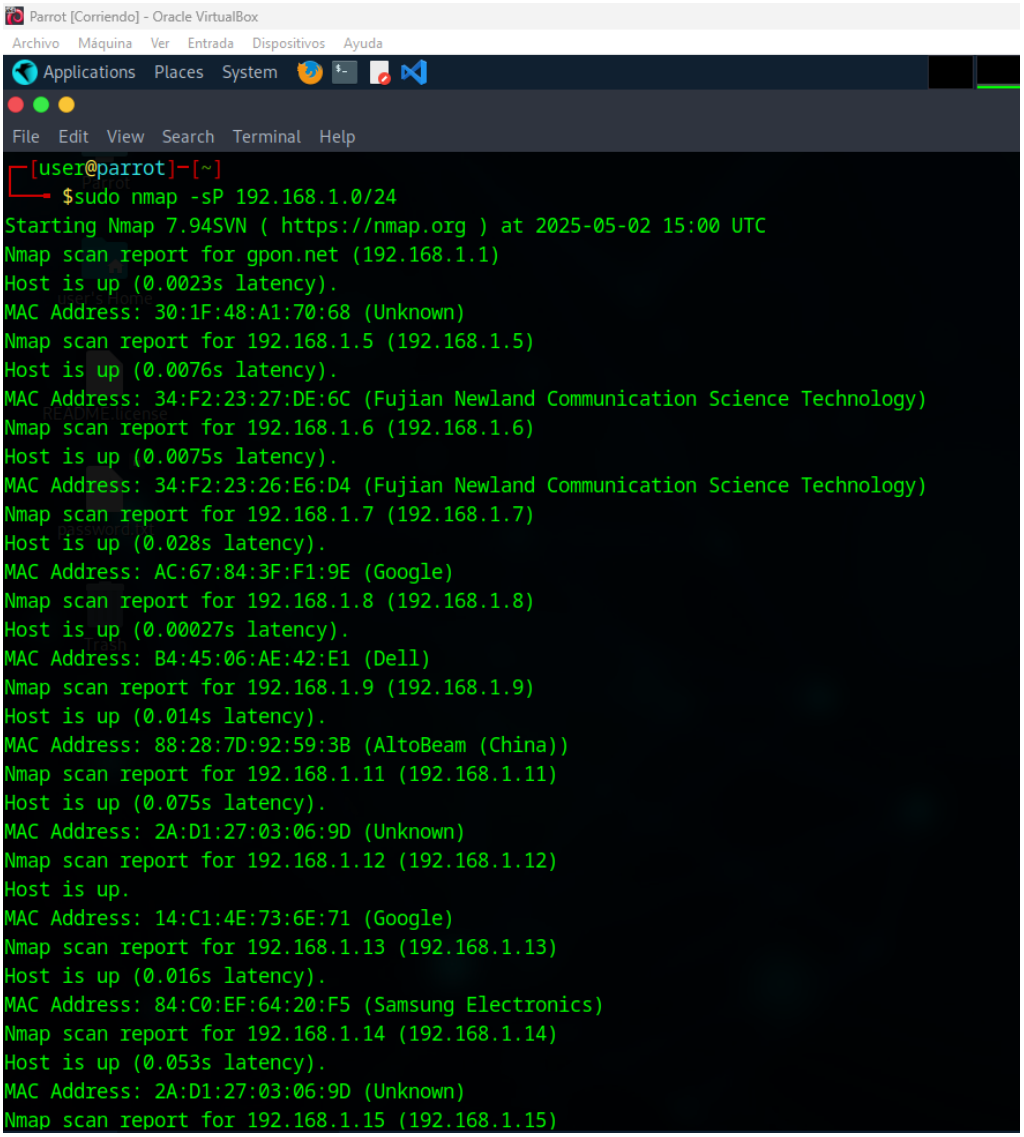
Nuestro equipo atacante tiene asignada la dirección IP 192.168.1.16. Continuando con el reconocimiento de nuestras máquinas, se procede a identificar los equipos que se encuentran conectados sobre la misma red, para esto emplearemos la herramienta Nmap. Esta herramienta permite realizar un mapeo de redes, para identificar los dispositivos conectados a ellas. Gracias a

Nmap es posible identificar los sistemas operativos, y servicios que se están ejecutando en una red, puertos abiertos, y posibles vulnerabilidades. A partir del direccionamiento identificado en nuestro equipo atacante, procederemos a ejecutar el siguiente comando "nmap -sP ip/rango"

(nmap –sP 192.168.1.0/24), con el objetivo de determinar que host están activos o no en nuestra red.

Figura 12

Escaneo de red con nmap -sP ip/rango desde el equipo atacante



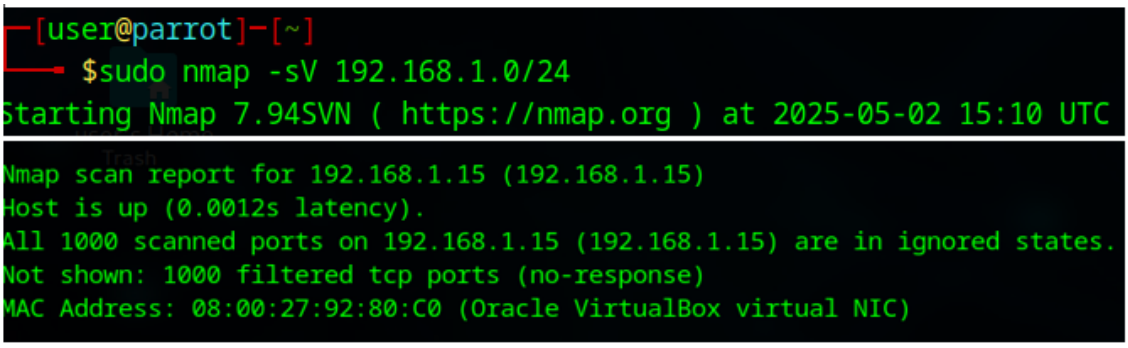
Nota. Elaboracion propia.

Por el momento logramos identificar los equipos activos sobre la red, pero aún no conocemos nuestra maquina objetivo. A continuación, utilizaremos el comando“Nmap -sV

ip/rango” (Nmap -sV 192.168.1.0/24), que nos permitirá observar un poco mas de detalles sobre los equipos previamente detectados, en este caso no nos permitió visualizar el sistema operativo puntual de nuestro equipo objetivo, pero deducimos cual puede ser porque hay uno que hace referencia al virtualizador, sobre el cual solo tenemos activos dos equipos, y ya sabemos que la IP de nuestro equipo atacante es la 192.168.1.16, por lo que la de nuestro equipo objetivo debería ser 192.168.1.15.

Figura 13

Escaneo de red con Nmap -sV ip/rango desde el equipo atacante

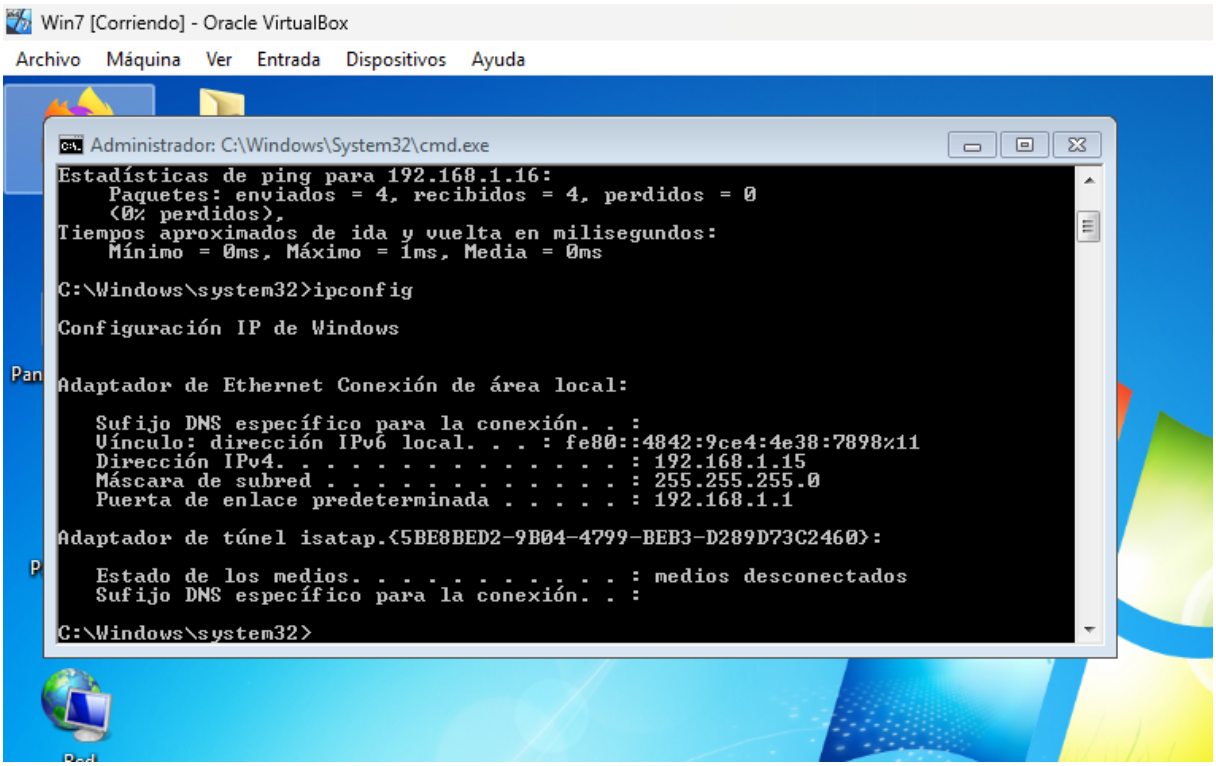


Nota. Elaboracion propia.

En este caso como tenemos acceso a la maquina Windows 7, podemos comprobar su direccionamiento.

Figura 14

Comprobación direccionamiento IP equipo objetivo



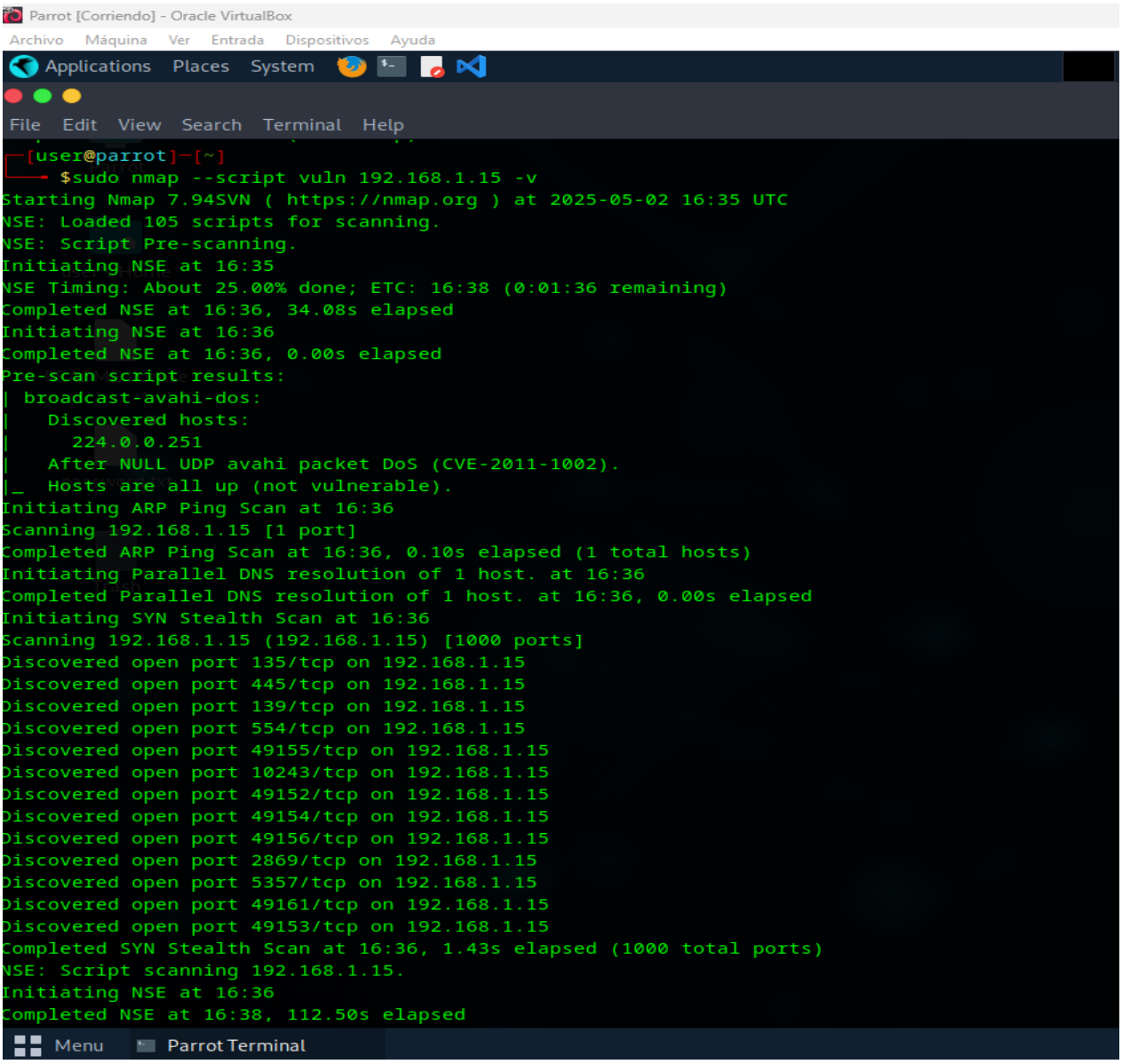
Nota. Elaboracion propia.

