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

José Leonidas Quiroga Moya

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

Entendiendo en primer lugar, que existe para Colombia un marco legislativo actualizado y armonizado con la evolución global en los asuntos de la ciberseguridad, resulta pertinente complementar con el estudio de las capacidades de los equipos Red Team y Blue Team y las herramientas que apoyan sus actividades.

Con el desarrollo de este documento se ofrece un acercamiento a las principales leyes que ha promulgado el gobierno colombiano en lo que concierne a la ciberseguridad, solucionando frente a ellas, algunos cuestionamientos éticos basados en un caso hipotético. Posteriormente se realiza una exploración de las etapas que se deben seguir para efectuar un pentesting, llegando a la ejecución efectiva de una intrusión en un escenario controlado, reconociendo las capacidades para los equipos Red Team, de herramientas como NMAP y METASPLOIT. Finalmente se plantean algunas posturas de contención y hardenización para el escenario configurado analizando el aporte que los SIEM puede dar a los equipos Blue Team y evaluando el valor que se puede obtener para estos equipos, de la implementación de algunos controles CIS.

***Palabras clave*:** Ciberseguridad, blue Team, gobernanza, hardenización, pentesting, red team

Abstract

Understanding first of all that Colombia has an updated legislative framework that is harmonized with the global evolution in cybersecurity matters, it is pertinent to complement it with a study of the capabilities of the Red Team and Blue Team and the tools that support their activities.

The development of this document offers an approach to the main laws enacted by the Colombian government regarding cybersecurity, solving some ethical questions based on a hypothetical case. Subsequently, an exploration of the stages that must be followed to perform a pentesting, reaching the effective execution of an intrusion in a controlled scenario, recognizing the capabilities of tools such as NMAP and METASPLOIT for Red Team teams. Finally, some containment and hardening positions are proposed for the configured scenario, analyzing the contribution that SIEMs can give to Blue Teams and evaluating the value that can be obtained for these teams from the implementation of some CIS controls.

Keywords**:** Ciberseguridad, blue Team, gobernanza, hardenización, pentesting, red team.

Contenido

Lista de Figuras

Introducción

El entendimiento del marco regulatorio y legislativo colombiano acerca de la ciberseguridad y la apropiación de directrices para el ejercicio profesional deben ser guías prevalentes para los que nos dedicamos a las actividades que propenden por la seguridad de la información y la ciberseguridad, entendiendo que hay bases éticas y límites formales que regulan el adecuado proceder para el ejercicio de actividades como el hacking ético y en general las responsabilidades sobre el gobierno de la información, la información de datos personales o cualquier contacto con información que a todas luces puede ser sensible o de valor para los demás.

Las actividades realizadas por los equipos Red Team y Blue Team, en conjunto configuran una posición preventiva y proactiva frente a cualquier ataque cibernético debido a que ofrecen la ventaja de descubrir brechas de seguridad de forma temprana y actuar sobre ellas, con el debido cuidado de haber seguido una metodología rigurosa en la que se ha mantenido el cuidado de documentar experiencias.

Resulta valioso y enriquecedor mantener escenarios de simulación para ejecutar pruebas que promuevan el fortalecimiento de las capacidades técnicas de los profesionales de los equipos Red Team y Blue Team, aunado a la curiosidad e investigación constante frente a la par con la evolución de las nuevas y sofisticadas metodologías que los ciberdelincuentes modernos están implementando con apoyo de la inteligencia artificial. Por esta razón, también se debe señalar la relevancia del uso de herramientas que apliquen machine learning e inteligencia artificial como efectivamente ya se puede comprobar con las marcas que lideran el mercado de la ciberseguridad.

Justificación

El reconocimiento de los planteamientos y posturas del gobierno colombiano desde lo legislativo, en cuanto a la protección de datos personales y ciberseguridad, nos entrega un contexto cercano y realista de las capacidades tecnológicas que eventualmente nos pueden servir en lo que concierne a la atención de incidentes de seguridad de la información y las rutas que se pueden seguir en lo planes de continuidad de las operaciones cuando se define la matriz de comunicaciones.

Resulta relevante identificar las diferentes etapas de un pentesting para llevar a cabo un ejercicio formal y efectivo desde el actuar de los equipos Red Team, de manera que se consigan los objetivos de intrusión sin poder la oportunidad en la medida en que se avanza desde el reconocimiento del objetivo hasta la elaboración de los informes técnicos. Todo lo anterior apoyado en las diferentes herramientas de pago y de open source que facilitan el alcance y análisis de las vulnerabilidades de los sistemas que se proponen como objetivo de las pruebas.

Es importante entender la relación que tienen las actividades efectuadas por lo equipos Red Team frente a las que corresponden a lo equipos Blue Team, en cuanto a que los primeros se encargan de hallar las vulnerabilidades sobre los sistemas mientras que los segundos, a partir de los informes recibidos, se encargan de aplicar las configuraciones, remediaciones, implementación de herramientas y otras salvaguardas para proteger efectivamente los activos de información.

La realización de laboratorios en escenarios simulados fortalece el conocimiento y la confianza para proponer actividades similares en los escenarios reales, dentro de las compañías para las que trabajamos los profesionales ciberseguridad, además de que ofrecen un espacio para

realizar investigación y prolongación hacia la evolución retadora que nos proponen los actores maliciosos.

Objetivos

Objetivo General

Elaborar un informe técnico en el que se presenten los aspectos destacables del desarrollo las actividades planteadas en las etapas anteriores del seminario, que fueron solucionadas desde la perspectiva de los ejercicios de intrusión de los equipos Red Team y las actividades de contención de los equipos Blue Team, en el marco de criterios éticos y legales.

Objetivos Específicos

Redactar un resumen con respecto a las leyes colombianas en relación a los delitos informáticos y la protección de datos personales.

Definir cada etapa del pentesting describiendo algunas herramientas utilizadas en el proceso.

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Plantear estrategias para la contención, luego del análisis de los riesgos y vulnerabilidades en una infraestructura de TI.

Informe técnico acerca de las actividades planteadas en relación con los equipos Red Team y Blue Team.

Legislación y decretos identificados para Colombia, sobre delitos informáticos y protección de datos personales.

En Colombia, actualmente existen avances importantes en cuanto a la normativa relacionada con ciberseguridad y protección de datos personales, resultando muy completa en su alcance y alineada con los avances globales. Para este caso haré referencia algunas de las normas más reconocidas, en particular la que tiene que ver con la protección de datos personales.

Decreto 338 de 2022

Como es descrito en Función Pública (2022), este decreto establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital la identificación de infraestructuras críticas cibernéticas, la gestión del riesgo y la respuesta a incidentes de ciberseguridad.

El decreto 338 de 2022 pretende materializar los esfuerzos con respecto a la implementación de la política pública de ciberseguridad, formalizando los roles y responsabilidades de quienes trabajan directamente con este esquema y que además abren espacios de cooperación ente diferentes actores para fortalecer capacidades operativas.

De forma especial el decreto 338 promueve espacios para tomar conciencia frente a la responsabilidad que tenemos frente a la gestión de los riesgos resaltando la capacidad que debe tener el gobierno para enfrentar los nuevos retos que presenta el mundo digital.

En términos generales el decreto quiere asegurar que Colombia continúe fortaleciendo su confianza y mejorando en ciberseguridad para dar mayor valor socioeconómico en el ciberespacio.

Ley 1273 de 2009

La Función Pública (2009) indica que esta ley modifica el código penal, creando un nuevo bien jurídico tutelado llamado "De la protección de la información y de los datos "y se preservan completamente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

La ley 1273 en su capítulo 1 considera los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, enunciando los siguientes artículos:

- Artículo 269A: Acceso abusivo a un sistema informático: El que acceda sin autorización o permanezca dentro de sistemas protegidos con alguna medida de seguridad, incurrirá en pena de prisión entre 48 y 96 meses y multa de 100 a mil SMV.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: El que obstaculice o impida el acceso a un sistema informático, incurrirá en pena de prisión entre 48 y 96 meses y multa de 100 a mil SMV.
- Artículo 269C: Interceptación de datos informáticos: El que intercepte dados informáticos en su origen incurrirá en pena de prisión 36 a 72 meses.
- Artículo 269D: Daño Informático: El que dañe, destruya, altere, o suprima datos informáticos, , incurrirá en pena de prisión entre 48 y 96 meses y multa de 100 a mil SMV.
- Artículo 269E: Uso de software malicioso: El que produzca, transfiera, adquiera, distribuya, envíe, introduzca o extraiga software malicioso del territorio nacional o

cualquier programa de efectos dañinos, incurrirá en pena de prisión entre 48 y 96 meses y multa de 100 a mil SMV.

- Artículo 269F: Violación de datos personales: el que para provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión entre 48 y 96 meses y multa de 100 a mil SMV.
- Artículo 269G: Suplantación de sitios web para capturar datos personales: El que con propósitos ilícitos diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos.
    - Artículo 269H: Circunstancias de agravación punitiva: Las penas mencionadas aumentarán si las conductas se cometieren: Sobre redes sistemas oficiales, bancarios, por servidor público, aprovechando la confianza dentro del vínculo laboral, revelando el contenido en perjuicio de otro, obteniendo provecho para sí o terceros con fines terroristas, utilizando como instrumento a un tercero de buena fe.

Ley 1928 de 2018.

Mintic (2018) expone que mediante esta ley se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001 en Budapest.

Mediante esta ley Colombia ratifica el convenio sobre ciberdelincuencia, conocido como convenio de Budapest que fue creado y aceptado pen 2001 por el concejo de Europa. Este tratado

busca generar normas y mecanismos para luchar contra la ciberdelincuencia promoviendo la cooperación entre los países firmantes.

La ley 1928 de 2018 en Colombia ratifica este convenio con el fin de establecer los marcos legales para combatir los delitos asociados con el uso de las tecnologías de la información. Esto incluye el acceso ilegal a sistemas de información, el fraude, contenidos inapropiados, pornografía infantil, entre otros.

La ley 1928 facilita la cooperación ente los firmantes en el convenio de Budapest, permitiendo el intercambio y la cooperación, facilitando el combate contra la ciberdelincuencia.

Resolución 02239 de 2024.

Esta resolución actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución448 de 2022.

La resolución 02239 de 2024 tiene como objeto actualizar la política General de Seguridad y Privacidad de la Información y la Comunicaciones, así como definir lineamientos sobre el uso y manejo de información.

En cuanto a su ámbito de aplicación aplica a todos los niveles funcionales y organizacionales del Ministerio/Fondo Único de TIC, a todos sus funcionarios y partes interesadas que en cumplimiento de sus funciones utilicen o procesen información cualquier activo de información del ministerio.

