22-12-2024

Prueba Final Analista SOC Nvl1

Brian Almada
ALUMNO DE COMUNIDAD DOJO

TABLA DE CONTENIDO

        - Fuentes
        - Recomendaciones para Mitigar la Amenaza
    - Reporte de la Amaneza de la Hipótesis 3 Baiting:
        - Captura de pantalla de la amenaza en Splunk.
        - Análisis del incidente detectado en Splunk:
            - Descripción
            - Impacto Potencial
            - Fuentes
            - Recomendaciones para Mitigar la Amenaza
    - Reporte de la Amenaza de la Hipótesis 4 DDoS:
        - Introducción del reporte.
        - Capturas de pantalla de la amenaza DDoS en Wireshark
        - Análisis de ataque Slowloris (DDoS) en Wireshark:
            - Detalles del evento.
            - Descripción de ataque.
            - Impacto potencial.
            - Recomendaciones para mitigar la amenaza.
    - Reporte de la Amenaza de la Hipótesis 5 Explotación de Puertos:
        - Captura de pantalla de la amenaza EternalBlue en Splunk.
        - Análisis del incidente detectado en Splunk:
            - Descripción
            - Impacto Potencial
            - Recomendaciones para Mitigar la Amenaza
- PARTE 4: DOCUMENTACIÓN Y VIDEO
    - Informe:
        - Mis hipótesis y como las desarrollé.

- Detalles sobre mis datasets creados y su relación con las hipótesis.
- Resultados de los análisis.
- Conclusiones.

➢ Contenido del video:

- ¿Cómo usé las herramientas para analizar los datos?
- ¿Cómo identifiqué la amenaza?
- Explicación a la organización LongevityCorp sobre como prevenir incidentes simulares a futuro

❖ Glosario Técnico:

➢ Referencias a las técnicas y tácticas citadas en este documento.

➢ Referencia a CVE 2017-0144 EternalBlue

➢ ¿Qué es DVWA?

➢ ¿Qué es XAMPP?

Prueba Técnica

PARTE 1

Desarrollo de Hipótesis.

En esta sección desarrolle cinco (5) hipótesis basándome en el perfil de la organización LongivityCorp. Dichas hipótesis tienen sus técnicas y tácticas correspondiente al marco MITRE ATT&CK

Hipótesis 1: Técnica Phishing (T1566) con sub-técnica Spear-Phishing (T1566.001).

Táctica y Técnica usada:

- **Phishing** (T1566): Técnica usada para obtener información confidencial como nombres de usuarios, contraseñas y detalles financieros vía engaños.
- **Sub-Técnica: SpearPhishing** (T1566.001): Similar al phishing, pero dirigido específicamente a un individuo o grupo dentro de una organización, basada en información obtenida previamente sobre el objetivo.

Activo/Recurso en Riesgo:

- **Empleados de LongevityCorp**: Los empleados son el objetivo inicial del spear-phishing.
- **Red y Recursos Internos**: Una vez que los empleados son comprometidos, el atacante puede obtener acceso a la red interna y a recursos críticos de la organización.

Impacto Potencial:

- **Acceso No Autorizado**: Si un empleado ejecuta el archivo malicioso, el atacante puede obtener acceso a la red interna con los privilegios del empleado comprometido. Dicho de otra forma, si el empleado tiene privilegio de administrador entonces al ejecutar dicho archivo este tendrá privilegios de administrador.
- **Robo de Información Confidencial**: El acceso a la red interna puede permitir al atacante exfiltrar datos sensibles y confidenciales de la empresa.

- **Interrupción de Operaciones**: El atacante puede usar su acceso para interrumpir las operaciones normales de la empresa, afectando la productividad y la seguridad.