Escaneo y enumeración

Cabe aclarar que vamos a suponer que nuestro equipo Windows 7 no tiene activa la protección del Firewall del sistema, lo desactivamos temporalmente ya que sin ello no fue posible un escaneo completo del equipo objetivo, y procedemos con la ejecución del comando “sudo Nmap --script vuln <target domain or IP Address> -v” que permitirá realizar un escaneo de vulnerabilidades, utilizando una colección de scripts de Nmap específicos para detectar vulnerabilidades conocidas.

Figura 15

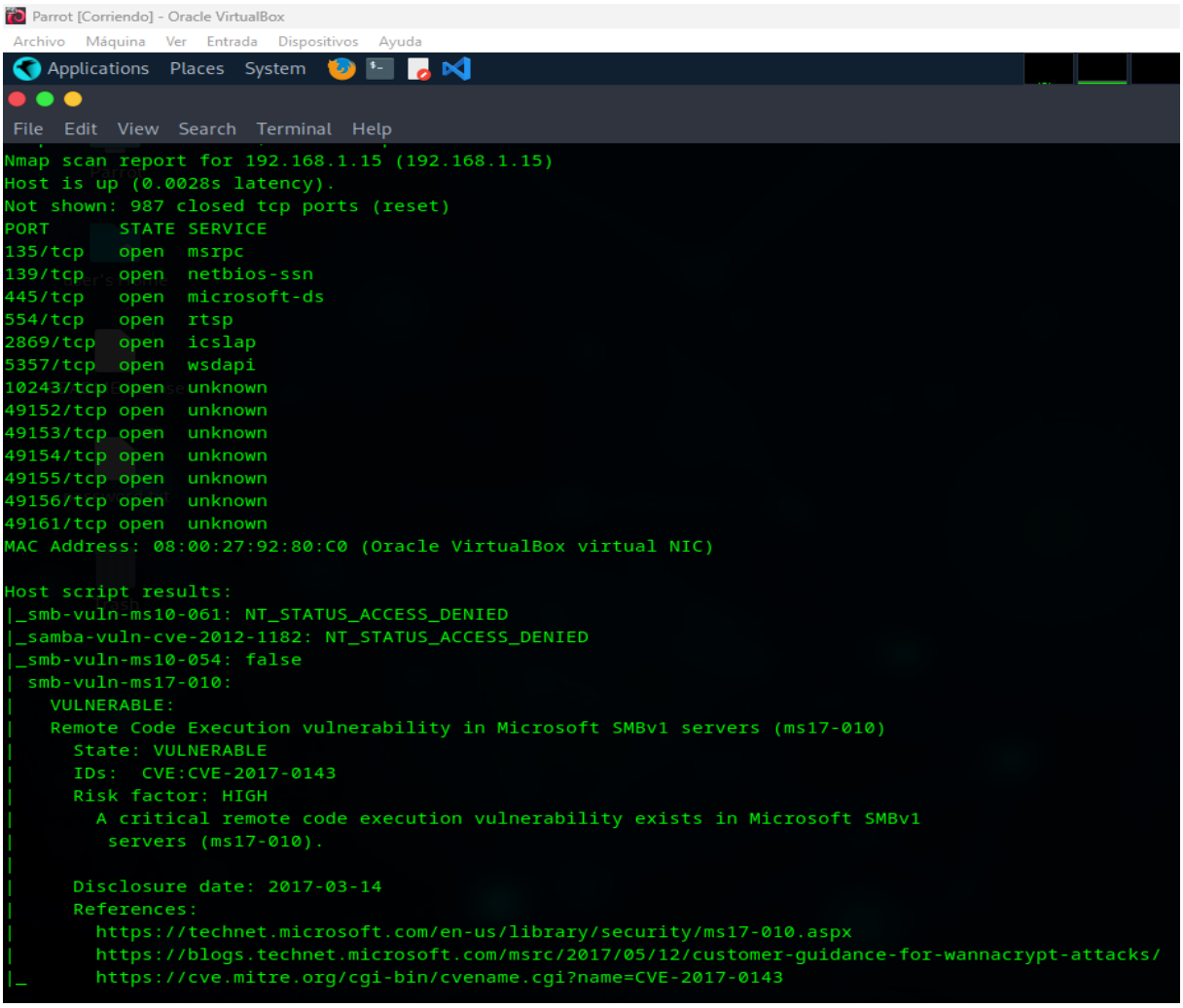
Primera parte ejecución del comando sudo Nmap --script vuln 192.168.1.15 -v



Nota. Elaboracion propia..

Figura 16

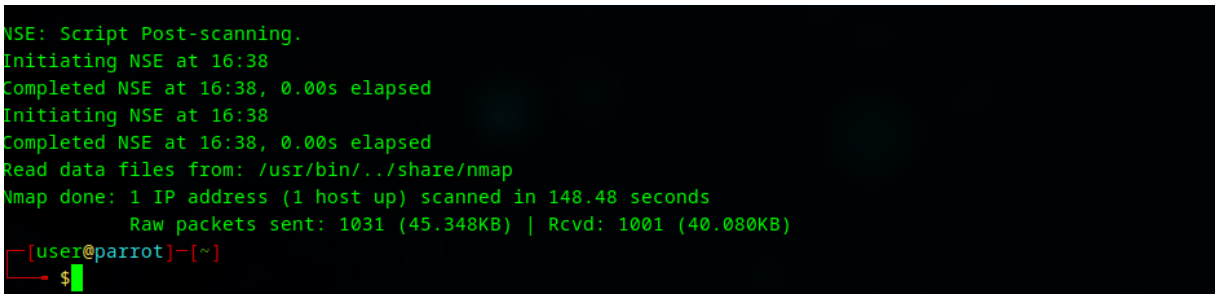
Segunda parte ejecucion del comando sudo Nmap --script vuln 192.168.1.15 -v



Nota. Elaboracion propia.

Figura 17

Tercera parte ejecución del comando sudo Nmap --script vuln 192.168.1.15 -v

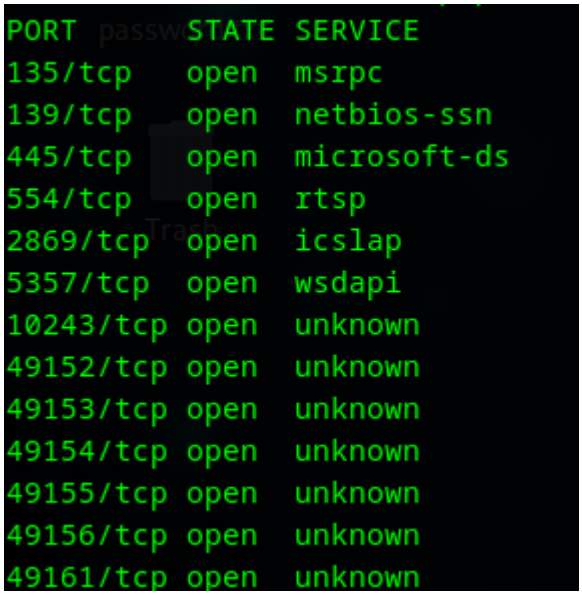


Nota. Elaboracion propia.

Este escaneo se realizó sobre 1000 puertos, encontrando varios de ellos abiertos:

Figura 18

Puertos abiertos host 192.168.1.15

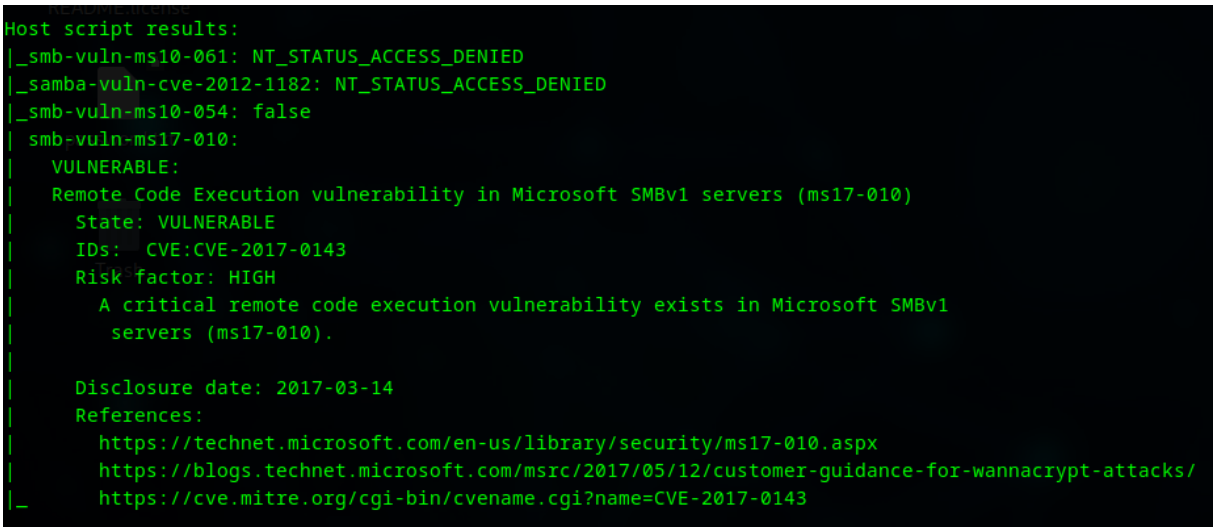


Nota. Elaboracion propia.

Entre los puertos abiertos, destacan los 135/tcp, 139/tcp y 445/tcp, que son utilizados por servicios de Microsoft y pueden ser susceptibles a ataques. También está el puerto 554/tcp, que se usa comúnmente para transmitir video. Hay otros puertos abiertos que no tienen un servicio conocido, pero podrían estar ejecutando servicios que no están documentados o que no son seguros.