La política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación tiene los siguientes objetivos:

- Definir y formular asuntos normativos sobre temas de protección de la información.
- Facilitar la gestión de riesgos y la continuidad de la operación
- Mitigar el impacto de los incidentes de seguridad.
- Establecer los mecanismos para el aseguramiento digital y físico.
- Definir los lineamientos para el manejo de la información en cualquiera de sus estados.
- Generar cambio mediante la concienciación y apropiación de la seguridad.
- Dar cumplimiento a los requisitos legales.
- Definir, operar y mantener del plan de continuidad de la operación.

Ley 1581 de 2012.

De la Función Pública (2012) se interpreta que mediante esta ley, se dictan las disposiciones generales para la protección de los datos personales.

Esta ley busca garantizar el derecho de las personas a tener control sobre su información personal. La ley 1581, establece el marco legal colombiano para asegurar la privacidad de la información, promoviendo la confianza y seguridad durante el tratamiento de a la información de datos personales por parte de terceros.

La ley aplica para para la personas y entidades que manejen datos de información personal, bajo los principios de transparencia, legalidad, finalidad, veracidad y circulación restringida y confidencialidad.

En el título III de la ley quedan definidas las categorías especiales de los datos como datos sensibles, es decir los que afectan la intimidad del titular o cuyo uso puede generar discriminación.

El título III de la ley indica que se prohíbe el tratamiento de datos personales excepto cuando el titular haya dado la autorización, el tratamiento sea necesario para salvaguardar el interés vital del titular, los datos sean necesarios para la defensa o reconocimiento de un derecho y finalmente para alguna finalidad histórica o estadística.

El artículo 7 del título 3 señala de especial interés el aseguramiento de los derechos de los niños, niñas y adolescentes en lo que concierne a su información personal.

De forma general se reconoce que los titulares de los datos personales tienen derecho a conocer, actualizar, rectificar y suprimir sus datos pudiendo revocar, incluso, el consentimiento otorgado para su tratamiento.

El ente encargado de vigiar el cumplimiento de la ley 1582 de 2012 es la Superintendencia de Industria y Comercio.

Defínción de cada una de las etapas del pentesting, incluyendo un ejemplo de una herramienta usada en cada etapa.

El pentest es un método seguro para evaluar la seguridad de una red o aplicación mediante la identificación y explotación segura de vulnerabilidades.

Además de identificar y explotar vulnerabilidades también sirven para probar los métodos defensivos existentes y las estrategias de seguridad.

Las pruebas de penetración consisten en 6 fases así:

Fase 1: Planificación y recolección de información (Reconocimiento).

En esta se revisa la logística ya las reglas para realizar las pruebas, se revisan las implicaciones legales y las posibles afectaciones.

En este punto se deben definir los objetivos de la prueba, determinar el alcance y analizar las implicaciones, recolectando información previa sobre el objetivo, identificando alguna superficie de ataque.

Hay 2 tipos de reconocimiento:

Reconocimiento activo: El pentester interactúa directamente con el sistema objetivo.

Reconocimiento pasivo: En este caso el pentester no interactúa con el sistema.

Ejemplo de una herramienta que se pueden usar en esta etapa:

Nmap: Es una herramienta de código abierto, basada en Linux, que sirve para escanear direcciones IP y puertos abiertos en una red, para identificar aplicaciones instaladas, servicios abiertos y detectar vulnerabilidades.

Fase 2: Escaneo y enumeración (Descubrimiento).

Se puede realizar en 2 partes:

1. Recopilación de información adicional: Los pentester obtienen más información sobre la red objetivo mediante técnicas como interrogación DNS, rastro de red para descubrir nombres de host e IP´s
2. Escaneo de vulnerabilidades: Los pentester analizan la aplicación o el sistema operativo en búsqueda de vulnerabilidades conocidas. Pueden realizar un análisis automático que compara contra bases de datos de vulnerabilidades.

El objetivo en esta etapa es identificar vulnerabilidades específicas, enumerar servicios y versiones y obtener información de configuraciones y sistemas operativos.

- **Ejemplo de una herramienta que se pueden usar en esta etapa:**

Nessus: Es una herramienta de escaneo de vulnerabilidades que ayuda a identificar y gestionar riesgos de seguridad en redes, sistemas operativos y aplicaciones.

Fase3: Explotación.

En esta fase se busca establecer acceso a un sistema mediante un ataque simulado usando las vulnerabilidades observadas en la fase anterior, En este punto el atacante debe ser cauteloso de no afectar los servicios o producir daños en el flujo de trabajo.

El pentester debe confirmar la existencia de la vulnerabilidad mediante las pruebas reales.

- **Ejemplo de una herramienta que se pueden usar en esta etapa:**

Metasploit: Es un framework de código abierto usado para realizar pruebas de penetración, desarrollar y ejecutar exploits. Metasploit cuunata con una base amplia de exploits, actualizada que permite ejecutar métodos recientes.

Fase 4: Escalada de privilegios.

El pentester intentará obtener acceso con usuarios administradores o root, para hacerse con el control de los sistemas

- **Ejemplo de una herramienta que se pueden usar en esta etapa:**

Mimikatz: Herramienta de Windows utilizada para extraer credenciales almacenadas y realizar ataques de escalada de privilegios en sistemas Windows.

Fase 5: Post Explotación.

Una vez que el pentester ha explotado una vulnerabilidad e identificado alguna falla del sistema y punto de entrada, se debe valorar ese punto analizando:

¿Cuánto acceso permite ese punto de entrada?

¿Qué tan fácil es mantener el punto de acceso?

¿Cuánto tiempo puede pasar hasta que se detecte la brecha?

¿Cuál es el grado de daño que puede causar la vulnerabilidad?

En esta fase es de gran importancia mantener la persistencia, es decir mantener el acceso al sistema.

- **Ejemplo de una herramienta que se pueden usar en esta etapa:**

Netcat: Herramienta de red utilizada para establecer conexiones de red bidireccionales y mantener acceso remoto a través de puertas traseras.

Fase 6: Reportes, informes y recomendaciones.

Todos los pasos de las fases anteriores deben estar bien documentadas, debido a que aportaran la información que ayudará a construir los informes para los interesados.

Los informes deben presentar:

- Descripción de las vulnerabilidades.
- Informe detallado de los hallazgos
- Calificaciones según el sistema CVSS.
- Gravedad e impacto de las vulnerabilidades.
- Informe de evaluación de riesgos.

- Recomendaciones para mitigar los riesgos.

- **Ejemplo de una herramienta que se pueden usar en esta etapa:**

Faraday: Plataforma de pruebas de penetración que facilita la gestión de hallazgos y la elaboración de informes.

Definición y explicación de herramientas que pueden ser usados por equipos Red Team y Blue team:

- **Metasploit:**

Como lo explican en Keep Coding (2024), se trata de un framework de código abierto, mudular y flexible, utilizado para realizar pruebas de penetración, especialmente dentro del sistema operativo Kali Linux. Metasploit cuenta con más de 900 exploits que son cruciales para poner a prueba las vulnerabilidades de propios de muchos sistemas.

Algunos usos de Metasploit: Escanear y recopilar información, identificar y explorar vulnerabilidades, escalada de privilegios, instalar backdoors, hacer Fuzzing, evasión de antivirus.

- **Nmap:**

Nmap es una herramienta de código abierto, gratuita, para la exploración de redes y auditorías de seguridad. Fue diseñado para escanear rápidamente grandes redes, aunque funciona bien con host individuales. Nmap usa paquetes IP para determinar que host están disponibles en la red, qué servicios ofrecen los hosts, (nombre y versión de la aplicación), qué sistema operativo y su versión que filtros están en el firewall.

- **Open Vas**

Welivesecurity (2025) ofrece una descripción en la que señala que se trata de un framework con base en servicios y herramientas que pueden estar de forma individual o como parte de herramientas OSSIM.

Algunas distribuciones de Kali Linux ya la incluyen y se puede usar desde Metasploit.

Open Vas es un escáner de vulnerabilidades que incluye funciones de pruebas autenticadas y no autenticadas, varios protocolos industriales y de internet, optimización de rendimiento para análisis a gran escala e incluye un lenguaje de programación interno para implementar cualquier tipo de pruebas,

Open Vas ofrece, entre otras, las siguientes opciones:

- Scans: La gestión del escáner permite crear nuevas tareas de exploración, modificar aquellas que se hayan creado previamente,
- Assets: Gestión de activos se enlistan los hosts que han sido analizados junto con el número de vulnerabilidades identificadas.
- Configuration: Permite configurar los objetivos, asignar credenciales de acceso para revisiones de seguridad locales, programar escaneos, generar informes, etc.
- Administration: Gestiona usuarios del escáner, la configuración para la sincronización de NVT Feed y muestra las opciones de configuración de la herramienta.

- **Exploit DB:**

Exploit DB es una plataforma que contiene una base de datos pública en línea para entregar información sobre vulnerabilidades de seguridad, exploits y su correspondiente prueba de concepto.

- **CVE:**

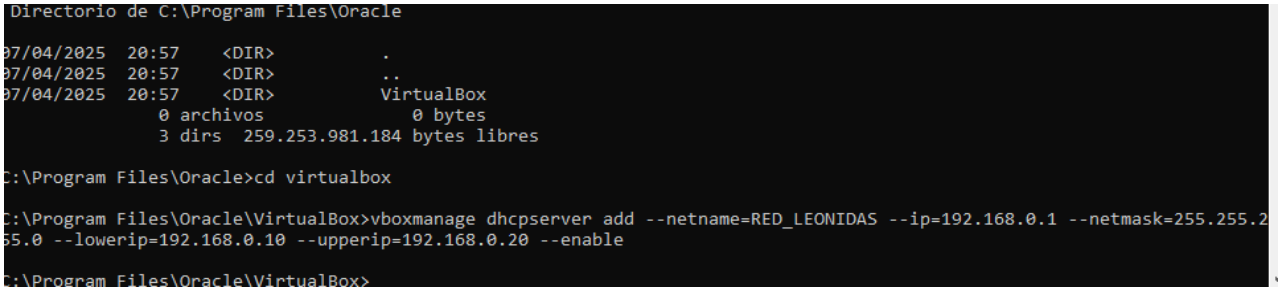
Las vulnerabilidades y exposiciones comunes (CVE) son un conjunto de amenazas de seguridad que se incluyen en un sistema de referencia que describe los riesgos conocidos públicamente. MITRE Corporation, una organización sin fines de lucro que dirige centros federales de investigación y desarrollo patrocinados por el gobierno mantiene la lista de amenazas de CVE. El CVE está patrocinado por la División Nacional de Ciberseguridad (NCSD) del Departamento de Seguridad Nacional de EE. UU.