Detalles de la Hipótesis:

- **Táctica de Reconocimiento**:
  - El atacante inicia una táctica de reconocimiento de la organización (T1591).
  - Identifica ubicaciones físicas (T1591.002) mediante análisis de perfiles de LinkedIn, imágenes del sitio de trabajo y enlaces al sitio web de LongevityCorp.
- **Táctica Desarrollo de Recursos** (Relaciones Comerciales):
  - Reconocimiento de las relaciones comerciales de la empresa (T1591.002).
  - Identificación de proveedores, contratistas y otras organizaciones que tienen acceso a la red.
- **Táctica: Acceso Inicial** (Phishing dirigido):
  - El atacante fabrica un spear-phishing dirigido a un empleado específico, haciéndose pasar por un proveedor.
  - Envío de un correo electrónico urgente con un archivo PDF adjunto que contiene una carga útil maliciosa.
- **Táctica: Ejecución** (Ejecución y Acceso):
  - Si el empleado abre el archivo PDF y ejecuta la carga útil, se establece una Reverse Shell que da al atacante acceso a la red interna
- **Táctica Persistencia**:
  - El acceso obtenido puede ser usado para moverse lateralmente vía red (T1078), robar información confidencial, y potencialmente interrumpir las operaciones de la empresa.

Resumen de la Hipótesis:

La hipótesis supone que un atacante podría usar técnicas de spear-phishing para comprometer a un empleado de LongevityCorp, obteniendo acceso no autorizado a la red interna y a datos confidenciales. Si se confirma esta hipótesis, las consecuencias

podrían incluir el robo de información crítica y la interrupción de las operaciones de la empresa.

Hipótesis 2: Amenaza Interna (Empleado Disconforme)

Técnica/Táctica usada:

- **Acceso Inicial** (TA0001): Táctica de acceso inicial mediante la colocación de hardware adicional(T1200).
- **Keylogging** (T1056.001): Técnica de registrar pulsaciones de teclas para capturar credenciales de acceso.

Activo/Recurso en Riesgo:

- **Credenciales con Privilegios Elevados**: Credenciales obtenidas vía keylogging.
- **Formulas Únicas y Datos sensibles de la Empresa**: Información crítica y confidencial de las investigaciones y desarrollos de LongevityCorp.

Impacto Potencial:

- **Exfiltración de Información Sensible**: El empleado disconforme podría robar datos críticos, como las fórmulas únicas, y exfiltración a una ubicación externa.
- **Modificación o Eliminación de Información Crítica**: El empleado podría alterar o eliminar datos importantes, causando una pérdida significativa de información valiosa.
- **Impacto Monetario y Reputacional**: La pérdida o manipulación de datos críticas podría causar un gran impacto económico y dañar la reputación de LongevityCorp.

Detalles de la Hipótesis:

- **Acceso Inicial**:
  - El empleado disconforme instala un dispositivo de hardware en su estación de trabajo o en un área común, diseñado para registrar las pulsaciones de teclas.
  - El dispositivo de keylogging captura credenciales de acceso a sistemas con privilegios elevados.

- **Credenciales Robadas**:
  - Las credenciales robadas son usadas para acceder a sistemas internos y bases de datos de LongevityCorp.
- **Exfiltración de Información**:
  - El empleado usa las credenciales obtenidas para acceder a información crítica, como las fórmulas únicas de la empresa.
  - Los datos son exfiltrados a una ubicación externa controlada por el empleado disconforme.
- **Modificación/Eliminación de Datos**:
  - Además de exfiltrar información, el empleado podría modificar o eliminar datos críticos, afectando la integridad de los sistemas de LongevityCorp.

Resumen de la Hipótesis:

En esta hipótesis se plantea que el empleado disconforme podría instalar un dispositivo de hardware con funcionalidad de keylogging para capturar credenciales de acceso con privilegios elevados. Usando estas credenciales, el empleado podría acceder a datos sensibles, exfiltrarlos, y potencialmente modificar o eliminar información crítica de la empresa. Si se confirma esta hipótesis, La organización enfrentaría un gran impacto económico y reputacional.

Hipótesis 3: Baiting

Técnica Usada:

- **Baiting**: Uso de un cebo físico (USB) para atraer a las víctimas a realizar una acción que comprometa la seguridad.
- **Replicación vía medios removibles** (T1091): Técnica que implica la propagación de un programa malicioso vía medios extraíbles como dispositivos USB.

Activo/Recurso en Riesgo:

- **Dispositivos de la Organización**: Computadoras y sistemas en la red interna de LongevityCorp.