Figura 19

Vulnerabilidades detectadas



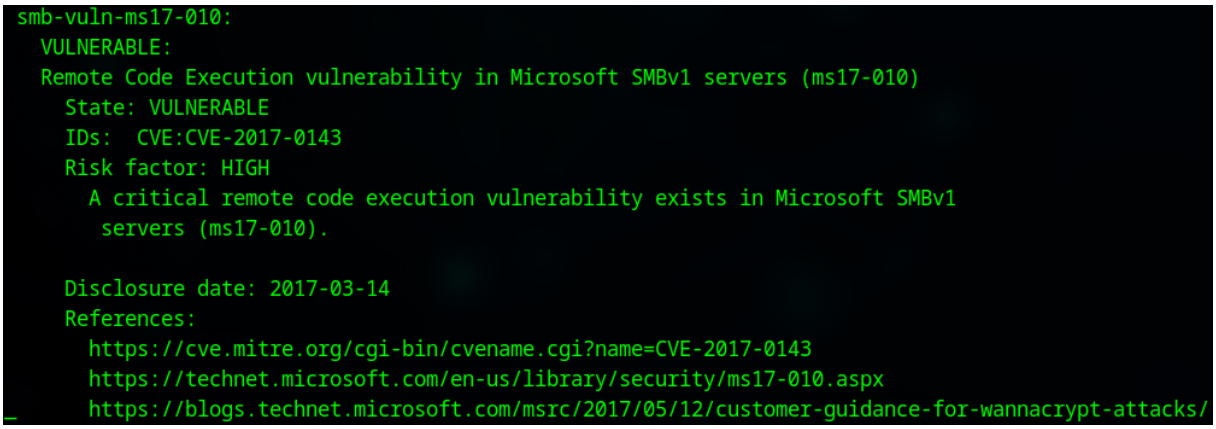
Nota. Elaboracion propia.

Los resultados revelaron varias vulnerabilidades, entre ellas smb-vuln-ms10-061, samba-vuln-cve-2012-1182 y smb-vuln-ms10-054, que se encuentran en un estado de acceso denegado. Esto sugiere que el sistema tiene permisos restringidos, lo cual indica que podría estar protegido contra estos tipos de ataques.

Por otro lado, los hallazgos también señalaron un alto grado de riesgo asociado con la vulnerabilidad CVE-2017-0143 (smb-vuln-ms17-010), conocida como EternalBlue. Esta falla crítica en el protocolo SMB de Microsoft permite a los atacantes ejecutar código de forma remota, con lo que podría tomar control del sistema afectado y, potencialmente, propagar malware a través de la red.

Figura 20

Vulnerabilidad activa



Nota. Elaboracion propia.

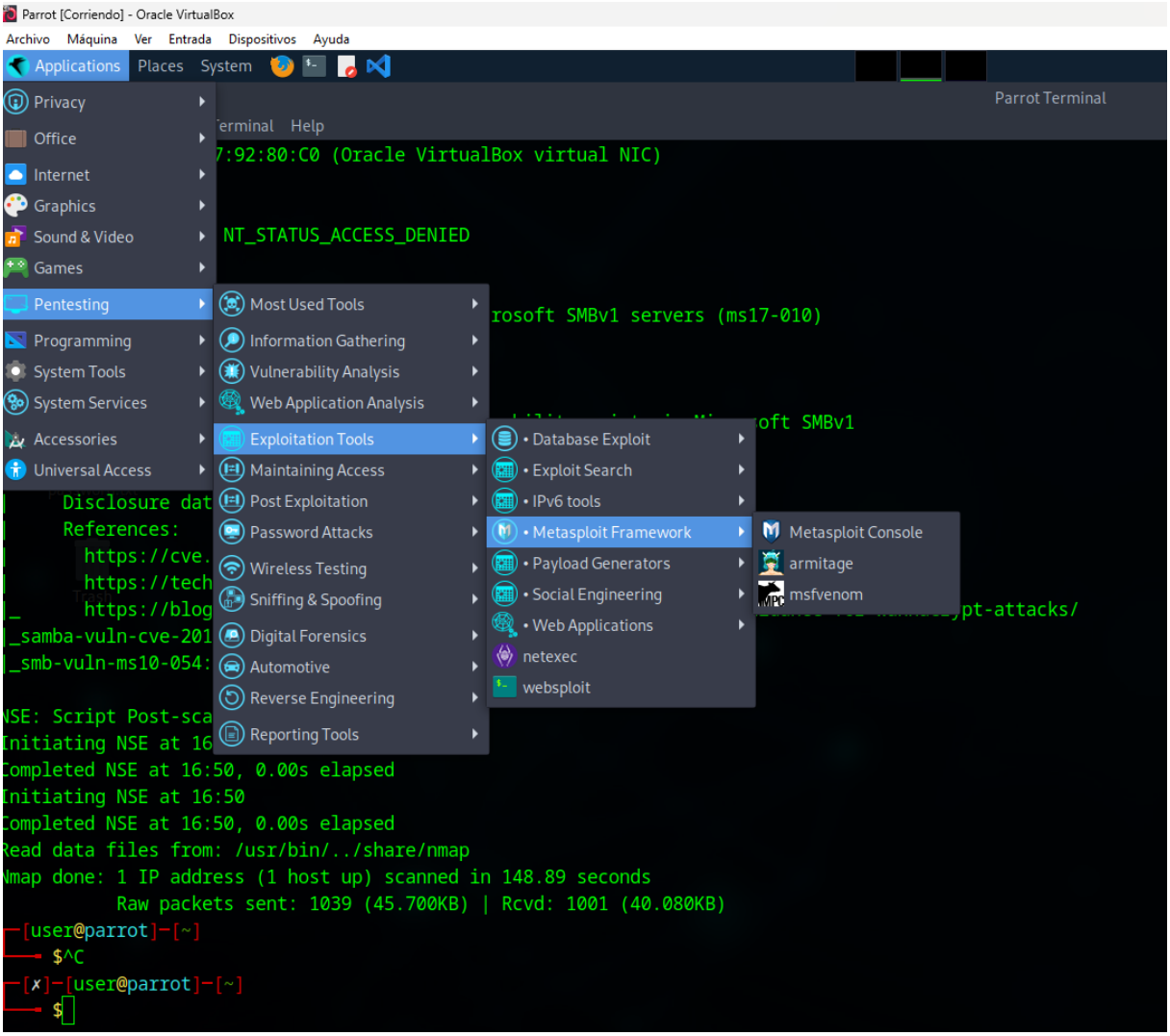
Exploit

La vulnerabilidad encontrada nos sugiere que es posible ejecutar código de manera remota en el equipo objetivo, lo cual coincide con lo solicitado en el escenario 3, donde intentaremos crear un usuario administrador con mi primer nombre y mi primer apellido.

Validamos dentro de las aplicaciones de pentesting de nuestro S:O. Parrot, y encontramos dentro de las herramientas de explotación, la consola de Metasploit, con la que hemos interactuado en otras oportunidades, la cual utilizaremos para esta práctica.

Figura 21

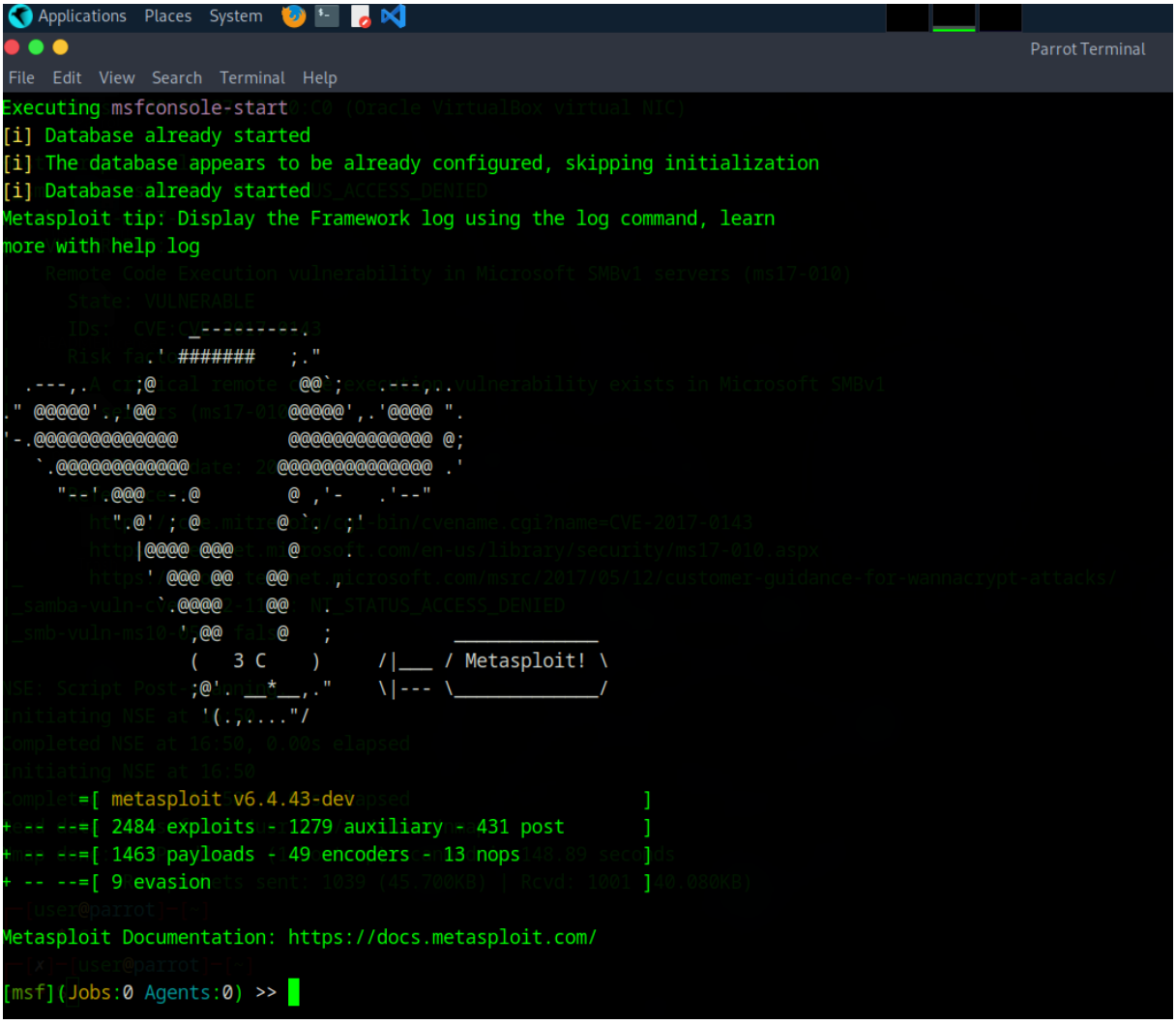
Validación herramientas de explotación preinstaladas



Nota. Elaboracion propia.