CVE define las vulnerabilidades que permiten a los atacantes tener acceso no autorizados a sistemas de información o redes. El objetivo de CVE es ayudar a las organizaciones a mejorar la postura de ciberseguridad entregando un catálogo de vulnerabilidades de software poniéndolo en un diccionario gratuito.

Configuración del banco de trabajo.

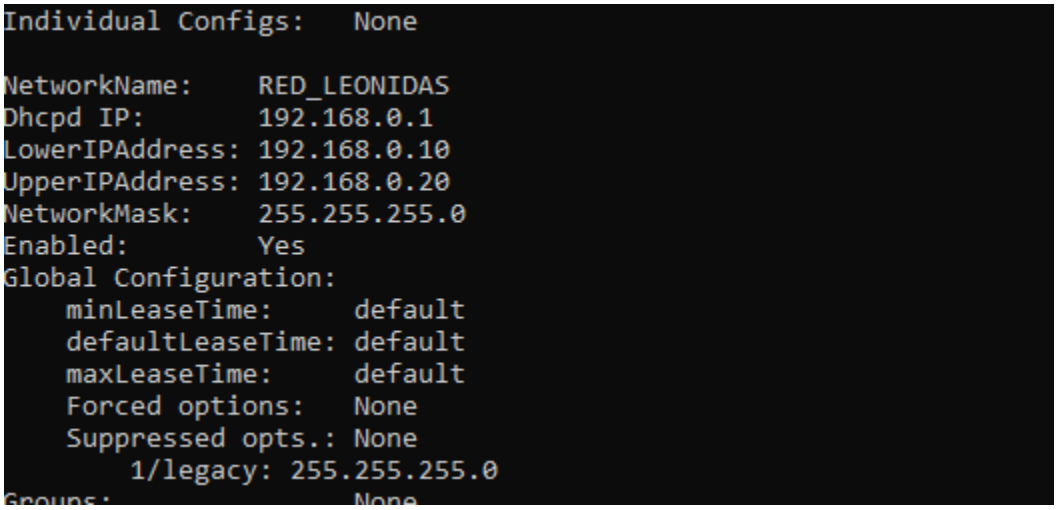
Se descarga e instala la última versión de Virtual Box y sobre ella se importan las máquinas que fueron dispuesta en el entorno de trabajo. A continuación, evidencia de la configuración final dentro de la misma red, llamada RED_LEONIDAS, en la que quedaron la máquina Windows 7 y Parrot.

Figura 1- Comando para incluir los equipos en RED_LEONIDAS



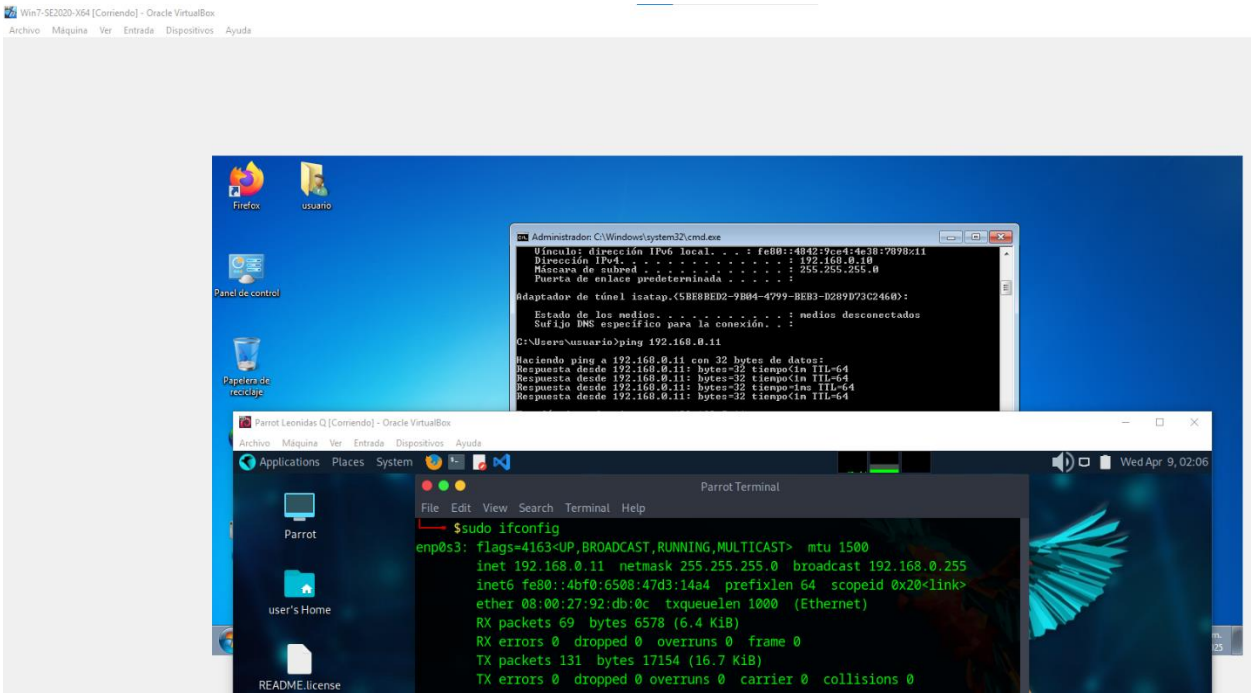
Fuente: Elaboración propia.

Figura 2- Verificación de la creción de la red interna.



Fuente: Elaboración propia.

Figura 3- Verificación de que las máquinas se pueden alcanzar entre si.



Fuente: Elaboración propia.

La máquina virtual de WIN7-SE2020-X64 quedó configurada como se resume más adelante:

- **Memoria base:** 2878 Mb
- **Memoria de video:** 128 Mb
- **Disco duro:** 50Gb
- **Adaptador de red:** Adaptador Intel PRO/1000 MT (Bridged Adapter)
- **USB:** Controladores OHCI y EHCI habilitados.

La máquina virtual PARROT, queda configurada como se evidencia en la imagen y se resume a continuación:

- **Memoria base:** 2790 Mb
- **Memoria de video:** 128 Mb

- **Disco duro:** 64 Gb
- **Adaptador de red:** Adaptador Intel PRO/1000 MT (Bridged Adapter)
- **USB:** Controladores OHCI y EHCI habilitados.

Respuesta a las preguntas con referencia al problema que se encuentra en el anexo 2 y anexo 3, en cuanto a lo ilegal y no ético.

¿Usted logra evidenciar algún proceso ilegal y no ético que esté estipulado en dicho acuerdo?

En efecto hay diversas situaciones que dan cuenta de procedimientos ilícitos y descuidados durante el proceso de contratación. A continuación, refiero aquellos procedimientos y acuerdos que, desde mi punto de vista, no atienden a la transparencia y el rigor de lo que debería cumplirse en un proceso de contratación para configurar equipos de ciberseguridad:

En primer lugar, debería tener gran relevancia, que todos los contratos elaborados por un profesional que ha sido desvinculado por estar inmerso en procedimientos ilícitos.

Por otra parte, del mismo **anexo 2 – Escenario 2**, hay referencia a problemas internos y que por ello se debe dar cumplimiento de una primera misión, en poco tiempo, bajo presión, bajo el entendimiento de que es una característica propia de los equipos red team y blue team.

En lo que concierne al **Anexo 3 – Acuerdo**, puntualmente, señalo los siguientes acuerdos que no corresponden a lo que se entiende como adecuado para para el compromiso que debe aceptar el receptor de la información:

En el primer punto de consideraciones, se indica que la información pertenece a CyberFort Technologies, pero resulta claro que se trata de información de datos personales.

En el punto 3 de las consideraciones, me parece que se está otorgando una responsabilidad demasiado amplia al decir que el contratante puede ser revelador, guarda y administrador de la información de CyberFort Technologies, creo que es innecesario para el objeto de la contratación.

En cuanto a las cláusulas suscritas se pueden resaltar los siguientes acuerdos con intención ilícita:

Clausula primera: Objeto: Se traza una obligación de no divulgar información sobre procesos ilegales dentro de CyberFort Technologies.

Clausula segunda. Definición de información confidencial: En el punto 2 de la definición de información confidencial incluyen datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos.

Tercera clausula. Origen de la información confidencial: Aunque ciertamente se debe ser amplio en la descripción de la información que puede ser confidencial para CiberFort Technologies, debido a que el receptor durante el desarrollo del objeto contractual puede conocer más información de la que requiere para la selección del personal, se puede considerar que no es necesario llegar a detalles como, a la naturaleza, formas de distribución, etc. Es de especial cuidado en esta cláusula la parte final que menciona que no se requiere advertir el carácter de confidencialidad de manera tácita y frente a ello considero que si se debe indicar específicamente para algunos casos, que si es o no confidencial, es cierto que hay información que se puede interpretar como confidencial, pero otra se debe etiquetar con esa característica para que quien la acceda le dé el debido tratamiento.

Cuarta clausula. Obligaciones de la parte receptora: En el punto 1 de esta cláusula queda una indicación que literalmente dice "Usarla únicamente para los propósitos relacionados con él"

acá queda una posibilidad para interpretar que el receptor pueda usar la información para propósito de propio interés.

En el punto 2 de esta cláusula refiere la protección de la información por parte del receptor, restringiendo el uso exclusivamente a las personas que tengan la necesidad de conocerla, creo que no basta la mera necesidad de conocerla sino especialmente la debida autorización y derecho para ello.

En el punto 3 de la cláusula cuarta de forma intencional se estable el compromiso ilícito de no denunciar el conocimiento de información ilegal que sea conocida durante la ejecución del contrato.

En el punto 5 queda una indicación escueta en cuanto al uso de la información confidencial, en cuanto a que solamente se indicará su uso al momento de la entrega de dicha información, esto puede ser un gran inconveniente para el receptor.

En el punto 6, se establece una obligación de mantener la información confidencial hasta que adquiera el carácter de pública, resulta poco común que la información confidencial tome esa característica y además no tiene mucho sentido que el receptor mantenga información que ya no requiera a través del tiempo.

El punto 8 desprende de cualquier responsabilidad a CyberFort Technologies, y carga el receptor de la responsabilidad frente a cualquier allanamiento, indicando además que la empresa se ve frente a esa posibilidad de allanamiento que normalmente sucede a empresas de actividades ilícitas.

El punto 9 de nuevo a hace referencia al compromiso por parte del receptor de no divulgar información ilegal haciendo énfasis en que solamente lo puede hacer bajo autorización de CyberFort Technologies.

Quinta clausula. Obligaciones de la parte reveladora: Seguramente de manera intencional esta obligación apenas queda enunciadas de manera incompleta así: “Mantener la reserva de la información confidencial hasta tanto”

Sexta clausula. Responsabilidad: Viniendo de un contrato que a toda luz tiene varios vicios e intenciones inapropiadas, resulta una gran responsabilidad para el receptor aceptar la carga que impone esta cláusula.