- **Red Interna**: La infraestructura de red de la organización que podría ser comprometida.

Impacto Potencial:

- **Instalación del programa malicioso**: Si un empleado conecta el dispositivo USB, el programa malicioso se descarga e instala puertas traseras en el sistema comprometido.
- **Exposición de la Red Interna**: La instalación de puertas traseras puede permitir al atacante acceder a la red interna de la organización.
- **Futuros Ataques**: Una vez comprometida, la red interna puede ser vulnerable a futuros ataques, como ransomware.

Detalles de la Hipótesis:

- **Táctica de Acceso Inicial** (cebo):
  - El atacante coloca el USB cerca de la entrada de la organización esperando que un empleado lo recoja y lo inserte en un dispositivo de la empresa.
- **Táctica Ejecución – TA0002** (Inserción del Dispositivo extraíble):
  - Si un empleado encuentra el USB y lo inserta en un dispositivo de la organización, este se ejecutará automáticamente el programa malicioso guardado en el USB.
- **Táctica Movimiento Lateral – TA0008** (Replicación vía Medios Extraíbles):
  - El programa malicioso se replica vía medios extraíbles (T1091), propagándose a otros dispositivos conectados a la misma red.
- **Táctica Persistencia – TA0003** (Backdoors):
  - El programa malicioso instala puertas traseras en el dispositivo comprometido, permitiendo al atacante acceso remoto continuo.
- **Táctica Movimiento Lateral y Exposición**:
  - El atacante usa las puertas traseras para moverse lateralmente vía red interna, comprometiendo más sistemas y recolectando datos sensibles.
- **Táctica Impacto – TA0040**:

- El acceso no autorizado y la instalación de puertas traseras exponen la red interna a futuros ataques, como ransomware, que pueden encriptar datos críticos y exigir rescates.

Resumen de la Hipótesis:

Esta hipótesis supone que un atacante podría usar la técnica de Baiting, colocando un USB malicioso cerca de la entrada de la organización. Si un empleado inserta el dispositivo en un equipo de la organización, el programa malicioso puede instalar puertas traseras, permitiendo al atacante acceso remoto continuo y exponiendo a la red interna a futuros ataques. Si se confirma esta hipótesis, la red estaría en riesgo de compromisos adicionales y posibles ataques de ransomware.

Hipótesis 4: Extorsión DDoS

Técnica Usada:

- Denegación de Servicio de Red (T1498).
- Sub-Técnica: Inundación directa de la red (T1498.001).

Activo/Recurso en Riesgo:

- **Servidor Web de LongevityCorp**: Servidor que ofrece servicios clave, como la venta por mayor de productos a farmacias.
- **Red interna y Conectividad**: Infraestructura de red que puede ver afectada por el ataque DDoS.

Impacto Potencial:

- **Inutilización del Servicio Web**: La página web de la organización podría volverse inaccesible debido a la sobrecarga del servidor.
- **Impacto Monetario**: La interrupción de servicios clave podría resultar en pérdidas económicas significativas, especialmente si afecta ventas y transacciones.
- **Daño a la reputación**: La inhabilidad para mantener el servicio en línea podría dañar la reputación de LongevityCorp, afectando la confianza de los clientes y socios comerciales.

- **Extorsión y Demanda de Rescate**: El atacante podría extorsionar a la organización, exigiendo un rescate a cambio de detener el ataque.

Descripción Detallada de la Hipótesis:

- **Táctica Reconocimiento**:
  - El atacante identifica que LongevityCorp tiene una postura débil en materia de seguridad informática, usando únicamente un filtro de paquetes sin estado (UDP).
- **Táctica Desarrollo de Recursos**:
  - El atacante prepara una botnet de gran tamaño para lanzar un ataque de Denegación de Servicio (DDoS) usando la técnica de inundación directa de la red (T1498.001).
- **Táctica Acceso Inicial-Lanzamiento del Ataque DDoS**:
  - El atacante inicia el ataque DDoS, inundando el servidor web de LongevityCorp con una gran cantidad de tráfico malicioso para sobrecargarlo y causar su caída.
- **Táctica Impacto**:
  - La página web de LongevityCorp se vuelve inaccesible debido al ataque.
  - La interrupción del servicio causa pérdidas económicas significativas y daña la reputación de la organización.
- **Táctica Impacto – Extorción**:
  - Aprovechando la situación, el atacante extorsiona a LongevityCorp, exigiendo un rescate a cambio de detener el ataque y restablecer el acceso al servicio.