Figura 22

Metasploit framework

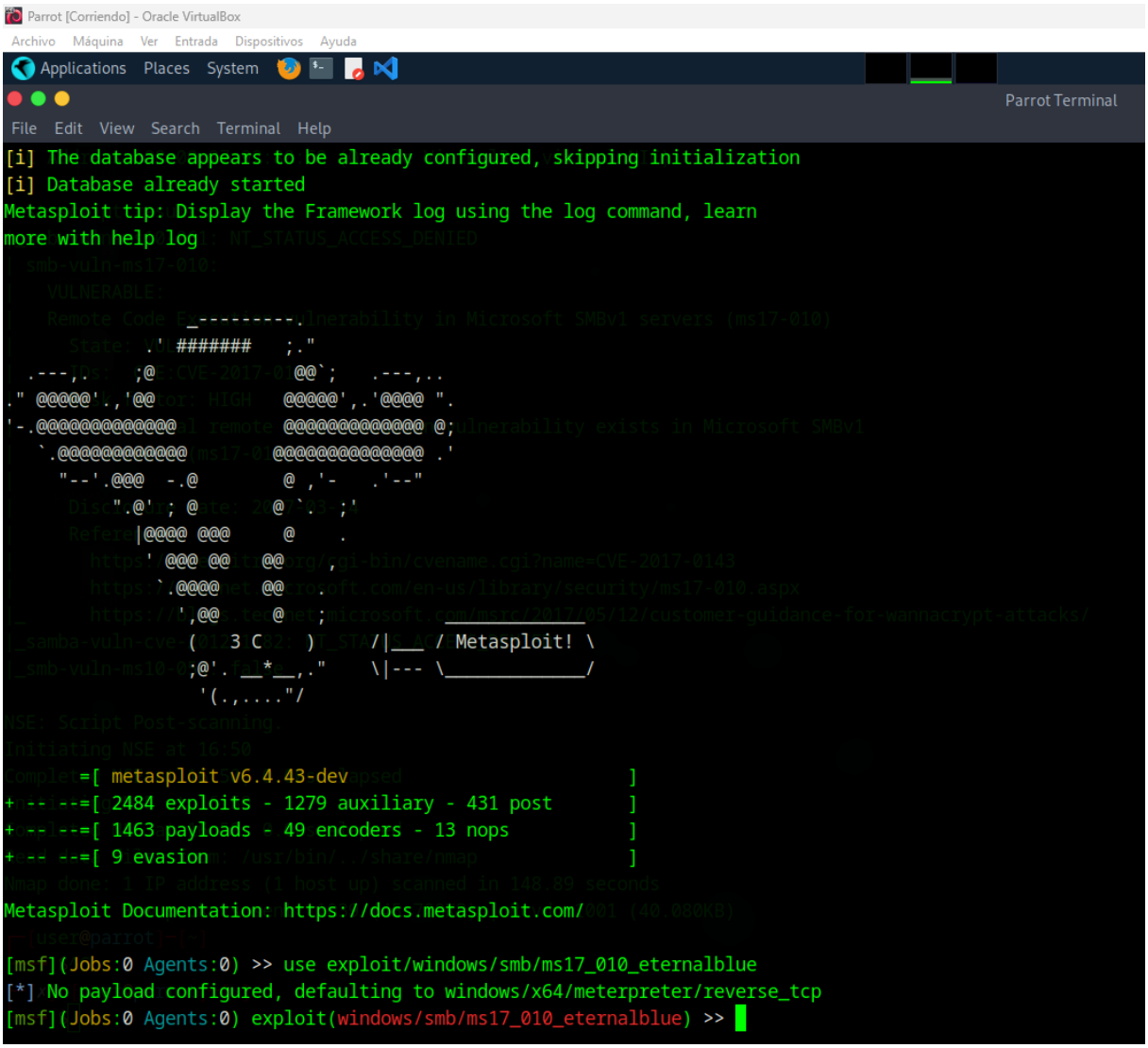


Nota. Elaboracion propia.

Procedemos a cargar el modulo de EternalBlue a través del comando use exploit/windows/smb/ms17_010_eternalblue

Figura 23

Cargue del módulo Eternalblue

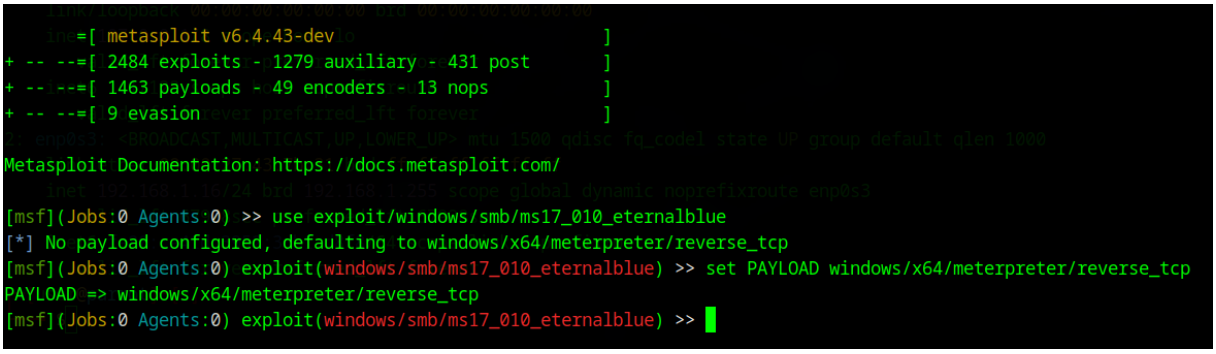


Nota. Elaboracion propia.

Podemos configurar el payload que podemos utilizar para la creación del usuario set PAYLOAD windows/x64/meterpreter/reverse_tcp.

Figura 24

Configuración de PAYLOAD

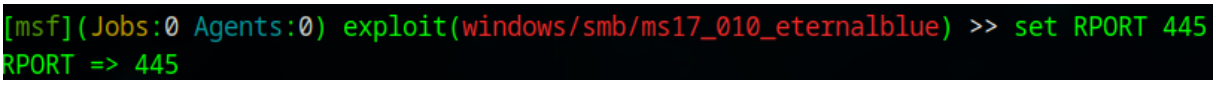


Nota. Elaboracion propia.

Establecemos el puerto 445 por defecto

Figura 25

Asignación del puerto por defecto

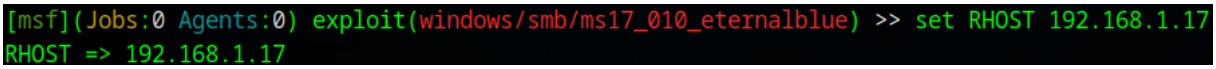


Nota. Elaboracion propia.

Configuramos la dirección IP del objetivo, que cambio durante un reinicio que tuve que hacer del equipo físico, la IP de nuestro equipo objetivo con Windows 7 ahora finaliza en 17, ejecutamos el siguiente comando set RHOST 192.168.1.17.

Figura 26

Configuración IP del equipo objetivo

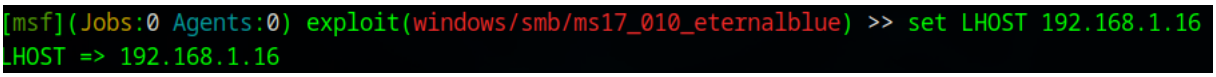


Nota. Elaboracion propia.

A continuación, configuramos la dirección IP de nuestro equipo atacante para recibir la conexión, lo hacemos a través del comando set LHOST 192.168.1.16.

Figura 27

Configuración IP del equipo atacante

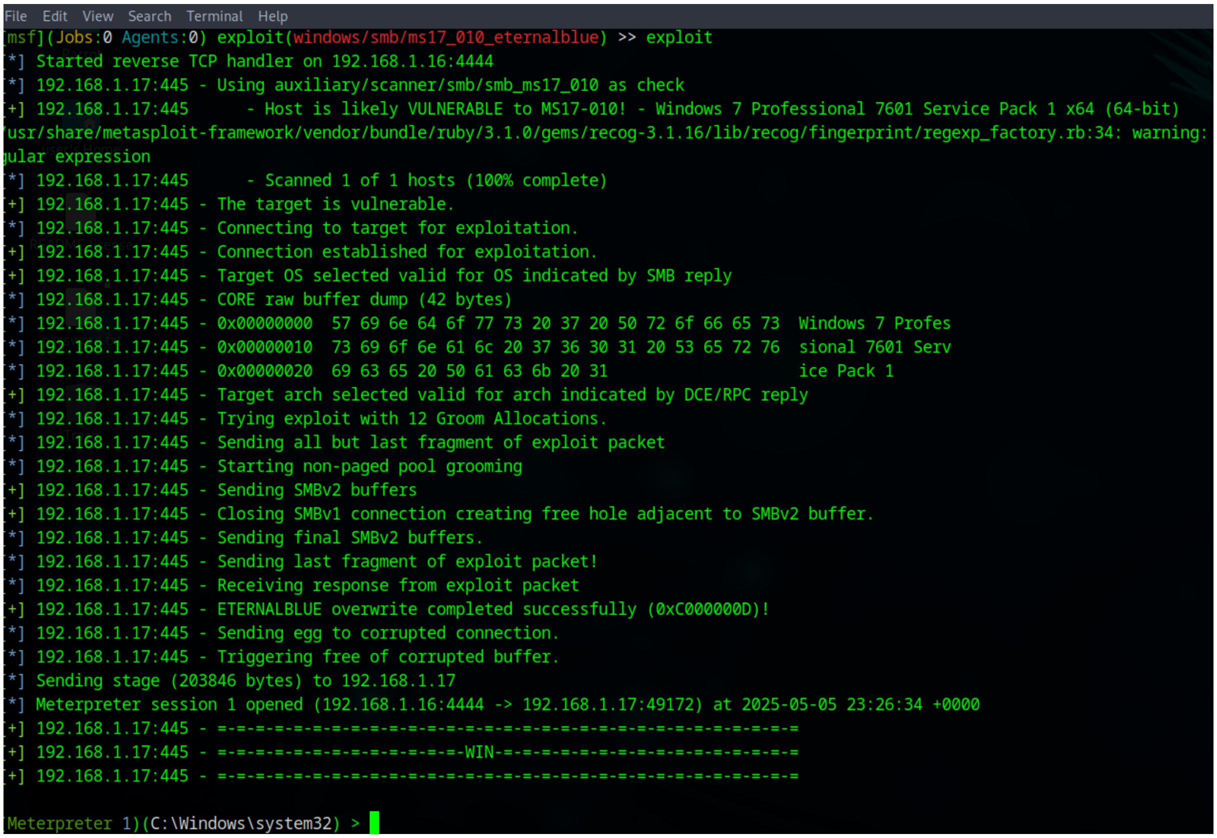


Nota. Elaboracion propia.

Ejecutamos el exploit

Figura 28

Ejecución del Exploit

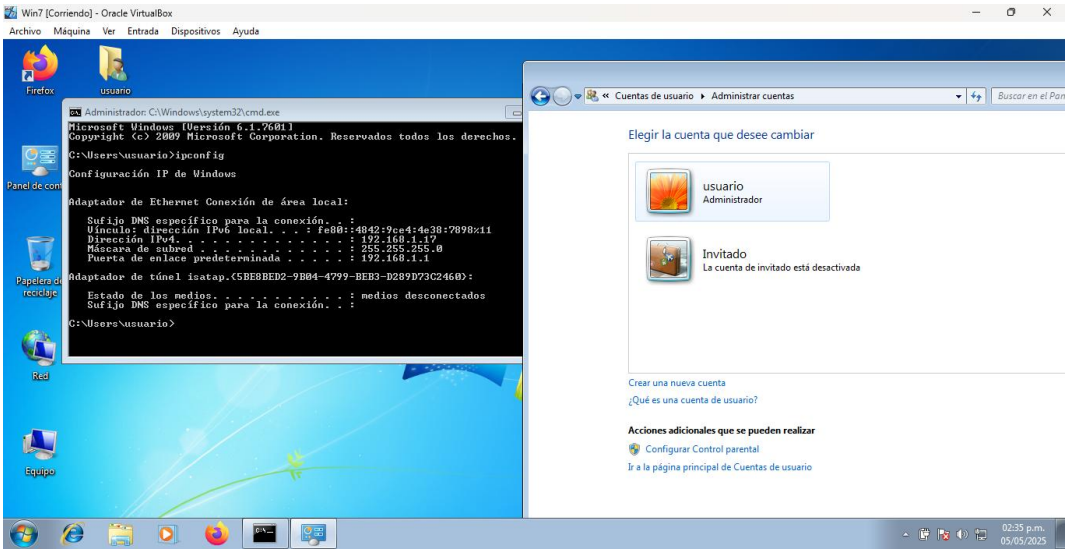


Nota. Elaboracion propia.

Como podemos observar la explotación es exitosa y obtenemos el acceso, pero antes de proceder con la creación del usuario requerido, validaremos con los que actualmente cuenta el equipo objetivo.

Figura 29

Usuarios equipo objetivo previos a la explotación

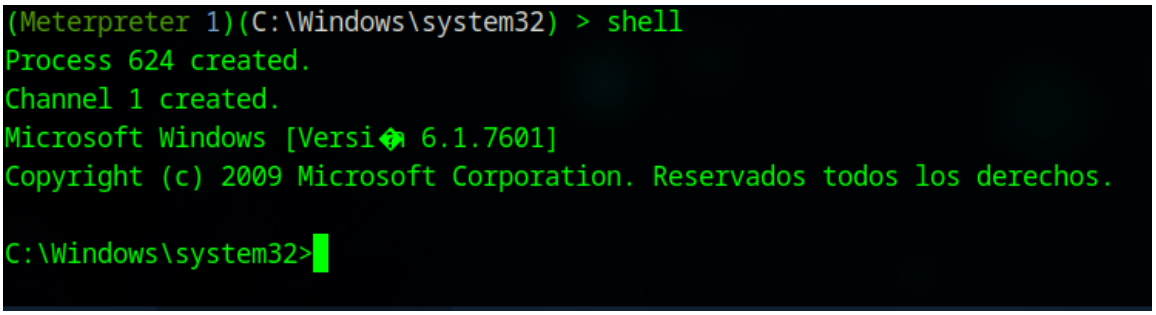


Nota. Elaboracion propia.