Clausula octava. Solución de controversias: De nuevo hay referencia a la información ilegal y en este caso indica que si es hallada en manos del receptor, este debe contratar un abogado privado y dejar exenta de responsabilidades a CyberFort Technologies.

Mencione que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

El acuerdo vulnera el artículo 269F. Violación de datos personales en cuanto a que CyberFort Tecnologies se otorga la potestad sobre toda la información confidencial, entendiendo que incluso posee información de los prospectos para conformar los equipos Blue Team y Red Team, sabiendo que esta pertenece a esas personas naturales.

También existe una vulneración al artículo 269H: Circunstancias de agravación punitiva, en su punto 7, en cuanto a que el acuerdo pretende utilizar como instrumento a un tercero de buena fe, al redactar los acuerdos con líneas de intención ilegal.

De igual manera hay referencia en el artículo 269H en su punto 8, en lo que tiene que ver con la responsabilidad si el que incurre en la conducta es el responsable de la administración, manejo o control de dicha información.

Existiendo procesos poco confiables en el anexo 3 – Acuerdo, ¿Usted como experto en ciberseguridad aplicaría a este trabajo en CyberFort Technologies, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

Efectivamente el proceso y sus acuerdos presenta una gran cantidad de propuestas de carácter ilegal que sin lugar a duda me indican que no es un trabajo que deba aceptar, aunque la propuesta económica sea tentadora, resultan claros los riesgos y las fallas en todo el proceso y además faltaría al código de ética de mi profesión que como se puede verificar en COPNIA (2017) enuncia lo siguiente:

- Artículo 31. Deberes generales de los profesionales:

Custodiar y cuidar los bienes, valores, documentación e información que, por razón del ejercicio de su profesión, se le hayan encomendado.

- Artículo 35. Deberes de los profesionales para con la dignidad de sus profesiones:

Respetar y hacer respetar las disposiciones, así como denunciar todas sus transgresiones y velar por el buen prestigio de las profesiones.

- Artículo 36. Prohibición de los profesionales con respecto de la dignidad de sus profesiones:

Recibir o conceder comisiones, participaciones u otros beneficios, con el propósito de gestionar, obtener o acordar designaciones de índole profesional o la encomienda de trabajo profesional.

- Artículo 39. Deberes de los profesionales para con sus clientes y el público en general:

Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan.

- Artículo 40. Prohibiciones a los profesionales respecto de sus clientes y público en general:

Ofrecer la prestación de servicios cuyo objeto, por cualquier razón, sea de dudoso o imposible cumplimiento, o los que por circunstancias de idoneidad personal, no se pueda hacer.

- Aceptar para su beneficio o de otros, comisiones o bonificaciones.

Interrogantes acerca de las implicaciones legales y éticas del caso problema Ciberespionaje y Ética en CyberFort Technologies" (Anexo 7 - Escenario 2)

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

En general las empresas de ciberseguridad deben establecer acuerdos y contratos en los que quede claramente estipulado el alcance de las pruebas y acceso a los sistemas sobre los que se tendrá alcance para el cumplimiento de lo contratado. Los acuerdos contractuales deben fijar límites sobre el tipo de auditoría que realizará a sus clientes, indicar la profundidad, las herramientas, la metodología y enmarcar el ambiente sobre el que realizará la intervención.

Es importante establecer acuerdos de confidencialidad

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

En primer lugar, se espera que exista ética profesional por parte de los empleados que usan herramientas para ciberseguridad. Con relación a la ética, además los empleadores deben realizar campañas de concienciación frecuentes para mantener observación sobre el actuar apropiado frente a las responsabilidades que conlleva al acceder a los activos de información de los clientes.

En todo caso las empresas de ciberseguridad deben tener un control riguroso sobre las herramientas que dispone para trabajadores, definiendo roles y privilegios claros sobre su uso, complementado con actividades de monitoreo de logs.

De igual forma deben quedar establecidos acuerdos de confidencialidad con castigos disciplinarios ejemplares.

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

Deberían realizar las investigaciones a profundidad para establecer la culpabilidad y el grado de impacto que hayan causado, emitiendo en consecuencia las acciones disciplinarias, correspondientes, especialmente aquellas que impidan la continuidad de su actuar.

Los gobiernos deberían, frente a esta situación, fortalecer sus marcos normativos, y jurídicos, de manera que se incite a la transparencia y se alcance una mejor observación del proceder de las empresas de ciberseguridad.

Como medida adicional deberían buscar la manera de aislar los recursos afectados y emitir comunicados a quienes pudieran resultar afectados por la extracción de la información.

Los gobiernos, posterior a la detección de la fuga de información, deberían fortalecer sus políticas para la seguridad de la información, sustentando en el cumplimiento riguroso de normas como la ISO 27001 o marcos de seguridad como NIST.

Ejercicio de ataque y explotación sobre el banco de trabajo desde la perspectiva del equipo Red Team.

Describción de las herramientas software utilizadas para llevar a cabo el anexo 4 – escenario 3 enfocado a Red Team, siguiendo los pasos del pentesting.

Sobre la mesa de trabajo configurada previamente según las indicaciones ofrecidas en la etapa 1, se ejecutan las siguientes actividades y comandos siguiendo los pasos ya reconocidos para ejecutar un pentesting:

Fase 1: Planificación y recolección de información:

En primer lugar se lee cuidadosamente el anexo Anexo 4 – Escenario 3, en busca de alguna pista con respecto al sistema vulnerable, confirmando que se trata del sistema operativo Windows 7 con una aplicación que tiene asociado un exploit que puede permitir acceso mediante Shell o escalamiento de privilegios con el posible uso del rol de administrador.

Con la información diferenciada se procede a ejecutar comandos Nmap para identificar los puertos y servicios que puedan estar expuestos, sin embargo, en este primer intento no fue posible obtener alcance desde la máquina con Parrot hacia la máquina con sistema operativo Windows, según información verificada en internet y posterior verificación con el tutor, sería necesario bajar el firewall en la máquina Windows para conseguir alcance al recurso.

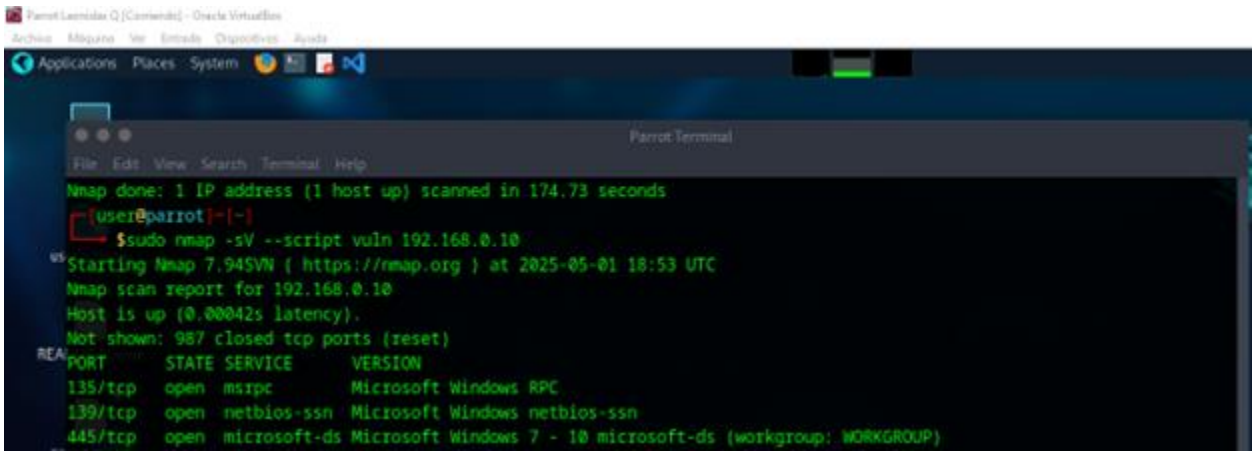
Se opta por el uso de Nmap que es una herramienta de código abierto, que sirve para escanear objetivos en una red, en búsqueda de aplicaciones, servicios, puertos abiertos y vulnerabilidades.

Se ejecuta el comando: sudo nmap –sV –Pn –script auth 192.168.0.10, para comprobar si hay usuarios con contraseñas vacías o algunos con contraseñas por defecto.

Como resultado del comando previamente referido, se confirma que no hay usuarios sin credenciales o contraseñas genéricas que se puedan explotar.

Se ejecuta el comando: sudo nmap –sV –script vuln 192.168.0.10, que permite identificar los servicios expuestos en el servidor objetivo, también los puertos abiertos y las vulnerabilidades:

Figura 4. Ejecución de comando para identificar vulnerabilidades. Print screen 1



Fuente: Elaboración propia

En este primer análisis ya se pueden identificar varios puertos abiertos que se pueden usar, como por ejemplo, el puerto 445 que expone el servicio Microsoft-ds que es un protocolo para intercambio de archivos en la red.

Especialmente, mediante este comando se obtiene información directa sobre la vulnerabilidad identificada como CVE-2017-0143, que es una vulnerabilidad propia de Windows que permite a los atacantes ejecutar código arbitrario mediante paquetes manipulados, conocido también como "vulnerabilidad de ejecución remota de código SMB en Windows"

Como lo explican en AVAST (2024) esta vulnerabilidad se relaciona con la identificada como smb-vuln-ms17-010, conocida como eternal blue que tiene que ver con el protocolo de Windows para compartir archivos SMBv1 que justamente se identifica en el puerto 445.

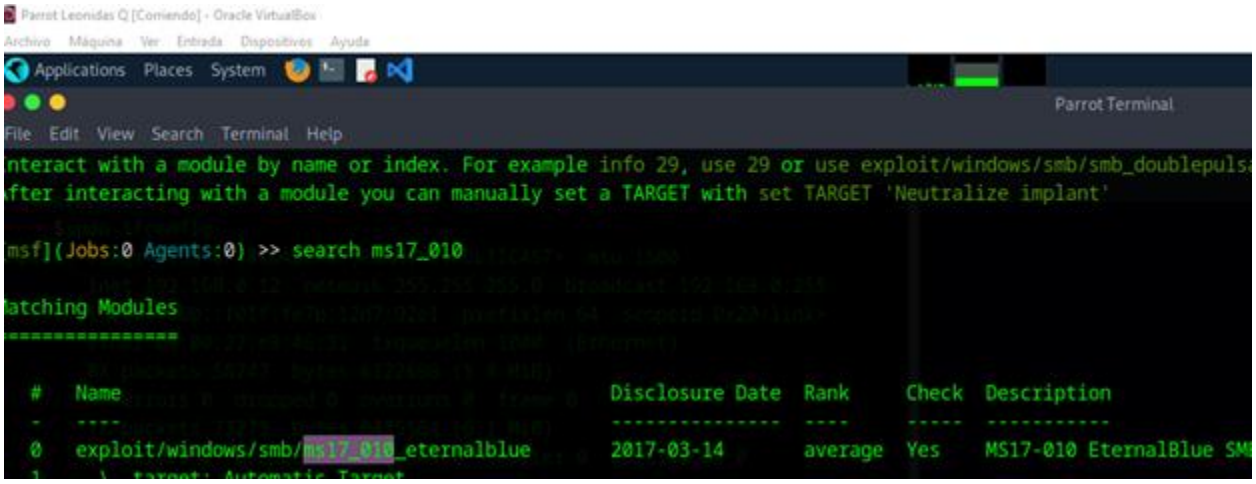
Se realiza la revisión con relación a la vulnerabilidad identificada en el paso anterior, y para ello se acude a las bases de datos de https://cve.mitre.org/

La **fase 2** de las etapas del pentesting se entiende cumplida con los comandos previamente ejecutados de Nmap, que nos aportan información necesaria y coherente frente a los descrito en el anexo4 –Escenario 3, aunque es cierto que también se puede ejecutar un análisis de vulnerabilidades haciendo uso de otra herramienta automatizada.