Resumen de la Hipótesis:

La hipótesis sugiere que un atacante podría lanzar un ataque de Denegación de Servicio Distribuido (DDoS) contra el servidor web de LongevityCorp, aprovechando una postura débil en materia de seguridad informática. Si la organización no mejora sus medidas de defensa, el ataque DDoS podría inutilizar servicios clave, causando un gran impacto monetario y dañando la reputación de la empresa. Además, el atacante

podría extorsionar a LongevityCorp, exigiendo un rescate a cambio de cancelar el ataque.

Hipótesis 5: Explotación de Puertos

Técnica/Táctica usada:

- **Táctica Reconocimiento – TA0043**: Técnica de escaneo activo (T1595) para sondear la infraestructura de la víctima mediante tráfico de red.
- **Sub-Técnica Escaneo de Bloques IP** (T1595.001): Escaneo de bloques IP para identificar sistemas y servicios activos.
- **Sub-Técnica Análisis de vulnerabilidades** (T1595.002): Análisis de vulnerabilidades para revelar software, versiones y posibles fallos de seguridad explotables.

Activo/Recursos en Riesgo:

- **Servidor Windows Server 2008 R2**: Sistema con el puerto SMB 445 abierto.
- **Red Interna y Datos Sensibles**: Infraestructura de red y datos confidenciales de LongevityCorp.

Impacto Potencial:

- **Compromiso de Información Sensible**: El atacante podría acceder a información crítica y confidencial almacenada en el servidor.
- **Control Total del Servidor**: El atacante podría tomar control completo del servidor afectado, permitiendo movimiento lateral y acceso a otros sistemas en la red.
- **Violación de la Triada de Seguridad Informática** (Confidencialidad, Integridad, Disponibilidad): El compromiso del servidor afectaría a la confidencialidad, integridad y disponibilidad de los datos y sistemas de LongevityCorp.
- **Impacto Monetario y Legal**: Las pérdidas monetarias y los problemas legales asociados con la violación de datos podrían ser significativos.
- **Daño a la Reputación**: La exposición de datos sensibles y la falta de seguridad podría dañar la reputación de la LongevityCorp, afectando la confianza de clientes y socios comerciales.

Descripción de la Hipótesis:

- **Táctica Reconocimiento-Escaneo Activo**:
  - El atacante realiza un escaneo activo de la red de LongevityCorp (T1595) para identificar sistemas y servicios expuestos.
  - Usa la sub-técnica de escaneo de bloques ip (T1595.001) para identificar dispositivos en la red.
- **Táctica Reconocimiento-Análisis de vulnerabilidades**:
  - El atacante hace un análisis de vulnerabilidades (T1595.002) para identificar versiones de software y posibles fallos de seguridad en los dispositivos identificados.
  - Detecta que uno de los servidores es un Windows Server 2008 R2 con el puerto SMB 445 abierto.
- **Táctica Ejecución-Explotación de la Vulnerabilidad**:
  - El atacante usa la vulnerabilidad EternalBlue para explotar el puerto SMB 445 en el servidor comprometido.
  - Usando Metasploit, el atacante ejecuta el exploit para obtener acceso no autorizado al servidor.
- **Táctica Persistencia-Compromiso del Servidor**:
  - Una vez dentro del servidor, el atacante instala herramientas de persistencia para mantener el acceso y control total del sistema.
  - Puede moverse lateralmente a través de la red para comprometer otros sistemas y recolectar datos sensibles.
- **Táctica Impacto**:
  - El atacante puede exfiltrar datos confidenciales, modificar o eliminar información crítica y potencialmente inutilizar servicios clave.
  - La organización enfrenta pérdidas monetarias, problemas legales y un daño significativo a su reputación.