Ejecutamos el comando shell en meterpreter, con lo cual obtenemos acceso a una shell de Windows en el sistema objetivo, lo que nos permite ejecutar comandos de sistema operativo directamente en el equipo comprometido.

Figura 30

Acceso a través de Shell

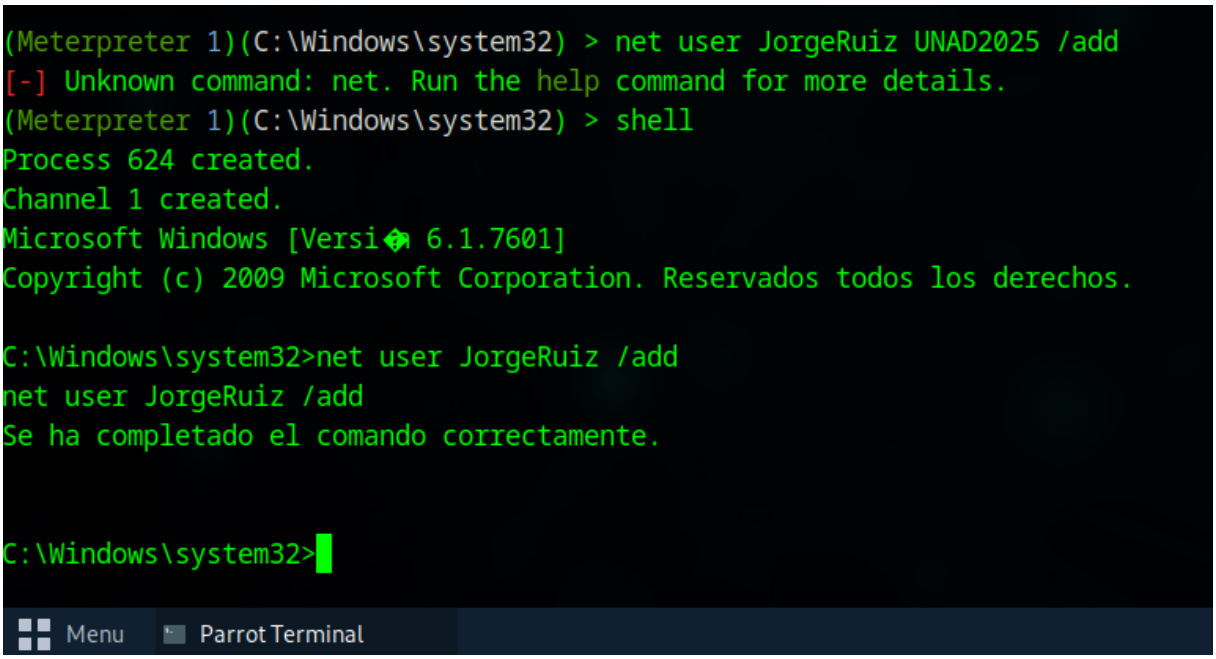


Nota. Elaboracion propia.

Procedemos con la creación de un nuevo usuario llamado JorgeRuiz a través del siguiente comando net user JorgeRuiz /add.

Figura 31

Creación del usuario JorgeRuiz

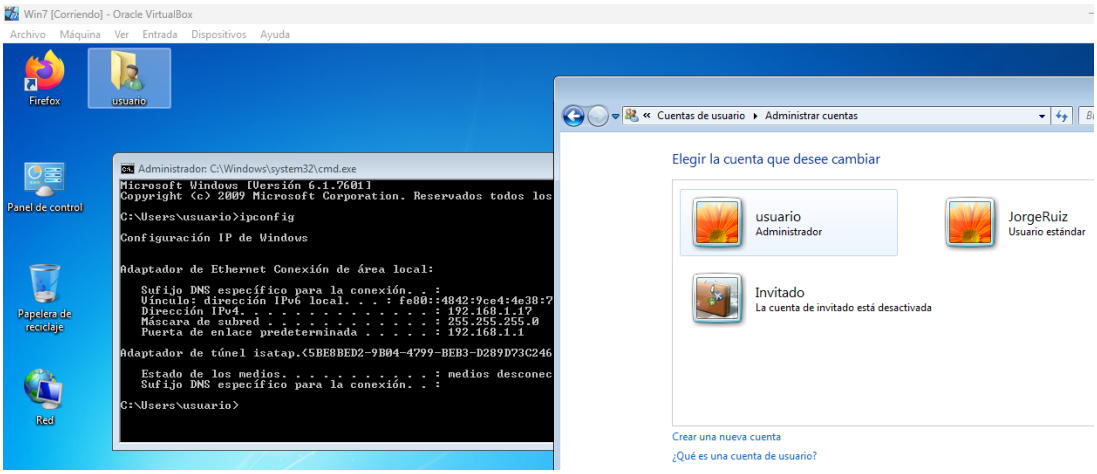


Nota. Elaboracion propia.

Como en este ejercicio contamos con acceso al equipo comprometido validamos la creación del usuario JorgeRuiz.

Figura 32

Validación creación de usuario JorgeRuiz

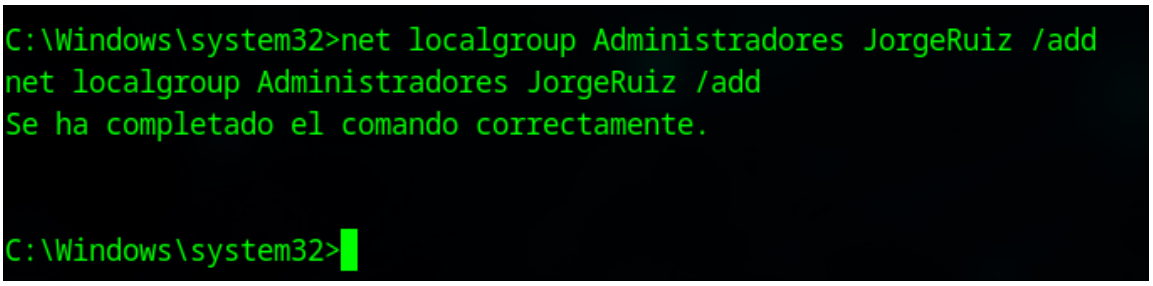


Nota. Elaboracion propia.

Se requiere que el usuario tenga privilegios de administrador, para lo cual ejecutamos el comando net localgroup Administrators JorgeRuiz /add.

Figura 33

Usuario agregado al grupo de Administradores

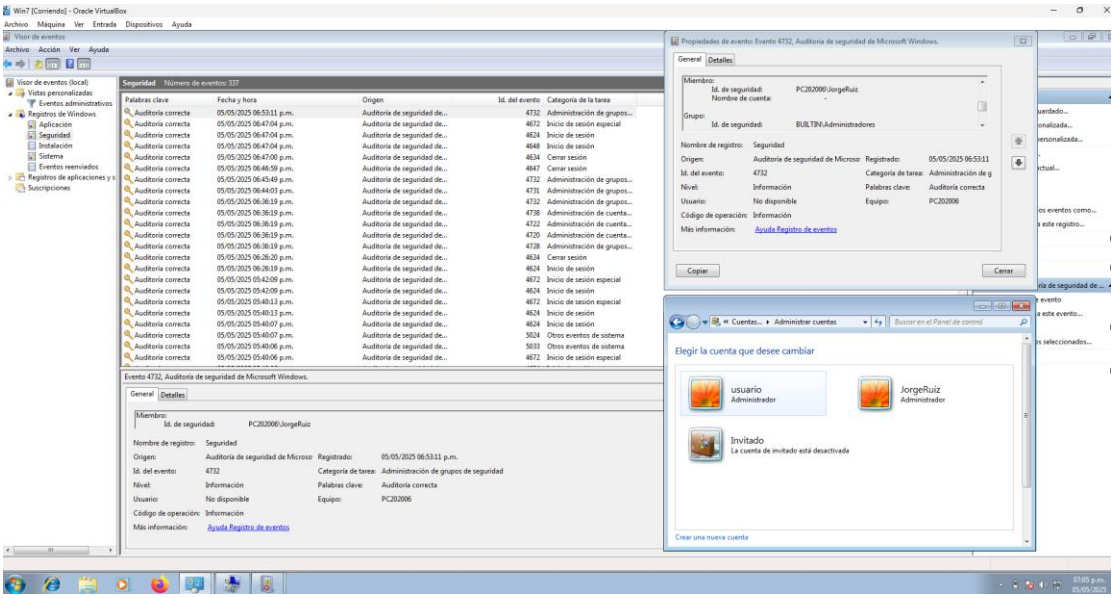


Nota. Elaboracion propia.

Verificamos que el nuevo usuario fue agregado correctamente al grupo de administradores en el sistema objetivo. Al otorgarle al usuario JorgeRuiz el rol de administrador, se han escalado sus privilegios en el equipo comprometido. Esto le da un alcance y control mucho mayor sobre el sistema, lo que podría permitirle llevar a cabo acciones más avanzadas y potencialmente dañinas.

Figura 34

Validaciones usuario administrador creado



Nota. Elaboracion propia.

Medidas de Hardenización que Propondría Blue Team para que el ataque no se Repita

- Garantizar que todos los sistemas instalen las últimas actualizaciones de seguridad, en nuestro caso para el equipo objetivo con Windows 7, Microsoft lanzo actualizaciones de seguridad para rectificar la vulnerabilidad CVE-2017-0143 (MS17-010).
- Desactivar los servicios y puertos de red que no sean realmente necesarios.

- Deshabilitar el uso del protocolo SMBv1, dado que numerosas vulnerabilidades críticas se vinculan con esta versión anterior.
- Restringir el acceso a los puertos abiertos únicamente a direcciones IP y usuarios autorizados.
- Establecer reglas de firewall rigurosas para bloquear el tráfico no autorizado, en este caso hacia los puertos usados por SMB.
- Examinar regularmente los registros del sistema para detectar actividades sospechosas o intentos de intrusión.
- Implementar herramientas de código abierto como OSSEC para detectar comportamientos sospechosos y filtrar el tráfico en redes y ordenadores.
- Efectuar copias de respaldo y pruebas de restauración de manera constante.

Conclusiones del Laboratorio de Pentesting

Durante el desarrollo de la prueba de pentesting, se utilizó la herramienta Nmap en las etapas de reconocimiento, y de escaneo y enumeración. Esta herramienta nos permitió realizar un escaneo de la máquina Windows para identificar los puertos abiertos y los servicios en ejecución. Gracias a ella encontramos la vulnerabilidad CVE-2017-0143 (smb-vuln-ms17-010), conocida como EternalBlue, que según lo consultado implicaba un alto grado de riesgo asociado con la ejecución de código de manera remota en equipos Windows.