Con la información obtenida acerca de la vulnerabilidad CVE-2017-0143 se procede con la actividad de la **fase 3** del pentesting, que corresponde a la explotación.

Para este caso usaremos la herramienta disponible en Parrot que es Metasploit.

Figura 5. Se realiza búsqueda del exploit basado en la vulnerabilidad



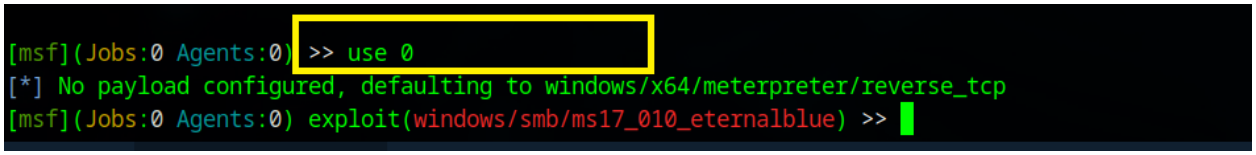
Fuente: Elaboración propia.

Metasploit es un framework diseñando para pentesting, que con una gran variedad de herramientas ayuda a identificar y mitigar riesgos de forma eficiente., su propósito general es generar y ejecutar payloads maliciosos basado en plantillas genéricas

Se inicia la herramienta Metasploit y posteriormente se procede con la búsqueda de los módulos asociados a la vulnerabilidad reconocida (smb-vuln-ms17-010), con el comando search ms17_010.

Una vez identificado el exploit que va a ser de utilidad se selecciona, en este caso indicando (use 0) en la línea de comandos.

Figura 6. Selección del exploit con USE.

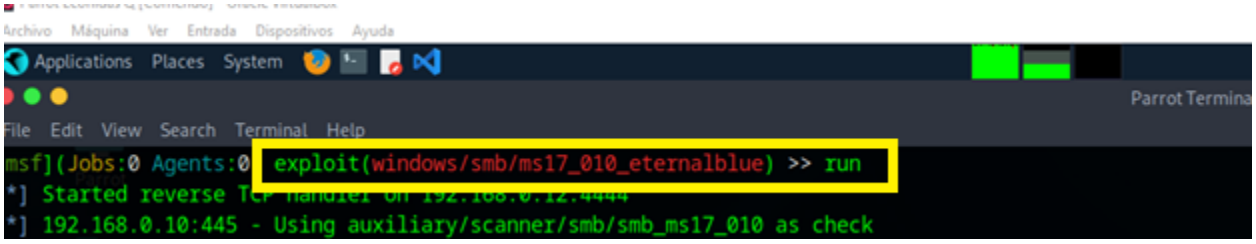


Fuente: Elaboración propia.

Haciendo uso del comando (show options) se verifican las configuraciones básicas que se deben definir previamente para ejecutar el exploit, como por ejemplo la IP de origen y la IP del objetivo.

En este caso se establece la IP de origen mediante el comando (set rhosts 192.168.0.10) y la IP de destino mediante el comando (set lhost 192.168.0.12).

Figura 7. Ejecución del exploit ms17_010_eternalblue



Fuente: Elaboración propia.

Se ejecuta el exploit que consiste en un payload llamado Meterpreter, propio del framework Metasploit, que permite obtener una gran cantidad del objetivo, como también manipular algunas características del mismo objetivo de explotación. Meterpreter cuenta con un intérprete que permite interactuar mediante comandos sencillos para realizar post-explotación.

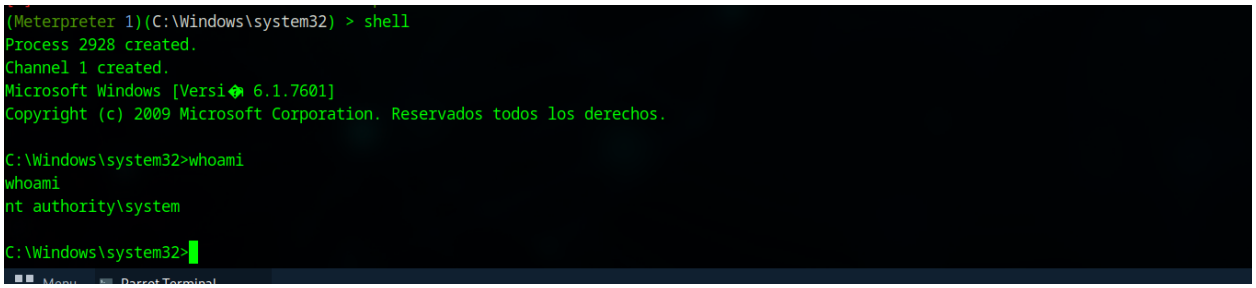
Una vez verificados los usuarios en el sistema objetivo, se retorna a punto en que conseguimos acceso por medio de meterpreter al sistema objetivo.

Se ejecuta el comando (Shell) sobre la línea de comandos de meterpreter para ejecutar comandos sobre la maquina objetivo como si se estuviera en ella.

En este punto se llega a la **fase 4** del pentesting que consiste en el escalamiento de privilegios. Se verifica el nivel de acceso que se ha obtenido mediante el comando (whoami), en

este caso nos confirma NT AUTHORITY\SYSTEM, que es una cuenta integrada de Windows con el máximo nivel de privilegios.

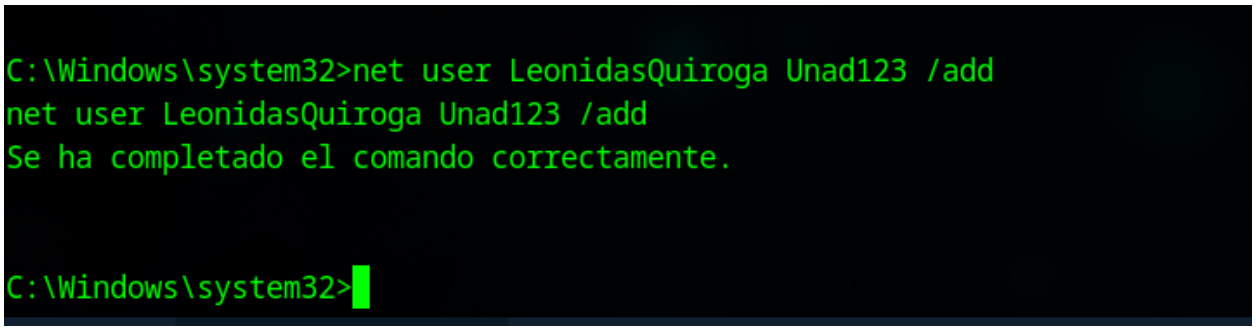
Figura 8. Ejecución comando shell.



Fuente: Elaboración propia.

Tomado de indicaciones presentadas en HARDMICRO (2024), se aprovecha el acceso obtenido se crea mediante comandos de Windows, la cuenta según las indicaciones del anexo 4. En este caso será LeonidasQuiroga con la contraseña Unad123

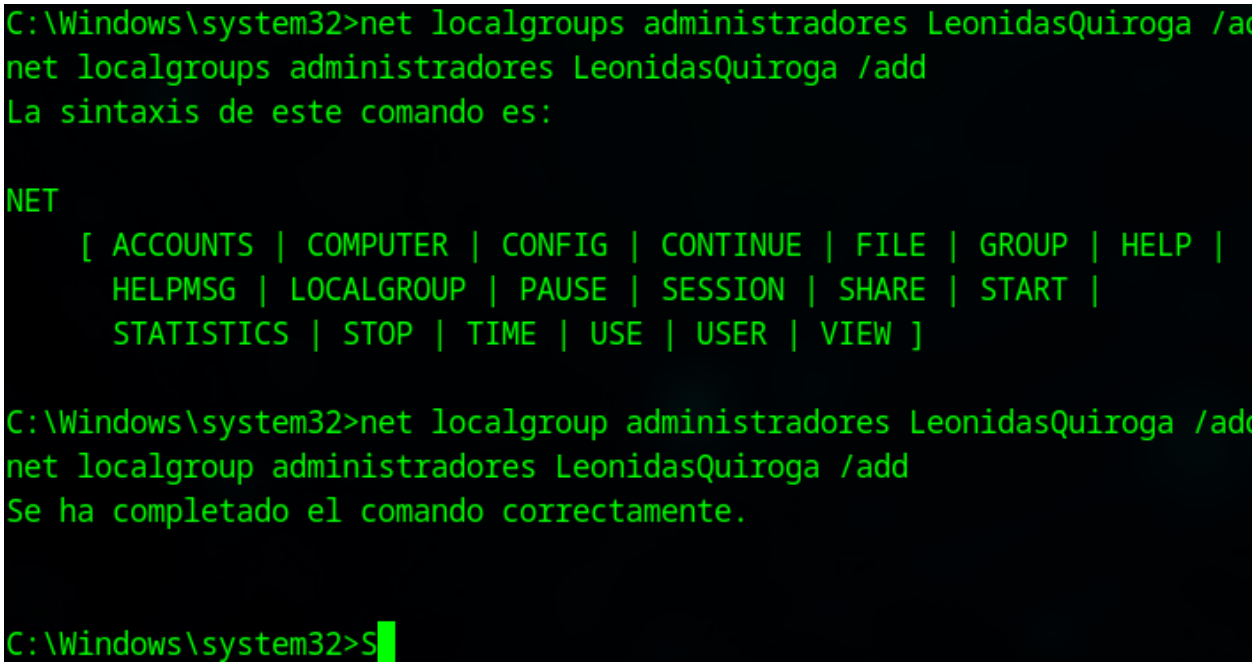
Figura 9. Creación del usuario administrador



Fuente: Elaboración propia.