Resumen de la Hipótesis:

En esta hipótesis planteo que un atacante podría hacer un escaneo activo y un análisis de vulnerabilidades en la red de LongevityCorp para identificar sistemas expuestas y

fallos de seguridad. Aprovechando la vulnerabilidad EternalBlue en un servidor Windows Server 2008 R2 con el puerto 445 (SMB) abierto, el atacante podría tener acceso no autorizado, comprometiendo información sensible y tomando control total del servidor. Si esta hipótesis se confirma, la organización enfrentaría un impacto significativo en términos de seguridad, finanzas y reputación.

Parte 2

Creación de un Dataset simulado

Introducción de la parte 2

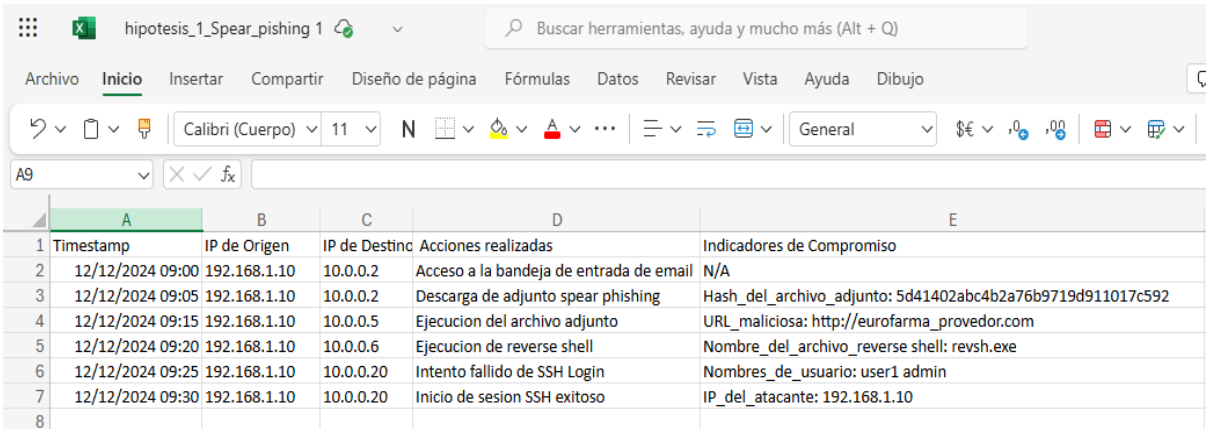
En esta parte 2 de la prueba diseñe para cada hipótesis un conjunto de Dataset simulado que incluirán:

- Timestamp
- IP de Origen
- IP de Destino
- Acciones realizadas
- Indicadores de Compromiso (IoCs).

Si bien los 5 Dataset comparten la misma estructura cada uno tiene datos específicos correspondiente a las hipótesis mencionadas en la parte 1 de la prueba.