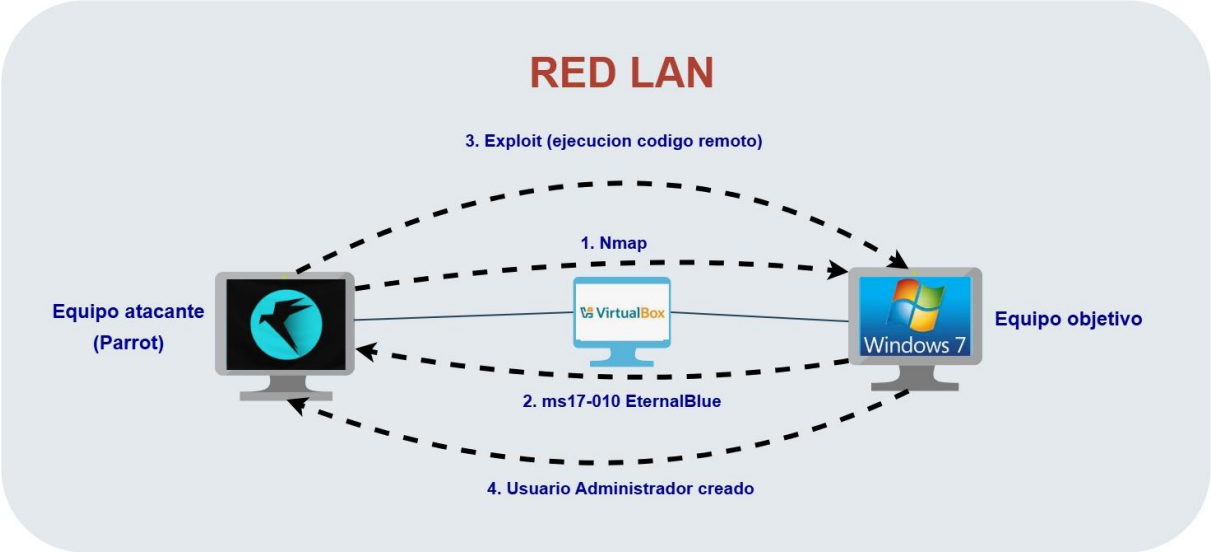
Para la etapa de explotación de la vulnerabilidad encontrada, se empleó metaexploit, que es un framework que permite explotar vulnerabilidades conocidas, como la encontrada a través de Nmap. A través de Metaexploit fue posible acceder al shell del equipo comprometido y crear un usuario con privilegios de administrador.

La vulnerabilidad ms17-010 (EternalBlue) explotada está relacionada con los puertos 135, 139 y 445, que son los puertos utilizados por los servicios SMBv1 de Windows a los que esta vulnerabilidad afecta.

Explotar la vulnerabilidad MS17-010, conocida como EternalBlue, tiene un impacto significativo sobre la maquina Windows, ya que permite ejecutar código remoto, y crear cuentas de usuario con privilegios de administrador, lo cual brinda un control total del sistema, esto podría tener consecuencias como el hurto de información privada, instalación de malware, propagación a otros sistemas de la red, y denegación de servicios.

Figura 35

Grafico explicativo del ataque



Nota. Elaboracion propia.

Vulnerabilidades y Tipos de Ataques Informáticos Más Comunes, y Cómo los Equipos de Seguridad Red Team y Blue Team Pueden Contribuir a Mitigarlos

Vulnerabilidades Más Comunes

Fallas en la Configuración de Sistemas

La configuración equivocada de los sistemas constituye una de las vulnerabilidades más habituales en el campo de la ciberseguridad. Estos fallos generalmente se producen cuando los administradores no establecen configuraciones seguras o mantienen configuraciones predeterminadas que pueden ser utilizadas con facilidad por intrusos.

Este tipo de fallos pueden propiciar el ingreso no permitido a sistemas, redes o aplicaciones, poniendo en peligro la privacidad, integridad y disponibilidad de la información, amenazando así la seguridad de la entidad.

Para tratar esta vulnerabilidad, el Red Team lleva a cabo pruebas de penetración con la finalidad de detectar configuraciones inseguras, como contraseñas configuradas de manera predeterminada o servicios no esenciales activados. Por otro lado, el Blue Team emplea estos descubrimientos para realizar modificaciones en las configuraciones, desactivar servicios no indispensables y realizar auditorías regulares. Este enfoque integral garantiza que las instalaciones sean sólidas y satisfagan los estándares de seguridad apropiados.

Software desactualizado

El uso de software sin actualizar es una de las vulnerabilidades más utilizadas por los ciberdelincuentes. Los sistemas desactualizados generalmente poseen fallos identificados, que los atacantes pueden aprovechar de manera sencilla mediante herramientas automatizadas.

Estos sistemas representan un blanco ideal para ataques como la explotación de vulnerabilidades (exploits), lo que puede resultar en pérdida de datos, interrupciones en el servicio e incluso el secuestro de información mediante ransomware. Las principales causas de esta situación incluyen la falta de soporte por parte del fabricante del software o la negativa de las organizaciones a realizar actualizaciones, ya sea por temor a provocar errores o incompatibilidades con sus sistemas internos.

En relación al software desactualizado, el Red Team simula ataques utilizando vulnerabilidades detectadas, para demostrar los peligros asociados a la falta de actualizaciones, mientras que el Blue Team establece procesos de gestión de actualizaciones, vigila las vulnerabilidades recientemente detectadas y realiza pruebas de compatibilidad antes de poner en marcha actualizaciones. Así se reduce el riesgo de utilización de sistemas desactualizados.

Errores humanos

El factor humano continúa siendo una de las principales razones de incidentes de seguridad en las entidades. Los errores cometidos por los empleados, ya sea por desconocimiento, falta de capacitación o descuido, pueden abrir la puerta a los atacantes, facilitando amenazas como el phishing, la instalación de malware o la divulgación involuntaria de información sensible.

Para reducir estos riesgos, el Red Team realiza simulacros de ataques de ingeniería social, tales como campañas de phishing, con la finalidad de valorar la susceptibilidad de los empleados

frente a estas estrategias. En contraposición, el Blue Team implementa programas de formación continua ajustados a las demandas de la organización y define políticas precisas para reducir el efecto del factor humano. Además, pone en marcha herramientas de monitoreo que facilitan la detección de actividades atípicas, previendo posibles fallos o accesos vulnerables. Este enfoque potencia la sensibilización y capacitación de los trabajadores ante las amenazas de seguridad.

Acceso no autorizado

La ausencia de mecanismos eficientes para administrar el acceso a sistemas y datos sensibles, constituye un serio peligro para la seguridad de las organizaciones, dado que facilita que individuos no autorizados pongan en riesgo su integridad. Esto puede resultar en el hurto de datos sensibles, sabotaje de sistemas o incluso espionaje empresarial, impactando directamente en el funcionamiento y la reputación de la organización.

Para tratar esta vulnerabilidad, el Red Team lleva a cabo ensayos dirigidos a detectar brechas en los controles de acceso, que incluyen el incremento de privilegios y movimientos laterales en la red, simulando estrategias que un atacante podría utilizar. Como respuesta, el Blue Team pone en marcha acciones como políticas fundamentadas en el principio de privilegio mínimo, una autenticación multifactor sólida y la segmentación de redes, lo que disminuye considerablemente el efecto de accesos no permitidos y fortalece la seguridad de los sistemas.

Falta de cifrado de datos

El cifrado de datos es un paso crucial para salvaguardar la información durante su almacenaje y difusión. La falta de cifrado deja los datos expuestos a ser interceptados o hurtados,

dado que pueden ser fácilmente leídos por atacantes que intercepten las comunicaciones o ingresen a sistemas vulnerables.

Frente a la ausencia de cifrado de información, el Red Team simula ataques como la interceptación de tráfico, con el objetivo de evidenciar cómo los datos no encriptados pueden ser robados, mientras que el Blue Team garantiza que los datos estén cifrados tanto en tránsito como en reposo, actualiza protocolos poco seguros y administra claves criptográficas de forma segura. Esto protege los datos frente a interceptaciones y hurtos.

Ataques Informáticos Más Comunes

Ataques de Phishing

El phishing es un método de engaño donde los atacantes se presentan como entidades de confianza para adquirir datos sensibles, tales como contraseñas, información bancaria o datos personales. Este tipo de ataque se lleva a cabo mayormente mediante emails, mensajes de texto (smishing) o llamadas telefónicas (vishing).

Malware

El malware, o software malicioso, es un programa diseñado para infiltrarse, dañar o controlar sistemas informáticos sin el consentimiento del usuario. Entre los tipos más comunes están los virus, gusanos y troyanos. El malware puede llegar a través de descargas de archivos aparentemente inofensivos o correos electrónicos maliciosos.

Ransomware

El Ransomware es un tipo de malware que cifra los archivos de un sistema y exige un rescate para desbloquearlos. Este tipo de ataque se ha vuelto cada vez más común y afecta tanto a empresas como a instituciones gubernamentales.

Ataques DDoS

Un ataque DDoS busca sobrecargar un servidor o servicio en línea enviando enormes cantidades de tráfico desde múltiples fuentes, lo que lo hace inaccesible para los usuarios legítimos.

Ingeniería Social

Los ataques de ingeniería social manipulan a las personas con el fin de revelar información sensible o realizar acciones que pongan en riesgo la seguridad. Los atacantes generalmente recurren a estrategias como el pretexto, la simulación de identidad o la creación de seguridad.

Hacking de Contraseñas

Este tipo de ataque utiliza técnicas como fuerza bruta o diccionarios para descifrar contraseñas y acceder a sistemas protegidos. Las contraseñas débiles son especialmente vulnerables.

Inyección SQL

La inyección SQL explota vulnerabilidades en bases de datos para manipularlas y acceder a información sensible. Este tipo de ataque es común en aplicaciones web mal configuradas.

Ataques Man-in-the-Middle (MitM)

Los ataques Man-in-the-Middle (MitM) son una técnica en la que un ciberdelincuente intercepta la comunicación entre dos partes (por ejemplo, un usuario y un servidor) para robar, manipular o alterar la información que se transmite. Estos ataques suelen ocurrir en redes Wi-Fi públicas, como las de cafeterías, aeropuertos o hoteles, donde la seguridad es limitada y los datos pueden ser fácilmente interceptados.

Ataques Zero-Day

Los ataques Zero-Day explotan vulnerabilidades desconocidas en software o hardware antes de que sean identificadas y corregidas. Son particularmente peligrosos porque no hay defensas disponibles contra ellos.

Secuestro de Sesiones.

Los atacantes toman control de sesiones activas para acceder a cuentas. En 2019, WhatsApp sufrió este tipo de ataque mediante la manipulación de códigos QR.

Suplantación de Identidad (Spoofing)

En un ataque de spoofing, los ciberdelincuentes se hacen pasar por otra persona o entidad para engañar a los usuarios y obtener acceso a sistemas o información.

Tabla 3

Vulnerabilidades comunes, ataques asociados y medidas de mitigación propuestas por los equipos Red Team y Blue Team

Vulnerabilidad	Ataques asociados	Medidas de mitigación (Red Team)	Medidas de mitigación (Blue Team)
Fallas en la configuración de sistemas	Acceso no autorizado	Pruebas de penetración para detectar configuraciones inseguras	Modificación de configuraciones, auditorías regulares
	Explotación de vulnerabilidades	Simulaciones de ataques para evidenciar fallos	Desactivación de servicios no esenciales
Software desactualizado	Malware	Simulación de ataques utilizando exploits conocidos	Gestión de actualizaciones y parches
	Ransomware	Demostración de riesgos de no actualizar	Pruebas de compatibilidad antes de actualizaciones
Errores humanos	Phishing	Simulacros de ingeniería social (campañas de phishing)	Programas de formación continua y políticas de seguridad
	Instalación de malware	Evaluación de susceptibilidad de empleados	Monitoreo de actividades atípicas
Acceso no autorizado	Hacking de contraseñas	Ensayos para detectar brechas en controles de acceso	Implementación de autenticación multifactor y segmentación
	Secuestro de sesiones	Simulaciones de movimientos laterales en la red	Políticas de privilegio mínimo
	Intercepción de datos	Simulaciones de ataques para evidenciar falta de cifrado	Implementación de cifrado en tránsito y reposo

Vulnerabilidad	Ataques asociados	Medidas de mitigación (Red Team)	Medidas de mitigación (Blue Team)
Falta de cifrado de datos	Robo de información	Demostración de cómo los datos no cifrados pueden ser robados	Gestión segura de claves criptográficas

Nota. Elaboracion propia.

Contención de Ataques Informáticos Blue Team

Ante un ataque en tiempo real, un integrante del equipo Blue Team seguiría los siguientes pasos:

Identificar y Contener el Ataque

- Comprobaría si el sistema está siendo explotado, para lo cual emplearía herramientas de código abierto, como Wireshark, para supervisar el tráfico en la red e identificar acciones sospechosas.
- Emplearía herramientas como Nmap para escanear el sistema y determinar qué puertos están abiertos y podrían estar siendo utilizados.
- En caso de confirmar la explotación, aislaría el sistema afectado de la red para contener el ataque y evitar su propagación.