Posteriormente se agrega al usuario LeonidasQuiroga al grupo de administradores.

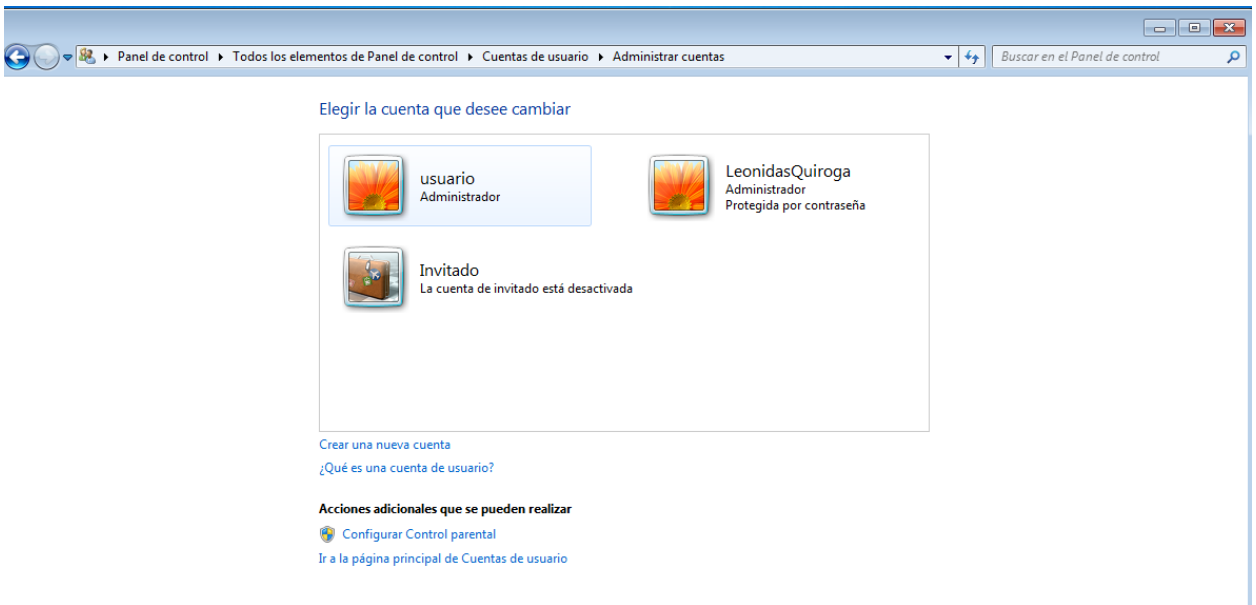
Figura 10. Se agrega usuario a grupo administradores



Fuente: Elaboración propia.

Se verifica sobre el sistema operativo objetivo, que efectivamente se haya creado el usuario con los privilegios determinados. A continuación, evidencia de que tuvieron efecto loas comando ejecutados de forma remota.

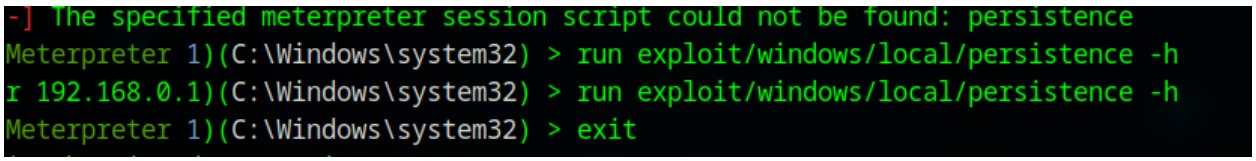
Figura 11. Verificación de la creación del usuario en sistema objetivo



Fuente: Elaboración propia.

Siguiendo indicaciones halladas en OFFSEC (2024) y para completar la **fase 5** del pentesting, se ejecuta el comando para mantener la persistencia, como se observa a continuación:

Figura 12. Ejecución del comando para mantener persistencia



Fuente: Elaboración propia

Datos del anexo 4 – Escenario 3 que fueron de ayuda para identificar el fallo de seguridad específico el cuál ataca a la máquina Windows.

La primera información orientadora es que la maquina Windows al parecer tiene asociado un exploit que mediante Shell, permite el escalamiento de privilegios, mediante la creación de un usuario con privilegios de administrador.

Esta información permite confirmar frente a los primeros escaneos que se trata de la vulnerabilidad eternalblue que permite la ejecución de código arbitrario, aprovechando el protocolo vulnerable SMB de Windows.

Afectación del ataque a la máquina Windows.

Esta explotación permite ejecutar de forma remota en la máquina Windows, permitiendo crear usuarios con elevados privilegios, además esta ejecución de comandos no exige

autenticación por parte del atacante debido a que ya ingresa con los privilegios más altos que otorga el sistema.

El acceso conseguido mediante este ataque permite establecer persistencia, facilita la extracción de información, permite la instalación de software malicioso e incluso ha sido usado para cifrar información.

Primeras indagaciones que se deberían realizar si se llegara a encontrarse un ataque en tiempo real.

Una de las primeras acciones que se deben considerar es la identificación de los activos que están siendo afectados para implementar el aislamiento de dichos activos para posteriormente analizar las causas y mecanismos usados para realizar la afectación.

Es importante en este punto dimensionar la afectación y proceder con el análisis de los logs de los sistemas afectados, bien sea desde las herramientas de monitoreo, si existen, los propios de los sistemas operativos o mediante al uso de herramientas de análisis forense. En todo caso, es necesario preservar cuidadosamente toda evidencia hallada, que pueda dar claridad con respecto a las rutas, tácticas y técnicas usadas, bien sea para documentar lecciones aprendidas como para atender requerimientos de investigación.

Identificar oportunamente los vectores de ataque y las vulnerabilidades aprovechadas, presentan la posibilidad de actuar de una manera precisa, mediante la aplicación de la remediaciones y correctivos ajustados al tipo de ataque, evitando una posible dispersión de esfuerzos que a la larga significan costos significativos.

Las primeras acciones se deben ejecutar de la forma más inmediata y coordinada con todos los profesionales que tengan la capacidad técnica resolutiva de forma que se logre impedir la expansión del ataque y afectaciones de mayor dimensión.

En la página de (Argentina.gov.ar, 2024), presentan el actuar frente a casos particulares de ransomware, y que, a mi modo de ver, puede ser general para cualquier tipo de ataque, desde la perspectiva de las responsabilidades como usuarios finales, como responsables de gestionar los incidentes y como autoridad o líder de área.

A los usuarios finales se les recomienda mantener la calma, recordar detalles de cómo sucedió, especialmente recordar la fecha y hora, no apagar los equipos, desconectarlos de la red si es posible, contactar a los responsables del área de seguridad de la información, entregar cualquier evidencia que le sea requerida.

Por parte de los responsables de gestionar los incidentes, de comenzar por aislar los equipos comprometidos, revisar las herramientas de monitoreo con el fin de identificar si pudo suceder un movimiento hacia otros equipos o las direcciones IP de donde proviene el ataque, indagar por cualquier evidencia que puedan aportar los usuarios afectados, realizar clonación de los discos afectados para preservar evidencia, ejecutar herramientas antimalware o los comandos conocidos para recuperar el sistema, para el caso de ransomware investigar si se trata de una variante conocida de a que exista documentación para posible recuperación o la restauración a partir de las copias de respaldo, realizar los informes detallados de lo analizado y acciones tomadas, aplicar medidas coherentes para cerrar la brechas de seguridad identificadas.

De la misma fuente (Argentina.gov.ar, 2024), finalmente presenta el quehacer como autoridad o líder de procesos, quienes deben brindar las herramientas que el equipo de gestión de

incidentes de seguridad requiera, manteniendo, en estos eventos una comunicación permanente, apoyando con decisiones.

Es relevante que las autoridades y lideres no cedan frente a cualquier petición de los cibercriminales, deben mantener un canal de comunicación con las partes interesadas para canaliza información apropiada, tomar acciones legales, según corresponda y apoyar a las autoridades.

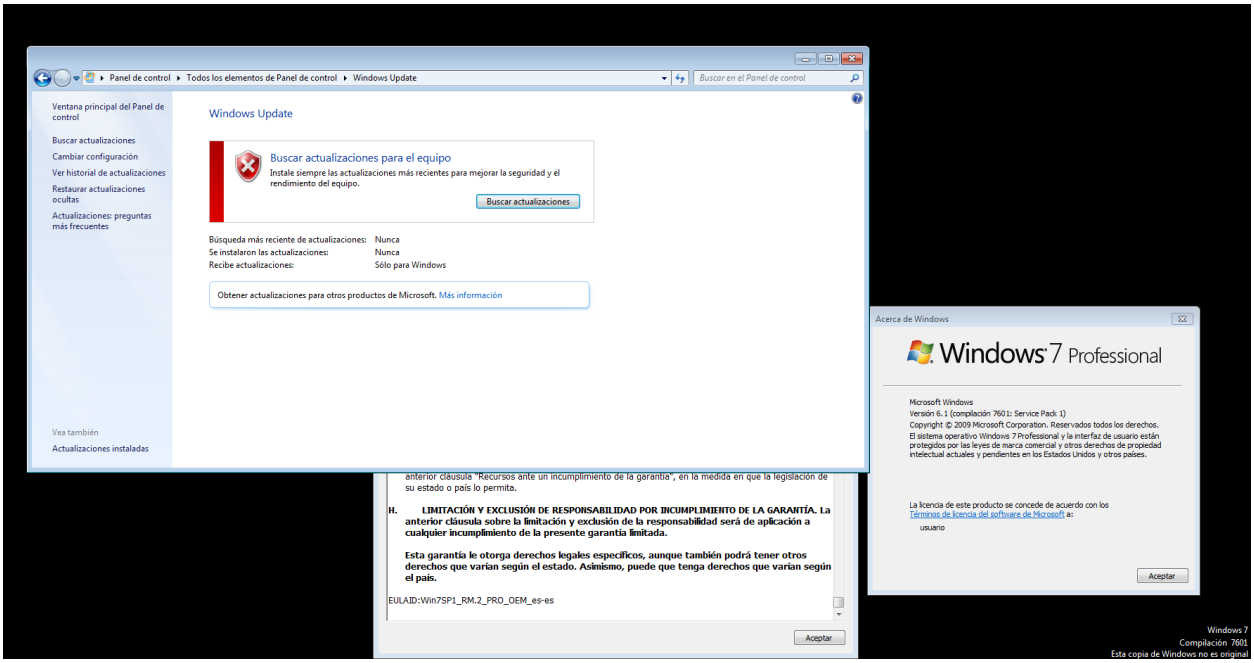
Medidas de hardenización a implementar para evitar el ataque.

Para el caso específico del escenario que se viene trabajando con Windows 7 y Parrot lo primero que resulta evidente solucionar, es la activación de los servicios del firewall de Windows.

En segundo lugar, es necesario **aplicar actualizaciones** al sistema operativo y asegurarse de que se reconozca con licencia original. El escenario trabajado indica que la instalación no es original. Para el caso que se pudo reconocer la posibilidad de explotación de eternalblue, se debe aplicar el parche de Windows MS17-010, que fue generado en al año 2017

Lo que correspondería en cualquier escenario real, es la migración a las últimas liberaciones funcionales y aprobadas de Windows, no debería trabajarse con un sistema operativo tan antiguo, al que ya no se le desarrollaron actualizaciones de seguridad.

Figura 13- Windows sin licencia y desactualizado.



Fuente: Elaboración propia.

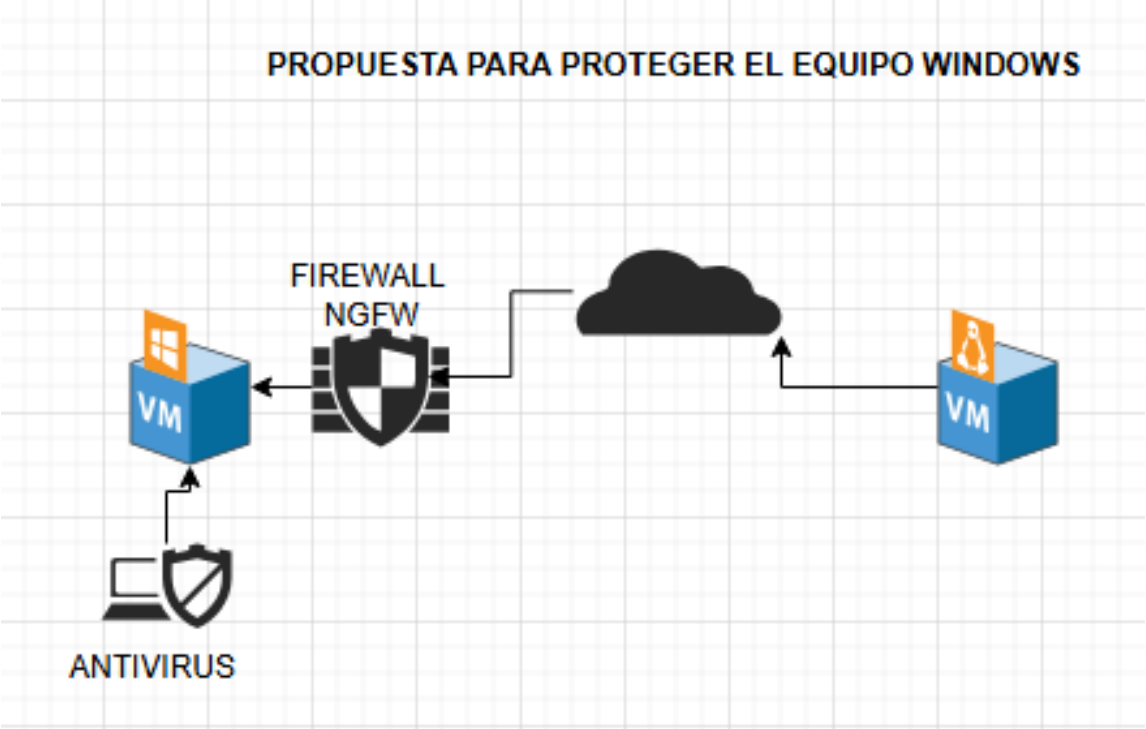
Dado que el protocolo vulnerable en este caso es el SMBv1, se debe deshabilitar dentro de las características de Windows.

Es relevante bloquear los puertos que fueron identificados en la fase de exploración, para el caso que se viene trabajando corresponde el bloqueo del puerto **TCP 445.**

Se debe instalar una herramienta de antivirus actualizada o realizar actualización de la versión de Defender ya instalada.

Frente a la explotación conseguida es necesario interponer herramientas y soluciones como un firewall de nueva generación o un IPS, de manera que se pueda aplicar directivas de filtrado más específicas, a continuación, se propone un esquema de cómo podría ser según el caso que se viene trabajando:

Figura 14- Propuesta de protección mediante Firewall



Fuente: Elaboración propia.

Con la implementación de herramientas como un Firewall o un IPS, se adquiere la capacidad adicional de realiza monitoreo constante a la red y esto constituye a su vez en una forma de hardenizar la infraestructura afectada.

Por último, es importante promulgar información a los usuarios con relación a la importancia de establecer contraseñas robustas, que no sean compartidas o expuestas. Se deben configurar políticas en las plataformas, que obliguen al cambio de contraseñas de forma frecuente y que controlen una longitud mínima de 12 caracteres.

Diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos.

Antes de presentar las diferencias entre estos equipos de trabajo, es necesario presentar la definición de cada uno de ellos.

Como es presentado en la página de Keep Coding (2025), los Blue Team son equipos compuestos por expertos en ciberseguridad, especializados en analizar el comportamiento de los sistemas, se encargan de reunir el inventario de activos, reforzar el acceso a los sistemas, establecer protocolos de vigilancia, realizar comprobaciones de los sistemas y efectuar evaluaciones de riesgos observando las amenazas.

Por otra parte, TechTarget (2025), define el CSIRT, equipo de respuesta a incidentes de seguridad informática, como un grupo de profesionales de TI que da servicios de soporte a las organizaciones, frente a la evaluación, gestión y prevención de asuntos relacionados con la ciberseguridad y la coordinación de actividades de respuesta a incidentes de forma rápida y eficiente para recuperar el control con el mínimo de daños posible.

A continuación, se presentan algunas diferencias entre los equipos descritos:

Figura 15- Dferencias ente Blue Team y CSIRT

Dimensión	BLUE TEAM	CSIRT
Objetivo	Detectar y prevenir amenazas	Invesigar y resolver incidentes criticos
Habilidades	Defensa, hardening, monitoreo	Análisis forense, análisis de malware, gestión de crisis
Interacciones	Trabaja con Red Team en simulaciones	Con la alta dirección, comunicaciones y partes legales
Funciones	Prevenir, detectar, dar respuesta inicial.	Respuesta a incidentes, forense digital, recuperación, comunicación
Enfoque	Trabajo constante y con sentido preventivo	Específico y reactivo, especializado en crisis
Temporalidad	Permanente	Solamante durante los incidentes
Relación	Proporciona datos de monitoreo al CSIRT	Informa al Blue Team sobre brechas de seguridad para cubrir.
Herramientas usadas	SIEM, EDR, NIDS	Herramientas forenses

Fuente: Elaboración propia.

Uso de CIS "Center For Internet Security" en un Blue Team

Laiba Siddiqui de Splunk, 2024 explica que los controles CIS son un marco de acciones que las compañías pueden implementar para mejorar su seguridad. Estos controles se organizan en 18 categorías, recibiendo actualizaciones constantes para atender la evolución permanente de las amenazas. En general los controles CIS se definen como el conjunto priorizado de medidas para atender los ciberataques que pueden impactar a redes y sistemas.

Ciertamente los Blue Team pueden recibir múltiples beneficios con la implementación de los controles CIS y en consecuencia las organizaciones se verían impactadas positivamente.

Los Blue Teams, verían los beneficios en los siguientes aspectos:

- **Priorización:** CIS entrega una lista de procedimientos de seguridad que ayuda a centrar esfuerzos en los aspectos más críticos.
- **Reducción de riesgos:** Con la adecuada gestión de activos y gestión de vectores, se reduce la exposición.
- **Estandarización:** Los controles CIS estandarizan controles de seguridad, estableciendo una manera estandarizada o lenguaje de referencia común de seguridad.
- **Progreso medible:** Los controles Cis ofrecen una hoja de ruta que facilita medir el progreso de las organizaciones en cuanto a la implementación de la seguridad.

Directamente sobre los controles CIS los Blue Teams puede aplicar y recibir beneficios de los siguientes controles: (Tomado de: SPLUNK 2024)

1- Inventario y control de los activos de la empresa.
2- Inventario y control de activos de sofware.
3- Protección de datos.
4- Configuración activa de activos y software empresarial.
5- Gestión de cuentas.
6- Gestión de control de acceso.
7- Gestión continua de vulnerabilidades.
8- Gestión de registros de auditoría.
9- Protecciones de correo electrónico y navegado web.
10- Defensa contra malware.
11- Recuperación de datos.
12- Gestión de infraestructura de red.

13- Monitoreo y defensa de la red.

14- Concientización sobre ciberseguridad y capacitación en habilidades.

15- Seguridad del software de aplicación.

16- Gestión de respuesta a incidentes.

Interpretando los que expone (TRLOGIC 2023), resulta claro desde la enumeración de algunos controles CIS, que aplican de forma ajustada a lo que se reconocen como las actividades propias de los Blue Teams y se integran de manera armoniosa su enfoque holístico, en el sentido en que son se limita a la defensa desde un solo punto de vista, sino que combina diferentes perspectivas como el gobierno de la práctica de la seguridad, la detección de vulnerabilidades, la gestión de terceros para corregir inconvenientes, la gestión de incidentes, la sensibilización y todos las actividades que correspondan a la mejora continua.

El SIEM, sus funciones y características principales

(IBM, 2025), presenta a la gestión de eventos e información de seguridad (SIEM), como una solución de seguridad que ayuda a las compañías a identificar y gestionar posible amenazas y vulnerabilidades de seguridad antes de que causen alguna afectación.

De manera general los SIEM realizan funciones de agregación, consolidación, y clasificación de datos para identificar amenazas y cumplir los requisitos de conformidad de datos (IBM, 2025)

De la misma fuente (IBM, 2025) es importante resaltar las siguientes funciones básicas de un SIEM:

- **Gestión de registros:** El SIEM consume datos de diferentes fuentes, luego de ser recopilados se correlacionan y analizan en tiempo real, incluyendo fuentes de terceros.

- **Correlación y análisis de eventos:** Se utilizan análisis avanzados para reconocer y entender patrones de datos complejos, entregando información para ubicar y mitigar amenazas de seguridad.
- **Supervisión de incidentes y alertas de seguridad:** Las herramientas SIEM proporcionan información centralizada mediante paneles, que pueden ser consultados por lo equipos de seguridad para identificar de manera oportuna las amenazas y dar respuesta
- **Gestión de la conformidad y elaboración de informes:** Estas soluciones pueden proveer informe de cumplimiento en tiempo real como por ejemplo sobre PCI-DSS, HIPPA, etc. Reduciendo la carga de trabajo y detectando infracciones de manera temprana para abordar su remediación.