Notificación del Incidente

- Informaría a los interesados acerca del incidente y las medidas que se están implementando para resolverlo.

Restaurar los Servicios

- Si el equipo afectado es un servidor, utilizaría copias de seguridad o imágenes del sistema para restaurarlo lo antes posible, mientras lo reviso.

Análisis Forense del Sistema

- Realizaría un análisis forense del sistema perjudicado empleando herramientas de código abierto como Autopsy o CAINE, para recolectar evidencia y comprender la magnitud del ataque.
- Analizaría los archivos del sistema (Event Viewer), los procesos en marcha (Process Explorer), las conexiones de red (netstat), que me permitan descubrir la actividad dañina.
- Investigaría la existencia de archivos, procesos o conexiones inusuales que podrían tener vínculos con las vulnerabilidades identificadas con Nmap.

Identificar y Clasificar Indicadores de Compromiso (IoCs)

- Identificar IPs que han sido reportadas como fuentes de ataques.
- Comparar los hashes de archivos en el sistema con bases de datos de malware conocidos.
- Registrar URLs que han sido utilizadas en ataques previos.
- Identificar archivos con nombres inusuales o que no deberían estar en el sistema.
- Comportamiento inusual en cuentas con privilegios administrativos.
- Intentos de acceso no autorizados o sospechosos.
- Consultas de DNS o HTTPS hacia dominios no reconocidos.

- Transferencias significativas de datos fuera de la red.

Aplicación de Parches y Mitigación

- Aplicaría actualizaciones o parches de seguridad relacionados con la vulnerabilidad identificada en el sistema perjudicado.
- Revisaría la configuración del firewall y otros controles de seguridad del sistema, para asegurar que esté debidamente protegido contra futuros ataques.
- Removería el malware o software malicioso de los sistemas afectados.

Análisis y Generación de Informes

- En un informe, registraría minuciosamente todo el proceso de investigación y contención del ataque, incluyendo los descubrimientos, las medidas adoptadas y sugerencias para mejorar la posición de seguridad.

Beneficios que Obtienen las Organizaciones al Adoptar Equipos de Seguridad Red Team y Blue Team en sus Estrategias de Seguridad Informática

La adopción de equipos de seguridad Red Team y Blue Team en las organizaciones representa una estrategia avanzada y proactiva para enfrentar los desafíos de la ciberseguridad. En un entorno digital que se vuelve progresivamente más complicado y lleno de amenazas, especialmente en países como Colombia, donde los ataques cibernéticos han aumentado significativamente en los últimos años, contar con estos equipos especializados no solo mejora la defensa de los sistemas, sino que también fortalece la confianza de los clientes, empleados y socios comerciales. A continuación, se analizan los beneficios más destacados de esta práctica.

Detección Temprana de Vulnerabilidades

Una de las mayores ventajas de integrarse con los equipos Red Team y Blue Team es la habilidad para detectar vulnerabilidades antes de que los atacantes reales las exploten. Al simular ataques reales, el Red Team facilita a las organizaciones la comprensión de cómo los ciberdelincuentes podrían poner en riesgo sus sistemas, procedimientos y datos. Estas simulaciones evidencian aspectos débiles que podrían pasar inadvertidos en las auditorías convencionales. Por ejemplo, en Colombia, situaciones como los ataques de phishing destinados a organismos gubernamentales como la DIAN han evidenciado que las entidades deben estar listas para identificar y atenuar amenazas sofisticadas. Mediante la labor del Red Team, las compañías pueden prever los peligros y robustecer sus defensas.

Fortalecimiento de la Defensa Activa

El Blue Team desempeña un rol esencial en la puesta en marcha de estrategias defensivas. Estos equipos no solo se encargan de las amenazas identificadas por el Red Team, sino que también se esfuerzan en la mejora de los sistemas de vigilancia, la configuración de herramientas de seguridad y la formación del personal. En Colombia, donde empresas de todas las dimensiones han sufrido ataques de ransomware y malware, el Blue Team garantiza que las organizaciones estén listas para reaccionar con prontitud y reducir el efecto de un ataque. Adicionalmente, su énfasis en la protección activa contribuye a fomentar una cultura de prevención.

Mejora en la Capacitación del Personal

Uno de los beneficios más significativos de disponer de equipos Red Team y Blue Team es el efecto beneficioso en la formación de los trabajadores. Los ataques simulados del Red Team brindan a los empleados la oportunidad de vivir situaciones de riesgo reales, mientras que el Blue Team los orienta sobre cómo reaccionar de forma eficaz. En Colombia, donde los ataques de ingeniería social y phishing son particularmente habituales, es crucial formar a los trabajadores para que detecten y prevengan estas amenazas. Esta perspectiva no solo disminuye la posibilidad de un ataque tener éxito, sino que también capacita al personal para transformarse en una primera línea de defensa frente a los ciberdelincuentes.

Optimización de Procesos y Tecnologías

La cooperación entre el Red Team y el Blue Team posibilita que las empresas mejoren sus procesos internos y tecnologías de seguridad. Los ataques simulados muestran aspectos que pueden optimizarse en los sistemas, tales como configuraciones de red, políticas de contraseñas y

protocolos de autenticación. En Colombia, donde aplicaciones web mal configuradas han sufrido ataques de inyección SQL y secuestro de sesiones, esta optimización es particularmente significativa. Adicionalmente, el Equipo Azul se esfuerza en la implementación de soluciones avanzadas como cortafuegos de aplicaciones web (WAF), autenticación multifactor (MFA) y sistemas de detección de intrusiones (IDS/IPS), garantizando que las tecnologías sean sólidas y eficaces.

Reducción de Costos a Largo Plazo

A pesar de que la puesta en marcha de los equipos Red Team y Blue Team puede parecer una inversión considerable, las ventajas financieras a largo plazo son claras. Identificar y mitigar vulnerabilidades antes de que sean aprovechadas disminuye los gastos relacionados con la recuperación de datos, el pago de rescates por ransomware y la disminución de la imagen. En Colombia, donde los ataques DDoS y de ransomware han detenido las actividades de empresas e instituciones del gobierno, tener una estrategia robusta de seguridad informática puede ser la diferencia entre una interrupción momentánea y un perjuicio irreversible. Además, las entidades que muestran un compromiso con la ciberseguridad tienen más oportunidades de captar clientes y aliados comerciales que aprecien la salvaguarda de sus datos.

Fortalecimiento de la Confianza y Reputación

En un mundo en el que los sucesos de seguridad pueden perjudicar seriamente la reputación de una entidad, tener equipos Red Team y Blue Team refleja un compromiso firme con la salvaguarda de la información y la privacidad. Las compañías que implementan estas tácticas transmiten un mensaje claro a sus clientes y asociados: están listos para lidiar con amenazas y

salvaguardar sus intereses. En Colombia, donde entidades bancarias y empresas del sector financiero han sufrido ataques de suplantación de identidad y spoofing, la confianza es un recurso inestimable. Al evidenciar la adopción de acciones proactivas para asegurar la seguridad, las entidades pueden destacarse en un mercado competitivo.

Preparación Frente a Amenazas Emergentes

Las técnicas de ciberataque recientes y los ataques Zero-Day exigen una preparación continua. Los equipos Red Team y Blue Team colaboran para estar actualizados con las tendencias más recientes en ciberseguridad, garantizando que las organizaciones estén listas para lidiar con amenazas en ascenso. En Colombia, donde la evolución de los ataques sofisticados ha sido acelerada, esta habilidad para adaptarse es crucial. Además, la cooperación entre estos grupos posibilita que las organizaciones elaboren planes de respuesta a incidentes particulares para cada clase de ataques, desde ransomware hasta ataques MitM, asegurando una respuesta rápida y eficaz.

Estudio del Caso IFX

En 2023, IFX Networks, una empresa que desempeña un papel crucial al gestionar la conectividad y los servicios en la nube para más de 4.200 empresas en América Latina, se vio envuelta en una pesadilla cibernética. Un grupo de atacantes conocido como RansomHouse logró infiltrarse en su infraestructura, encriptando datos vitales y bloqueando el acceso a sus sistemas. Este ataque no fue solo un golpe a IFX, sino que tuvo repercusiones devastadoras para numerosas entidades en Colombia. Instituciones gubernamentales como la Superintendencia de Industria y Comercio, la Superintendencia de Salud, el Ministerio de Salud y Protección Social, y el Consejo

Superior de la Judicatura se encontraron paralizadas, obligadas a regresar a métodos manuales para operar y, en algunos casos, a suspender servicios esenciales.

La magnitud del impacto fue alarmante. Los ciudadanos que dependían de estos servicios se vieron afectados en su vida diaria, desde la atención médica hasta la administración de justicia. La frustración y la incertidumbre se apoderaron de aquellos que necesitaban asistencia y no podían acceder a la información crítica que antes tenían al alcance de su mano.

Los informes revelaron que los atacantes ingresaron mucho antes de ejecutar el ataque, y tuvieron la oportunidad de planificarlo, además IFX incurrió en varios errores graves que facilitaron este ataque. Uno de los puntos vulnerables fue un producto de VMware, utilizado para crear y operar servidores virtuales, que había quedado sin actualizar. Esta negligencia permitió que los atacantes ingresaran sin dificultad a la red. Además, aunque IFX contaba con sistemas de respaldo, los tenían alojados en el mismo entorno tecnológico que fue atacado, lo que significó que no ofrecieron una respuesta oportuna ante la incidencia.

Cómo la Implementación de Equipos Red Team y Blue Team Podría Haber Beneficiado a IFX

La ciberseguridad se ha vuelto un pilar esencial para las organizaciones en la era digital, especialmente después de incidentes como el que sufrió IFX Networks en 2023. La creación de equipos Red Team y Blue Team podría haber sido determinante para identificar y mitigar vulnerabilidades antes de que fueran aprovechadas. Gracias al enfoque proactivo y colaborativo de estos equipos especializados, IFX podría haber disminuido considerablemente los riesgos asociados a su infraestructura tecnológica, evitando así el devastador impacto del ciberataque. A continuación, se exponen algunos de los beneficios que la puesta en marcha de estos equipos de seguridad especializados habría proporcionado a IFX:

Detección Temprana de Vulnerabilidades. Previo al ataque, IFX no había actualizado su software de virtualización (VMware), lo que facilitó a los atacantes el acceso a su red. La puesta en marcha de un Red Team podría haber detectado esta vulnerabilidad de manera oportuna, previniendo el ataque. Las simulaciones de incidentes habrían subrayado la importancia de mantener todos los sistemas al día.

Fortalecimiento de la Defensa Activa. IFX podría haber obtenido un gran beneficio de un Blue Team que pusiera en marcha tácticas defensivas sólidas. La ausencia de preparación y reacción inmediata ante la amenaza facilitó que los atacantes se mantuvieran en la red durante meses. Un equipo comprometido podría haber optimizado la identificación de intrusiones y la reacción frente a incidentes, reduciendo así el perjuicio.

Mejora en la Capacitación del Personal. La experiencia del Red Team en simulacros de ciberataques podría haber preparado mejor a los trabajadores de IFX para identificar y reaccionar correctamente ante circunstancias de riesgo.

Optimización de Procesos y Tecnologías. IFX disponía de sistemas de backup, aunque estos se encontraban ubicados en la misma infraestructura en peligro. La cooperación entre Red Team y Blue Team podría haber resultado en un análisis riguroso de la estrategia de respaldo, garantizando que las copias de seguridad se encuentren en ambientes seguros y aislados.

Reducción de Costos a Largo Plazo. El precio por el rescate de los activos tecnológicos requerido por los ciberdelincuentes era bastante elevado. La inversión en los equipos de Red Team y Blue Team podría haber evitado este chantaje, al evitar primero el ataque, así como los gastos relacionados con la recuperación de datos y la disminución de la reputación con la que contaba este proveedor.