Ventajas de un SIEM:

Continuando con la exposición que entrega (IBM, 2025), resulta de gran valor referir a continuación, algunas de las ventajas de implementar un SIEM:

- Reconocimiento de amenazas en tiempo real.
- Automatización mediante inteligencia artificial.
- Mejora de la eficiencia organizativa.
- Detección de amenazas avanzadas y reconocidas.
- Investigaciones digitales.
- Evaluación e informes de cumplimiento.
- Supervisión de usuarios y aplicaciones.

3 herramientas de contención de ataques informáticos (hardware o software)

En la actualidad se pueden hallar una cantidad importante de herramientas, ya sea de pago o gratuitas que ofrecen capacidades valiosas para contener ataques informáticos. Para este caso se hará referencia a 3, y cada de una de ellas pertenecientes a estrategias diferentes de contención (SIEM, IPS, EDR) :

- **WUAZUH:** Es una herramienta de código abierto para la gestión de eventos e información de seguridad **(SIEM),** que presenta todas las capacidades para la supervisión, detección y alertas de seguridad. Wazuh esta disponible sin algún costo y viene con el enfoque de código abierto, buscando presentar transparencia, flexibilidad y mejora constantes con soporte, igualmente gratuito, una documentación amplia y actualizada y sobre todo una comunidad activa que le da soporte y le sostiene actualizaciones.

(IMAGUNET, 2025), Wazuh usa un agente ligero de seguridad para endpoints que se despliega en los sistemas supervisados y un servidor de gestión inteligente que entrega la inteligencia sobre amenazas con el correspondiente análisis. Wazuh cuenta con un motor de búsqueda y herramientas para la visualización facilitando el entendimiento a los usuarios.

- **SNORT:** Es un sistema de prevención de intrusiones (I**PS**), de código abierto que usa reglas para definir actividad maliciosa de la red y mediante estas reglas busca coincidencias para generar alertas (SNORT, 2025). Snort usa esas reglas para combinar métodos de inspección de anomalías, protocolos y firmas que facilitan detectar actividades maliciosas.

  Snort ofrece características que ofrecen monitoreo de tráfico en tiempo real, registro de paquetes, análisis de protocolos, revisión de coincidencia de contenido,

validación de huella digital del sistema operativo, facilidad de instalación en cualquier plataforma o entorno de red y fuente abierta (FORTINET, 2025).

Snort funciona en 3 modos principales; modo analizador, capturando paquetes de red, modo de registrador de paquetes, captura y guarda para analizar y modo de intrusión de red, en este caso busca actividad maliciosa.

- **CROWDSTRIKE:** (DELL, 2025), en términos generales la describe como una herramienta de detección y respuesta a endpoints (EDR), que utiliza (IA) inteligencia artificial y análisis de comportamiento para identificar actividad maliciosa y aplicar contención en tiempo real. Crowdstrike también ofrece protección contra amenazas avanzadas (APT)

  Crowdstrike toma información de los endpoints a partir de un sensor ligero que luego envía los datos la nube para se analizados por su motor de inteligencia artificial, generando de inmediato las alertas y aplicando de forma automática el aislamiento o eliminación de malware.

  Crowdstrike no basa su análisis en la comparación de firmas tradicionales sino en el análisis con machine learning e IA, facilitando caza de amenazas y monitoreo continuo

Conclusiones

El gobierno colombiano ha emitido leyes robustas sobre ciberseguridad y protección de datos personales, has sido actualizadas frente a la evolución de las nuevas técnicas de los cibercriminales y alineadas con acuerdos y convenios a nivel global.

Estudiar las fases para la realización de pentesting nos ayuda a comprender que es una actividad que se debe realizar de forma metódica y ordenada para obtener resultados e informes de calidad.

El ejercicio de instalación de la máquina virtual y los sistemas operativos Parrot y Windows 7 ayudan a preparar el escenario para efectuar el laboratorio, mientras en la misma actividad se repasan conceptos para incluir los servios dentro de un mismo segmento de red.

Debe existir un fuerte compromiso por parte de los profesionales en ciberseguridad en cuanto al actuar ético, con un riguroso cumplimiento de los acuerdos contractuales y el respeto por la profesión.

El establecimiento de acuerdos contractuales exige un gran cuidado y entendimiento de lo redactado, entendiendo que lo firmado constituirá las obligaciones y responsabilidades.

Los gobiernos deberían implementar tempranamente equipos con suficientes capacidades para detectar y gestionar cualquier ataque que pueda afectar a la información en cualquiera de sus dimensiones.

El ejercicio realizado pone de manifiesto que los sistemas operativos se deben actualizar con frecuencia, pero especialmente que aquellos sistemas que ya no tiene soporte, ya no se les debe permitir su uso dentro de las organizaciones, debido a que son una puerta

abierta para los cibercriminales que los buscan como primer objetivo para moverse desde allí a objetivos de mayor valor.

Para el profesional en seguridad informática, resulta de especial importancia la realización de actividades pentesting, debido a que lo lleva a la investigación y al afianzamiento de conocimientos a partir de la práctica.

Las pruebas de pentesting ofrecen información mucho más precisa con respecto a las medidas de contención y remediaciones que se deben aplicar para proteger los activos de información, desde una perspectiva que resulta menos costosa para las organizaciones, eludiendo en gran medida el impacto que implica un ataque real.

Nmap y Metasploit constituyen una plataforma muy completa para la realización de pruebas de pentesting, además de que cuentan con una amplia base de conocimiento y una comunidad muy activa que está brindando soporte.

La vulnerabilidad conocida como eternal blue otorga una gran capacidad para ejecutar comandos con privilegios elevados, lo que facilita la toma de control del equipo objetivos, facilitando la ejecución de diversas posibilidades de explotación, por eta razón este exploit ha permanecido por mucho tiempo como uno de los más dañinos.

Frente a un ataque cibernético, cobra particular relevancia la identificación de los activos afectados para realizar su aislamiento e iniciar la etapa de investigación, preservando las evidencias. La etapa de investigación debe conducir de la manera más inmediata a la diferenciación de las causas para aplicar las acciones de contención y recuperación adecuadas.

Aplicar medidas de hardenización resultan valiosas como una estrategia de prevención debido a que impiden afectaciones y costosas actividades de recuperación luego del impacto de actividades maliciosas. Es conveniente en este punto reconocer claramente todos los activos de información y realizar la investigación de las recomendaciones de la industria de ciberseguridad y los fabricantes para asegurar los mínimos privilegios y las últimas liberaciones de actualizaciones.

Los equipos Blue Team realizan actividades permanentes de monitoreo y reconocimiento de las posibles vulnerabilidades, buscado cerrar las brechas de seguridad a partir de la información entregada por las herramientas o los informes recibidos por parte de los Red Teams. Los Blue Teams deben conocer con claridad los activos de información y mantener una comunicación constante con los usuarios, en el sentido de concientizar acerca de diversos temas de la ciberseguridad y sus responsabilidades dentro de la cadena de la seguridad de la información. Por su parte los equipos de respuesta a eventos de seguridad tienen su actuar especialmente sobre la solución de situaciones críticas cuando se materializa un incidente se seguridad de la información.

Recomendaciones

Es necesario, que desde las instituciones de educación superior y en particular las que se encargan de la formación de profesionales en seguridad informática y afines, se continúe motivando el acercamiento hacia los lineamientos del gobierno colombiano en cuanto a la ciberseguridad de manera que podamos entender con claridad el marco regulatorio, las normas y leyes que rigen nuestro contexto cercano para bajarlo y extenderlo dentro de las organizaciones para la que trabajamos, además de visualizar el apoyo que se puede obtener desde las instituciones del gobierno.

Resulta primordial para los profesionales en seguridad informática, mantener el ejercicio continuo de prácticas relacionadas con las actividades de los equipos Red Team y Blue Team, haciendo uso de las diferentes y mas novedosas herramientas para hacer intrusión y contención, complementando con la investigación para aplicar con actividades que necesariamente se deben realizar de forma manual según los contextos que propongan los retos laborales.

Ser metódicos y seguir un marco de trabajo específico son características que le dan solidez a las actividades efectuadas con el propósito de identificar vulnerabilidades y contenerlas, especialmente si se sustentan todas la experiencias y observaciones en la documentación y preservación de evidencias.

En todo caso hoy en día, frente a la evolución y sofisticación de los ataques cibernéticos con el apoyo de la inteligencia artificial, es absolutamente necesario hacerles frente con las mismas tecnologías como los EDR y los SIEM.

Referencias Bibliográficas

ARGENTINA.GOV.AR, 2024. Ransomware: Cómo actuar frente a este tipo de ataque. https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/publicaciones-0

AVAST 2024. ¿Qué es Eternalblue y por qué el exploit MS17-010 sigue siendo relevante? https://www.avast.com/es-es/c-eternalblue

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

DELL, 2025. ¿Qué es la plataforma Crowdstrike Falcon? https://www.dell.com/support/kbdoc/es-co/000126839/que-es-crowdstrike

FORTINET, 2025. ¿Qué es SNORT? https://www.fortinet.com/lat/resources/cyberglossary/snort

Función Pública (2022). Decreto 338 de 2022. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Función Pública 2009. Ley 1273 de 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Función Pública 2012, Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4998

HARDMICRO 2024. Cómo crear usuarios desde la consola de comando. https://hardmicro.net/es/art%C3%ADculos/198-como-crear-usuarios-desde-cmd

IMAGUNET, 2025. Protege tu infraestructura con wazuh.
https://www.imagunet.com/ciberseguridad-wazuh/

KEEPCODING 2025. ¿Qué es Blue Team en ciberseguridad?
https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

Keep Coding 2024. ¿Qué es metasploit? https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Normograma MINTIC 2018. Ley 1928 de 2018.
https://normograma.mintic.gov.co/mintic/compilacion/docs/ley_1928_2018.htm

OFFSEC 2024. Metasploit Unleashed – Free online ethical hacking course.
https://www.offsec.com/metasploit-unleashed/snmp-scan/

SIDDIQUI LAIBA, SPLUNK 2024. Controles de seguridad críticos del CIS.
https://www.splunk.com/en_us/blog/learn/cis-critical-security-controls.html

TARLOGIC, 2023. Blue Team: Fortalecer la defensa de una compañía.
https://www.tarlogic.com/es/blog/blue-team/

TECHTARGET 2025. Equipo de respuesta a incidentes de seguridad informática (CSIRT)
https://www.techtarget.com/whatis/definition/Computer-Security-Incident-Response-Team-CSIRT

WASUH, 2025. Who we are
https://wazuh.com/

Welivesecurity 2025. Evaluación de vulnerabilidades usando Open Vas.
https://www.welivesecurity.com/es/recursos-herramientas/evaluacion-vulnerabilidades-openvas/