Fortalecimiento de la Confianza y Reputación. La crisis ha generado desconfianza entre los clientes de IFX debido a la ausencia de comunicación y transparencia. Un enfoque proactivo en ciberseguridad, respaldado por dispositivos especializados, podría haber evidenciado a los clientes la dedicación de la compañía a salvaguardar sus datos.

Preparación Frente a Amenazas Emergentes. Los equipos Red Team y Blue Team resultan esenciales para estar actualizados con las tendencias en ciberseguridad. La habilidad de IFX para ajustarse a amenazas emergentes, tales como el ransomware, habría experimentado un notable avance con el respaldo de estos equipos.

Conclusiones

La legislación en Colombia cuenta con normas que protegen tanto la información personal de los ciudadanos como la de las organizaciones. Estas regulaciones respaldan las prácticas de protección de la información, lo que refuerza la necesidad de implementar equipos de seguridad Red Team y Blue Team para cumplir con los estándares de seguridad vigentes.

La ética y la legalidad son pilares fundamentales en la práctica de la ciberseguridad. Los especialistas deben actuar con responsabilidad y compromiso, asegurando que sus acciones no solo cumplan con las normativas, sino que también contribuyan al bienestar de la sociedad. Trabajar en entornos que valoren la ética y la legalidad Resulta fundamental para conservar la confianza de los clientes y salvaguardar la integridad profesional.

Los equipos Red Team y Blue Team son necesarios para garantizar el correcto funcionamiento de los controles de seguridad dentro de las organizaciones. Gracias a su labor, se pueden ejecutar medidas de protección y realizar simulaciones prácticas para identificar vulnerabilidades y corregir fallos en los sistemas de seguridad.

Asimismo las herramientas de pentesting son esenciales para que los equipos especializados comprendan las tácticas que utilizan los ciberdelincuentes para infiltrarse en las redes. El trabajo de estos equipos, junto con el uso de estas herramientas, permite fortalecer las defensas y proteger los activos tecnológicos de las organizaciones.

Es fundamental que los entrenamientos de Red Team y Blue Team se institucionalicen como una práctica constante en entidades públicas y privadas. En un mundo cada vez más interconectado y susceptible a ciberataques, estas estrategias colaborativas no solo facilitan la detección y mitigación de vulnerabilidades, sino que también promueven una cultura de seguridad

proactiva y resiliente. Al simular ataques y robustecer las defensas, las entidades pueden adaptarse a las amenazas en constante cambio y proteger de manera más efectiva sus activos tecnológicos.

Recomendaciones

Se recomienda que las entidades públicas y privadas integren entrenamientos de Red Team y Blue Team como una práctica constante para adaptarse a las amenazas cibernéticas.

Es muy importante que la ciberseguridad sea una prioridad, con el respaldo de estos equipos especializados se pueden corregir debilidades en la infraestructura antes de que un atacante las aproveche.

Tener equipos de Red Team y Blue Team permite revisar constantemente la seguridad de la organización, asegurando que siempre estén un paso adelante de las amenazas en constante cambio.

Adoptar estrategias de seguridad, como formar estos equipos, no solo debe verse como un gasto en tecnología, sino como una inversión clave para que la organización sea más fuerte y sostenible en el futuro.

La colaboración entre estos dos equipos ayuda a estar mejor preparados para cualquier incidente, lo que reduce el tiempo que la organización está inactiva y el impacto de un posible ataque.

Integrar estos equipos promueve un ambiente de trabajo donde todos colaboran en la seguridad, haciendo que sea un esfuerzo conjunto entre diferentes áreas de la organización.

Implementar equipos de Red Team y Blue Team también ayuda a las organizaciones a cumplir con las regulaciones de seguridad y estándares del sector, lo cual es vital para ganar la confianza de los clientes y mantener una buena reputación.

Referencias

AMBIT-BST. (2020, noviembre 10). Tipos de vulnerabilidades y amenazas informáticas. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-informáticas

Anderson, H., Holdsworth, K., & Kosinski, J. (2024). Red Teaming: ¿Qué es y cómo funciona?. https://www.ibm.com/es-es/think/topics/red-teaming

Arroba System. (2021, febrero 4). ¿Qué son las amenazas informáticas y cómo protegerte de ellas?. https://arrobasystem.com/blogs/blog/que-son-las-amenazas-informaticas-y-como-protegerte-de-ellas

Bardaji, E. (s.f.). Red team vs blue team: simulaciones de ciberataques para fortalecer la seguridad empresarial. ESEDsl. https://www.esedsl.com/blog/red-team-vs-blue-team-simulaciones-de-ciberataques-para-fortalecer-la-seguridad-empresarial

Bodnar, D. (2020, octubre 29). Ingeniería social y cómo protegerse. https://www.avast.com/es-es/c-social-engineering

Botero, M. (2023). Ciberataque a IFX Networks en Colombia. Universidad Javeriana. https://www.javeriana.edu.co/pesquisa/ciberataque-ifx-networks-colombia/

Chacín, J. (s.f.). Principales vectores de ataque. https://neverofftechnology.com/blog/principales-vectores-de-ataque

Chirou, Á. (2023, mayo 24). Ciberseguridad y Red Team Hacking: 43 herramientas imprescindibles. https://achirou.com/red-team-herramientas-gratuitas/

Cisco. (s.f.). ¿Qué es SIEM?. https://www.cisco.com/c/en/us/products/security/what-is-siem.html

Cilleruelo, C. (2024). ¿Qué es OSSEC?. KeepCoding. https://keepcoding.io/blog/que-es-ossec/

Cilleruelo, C. (2024). ¿Qué es pfSense?. KeepCoding. https://keepcoding.io/blog/que-es-pfsense/

Congreso de la República. (2008). Ley 1266 de 2008. https://www.redjurista.com/Documents/ley_1266_de_2008_congreso_de_la_republica.aspx

De Luz, S. (2023, abril 24). Veracrypt: Cifra y oculta tus archivos gratis. https://www.redeszone.net/tutoriales/seguridad/veracrypt-cifra-archivos-gratis/

División Computer Forensic. (s. f.). Delitos informáticos https://www.delitosinformaticos.info/delitos_informaticos

Díaz, M. R. O., & Rangel, P. E. S. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: Un análisis para Colombia. Revista Criminalidad, 62(2), 199–217.

Función Pública. (1999). Ley 527 de 1999. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

Función Pública. (2008). Ley 1266 de 2008. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Función Pública. (2009). Ley 1341 de 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913

Fortinet. (2023). Snort. https://www.fortinet.com/lat/resources/cyberglossary/snort

Garcia, J. (2023). Ciberataque en Colombia: detalles del ataque a IFX Networks. El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-detalles-del-ataque-a-ifx-networks-806778

Gómez, J. (2024). Herramientas de seguridad informática. DeltaProtect. https://www.deltaprotect.com/blog/herramientas-seguridad-informatica

Grabolosa, P. (2024). Wazuh: Una plataforma de código abierto que unifica SIEM y XDR. InLab. https://inlab.fib.upc.edu/es/articulos/wazuh-una-plataforma-de-codigo-abierto-que-unifica-siem-y-xdr/2024/

Guijarro, H. (2018, 22 de mayo). Qué es un test de penetración y para qué sirve. https://www.itgovernance.eu/blog/es/que-es-un-test-de-penetracion-y-para-que-sirve

IBM. (s. f.). NIST: Marco de ciberseguridad. https://www.ibm.com/mx-es/topics/nist

Infosecurity México. (2021). MITRE Shield y la defensa activa. https://www.infosecuritymexico.com/es/blog/mitre-shield-y-la-defensa-activa.html

Intelequia. (2021, enero 26). Red Team y Blue Team: Funciones y diferencias en ciberseguridad. https://intelequia.com/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

Jaimovich, D. (2022, noviembre 24). ¿Qué son los escenarios de red team? Metodología y ejemplos. https://blog.invgate.com/es/red-team

Jimenez, M. (2024). Posibles causas del ataque cibernético a IFX Networks. Pirani. https://www.piranirisk.com/es/blog/posibles-causas-ataque-cibernetico-ifx-networks

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 2023(E62), 16–31.

Kime, C. (2023). Cómo usar Nmap para el análisis de vulnerabilidades: Tutorial completo. eSecurity Planet. https://www.esecurityplanet.com/networks/nmap-vulnerability-scanning-made-easy/

Knechtel, J., Eslami, M., Zou, P., Sinanoglu, O., & Pagliarini, S. (2025). Trojan Insertion versus Layout Defenses for Modern ICs: Red-versus-Blue Teaming in a Competitive Community Effort. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(1), 37–77.

Maeng, Y., & Pihelgas, M. (2023). Request for a Surveillance Tower: Evasive Tactics in Cyber Defense Exercises. International Conference on Cyber Conflict, CYCON, 239–252.

ManageEngine. Controles de seguridad crítica CIS. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Martínez, J. J. C. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. Revista Científica General Jose Maria Cordova, 20(40), 815–832.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (1999). Ley 527 de 1999: Por la cual se establece el régimen de la firma electrónica y se dictan otras disposiciones. https://normograma.mintic.gov.co/mintic/compilacion/docs/ley_0527_1999.htm

Netskope. (s. f.). Cyber Security Kill Chain. https://www.netskope.com/es/security-defined/cyber-security-kill-chain

Nisha, P. (2021). Explotación de EternalBlue (MS17–010): Guía práctica y medidas de protección. https://eunishap.medium.com/exploiting-eternalblue-ms17-010-a-walkthrough-and-protection-measures-1ef4145f51ed

Ostec. (s. f.). Blue Team y Red Team, sepa cuáles son las diferencias. https://ostec.blog/es/aprendizaje-descubrimiento/blue-team-y-red-team-sepa-cuales-son-las-diferencias/

Prieto, D. (2024). Detección de virus y malware en Linux con ClamAV. STR Sistemas. https://www.strsistemas.com/blog/deteccion-de-virus-y-malware-en-linux-con-clamav

Rivas, A. (2025, 16 de marzo). Normas APA: La guía definitiva para presentar trabajos escritos. https://normasapa.in/

Rostick, P. (2018, 21 de febrero). Herramientas y principios para la seguridad de aplicaciones: ¿Qué funciona y qué no tanto?. https://www.b-secure.co/blog/herramientas-y-principios-para-la-seguridad-de-aplicaciones

Sánchez-García, I. D., Rea-Guamán, A. M., San Feliu, T., & Calvo-Manzano, J. A. (2024). Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 2024(E53), 69–87.

Saint Leo University. (2023, enero 23). ¿Cuál es la historia de la ciberseguridad?. https://worldcampus.saintleo.edu/noticias/historia-de-la-ciberseguridad

Shivanandhan, M. (2021). Cómo explotar la vulnerabilidad EternalBlue en Windows: guía paso a paso. FreeCodeCamp. https://www.freecodecamp.org/news/how-to-exploit-the-eternalblue-vulnerability-on-windows/

Tarlogic Security. (s. f.). Blue Team: Fortalecer la defensa de una compañía. https://www.tarlogic.com/es/blog/blue-team/

Tecnozero. (s. f.). Red Team en ciberseguridad: ¿Qué es y cómo funciona?. https://www.tecnozero.com/blog/red-team-en-ciberseguridad/

UNIR. (2020, enero 7). Red Team, Blue Team y Purple Team: Funciones y diferencias. https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

UNIR. (2023). Hardening: ¿qué es?. Universidad Internacional de La Rioja. Recuperado de https://www.unir.net/revista/ingenieria/hardening-que-es/

Vargas, N. (2023, enero 25). Las empresas que han sido blanco de ciberataques en Colombia en el último año. https://www.larepublica.co/empresas/las-empresas-que-han-sido-blanco-de-ciberataques-en-colombia-en-el-ultimo-ano-3529667

Wallarm. (2025, marzo 30). ¿Qué es el marco MITRE ATT&CK? 14 tácticas básicas. https://lab.wallarm.com/what/que-es-el-marco-mitre-attck-14-tacticas-basicas/?lang=es

Apendices

Apendice A Enlace sustentación

https://youtu.be/P2kgJBLiVnM