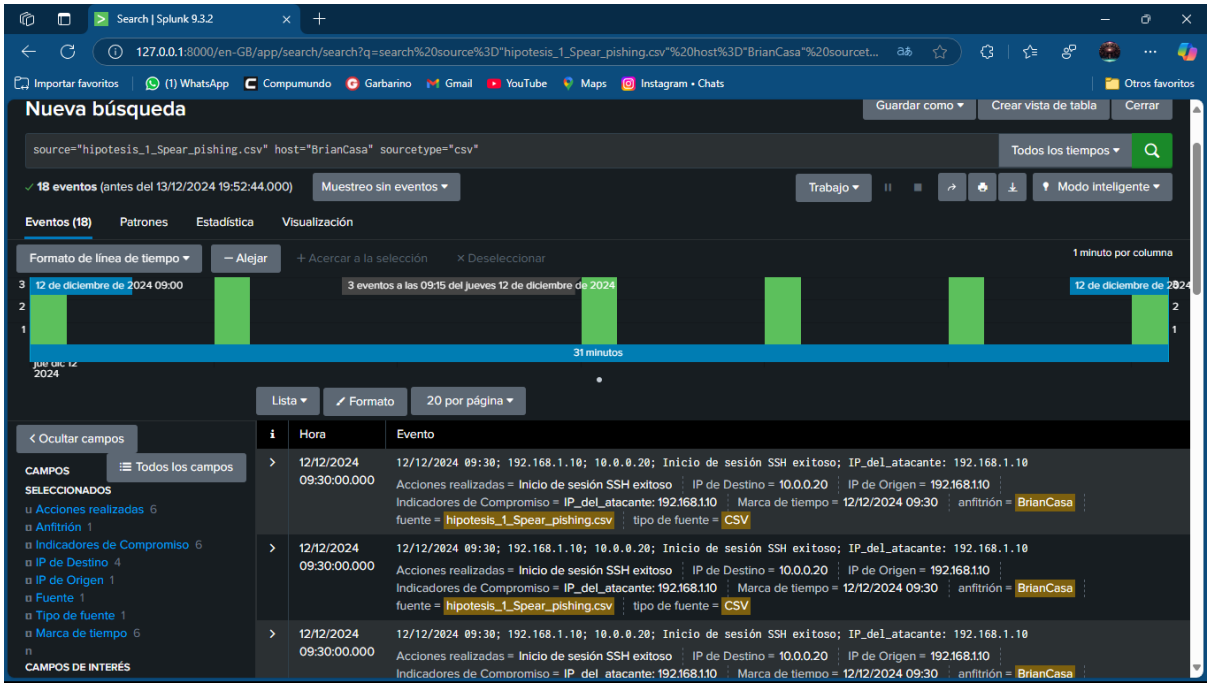
Capturas

Dataset Hipótesis 1 (Excel)

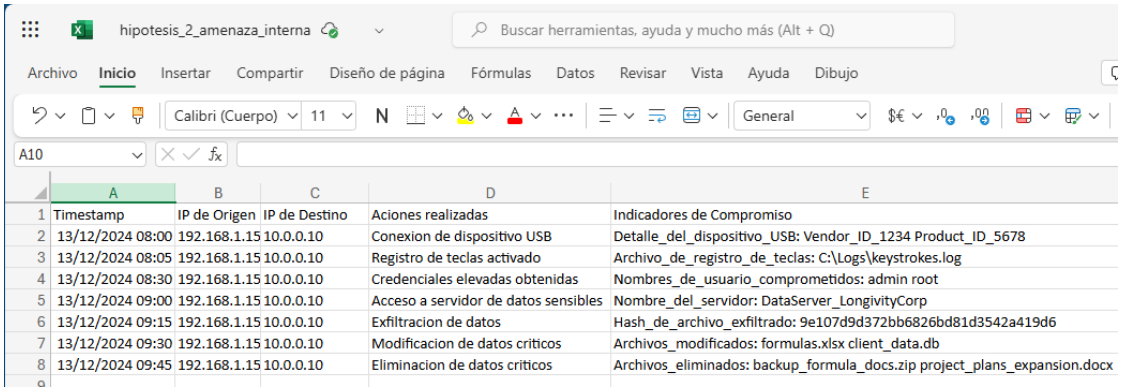


	A	B	C	D	E
1	Timestamp	IP de Origen	IP de Destino	Acciones realizadas	Indicadores de Compromiso
2	12/12/2024 09:00	192.168.1.10	10.0.0.2	Acceso a la bandeja de entrada de email	N/A
3	12/12/2024 09:05	192.168.1.10	10.0.0.2	Descarga de adjunto spear phishing	Hash_del_archivo_adjunto: 5d41402abc4b2a76b9719d911017c592
4	12/12/2024 09:15	192.168.1.10	10.0.0.5	Ejecucion del archivo adjunto	URL_maliciosa: http://eurofarma_provedor.com
5	12/12/2024 09:20	192.168.1.10	10.0.0.6	Ejecucion de reverse shell	Nombre_del_archivo_reverse shell: revsh.exe
6	12/12/2024 09:25	192.168.1.10	10.0.0.20	Intento fallido de SSH Login	Nombres_de_usuario: user1 admin
7	12/12/2024 09:30	192.168.1.10	10.0.0.20	Inicio de sesion SSH exitoso	IP_del_atacante: 192.168.1.10
8					

Dataset Hipótesis 1 (Splunk)

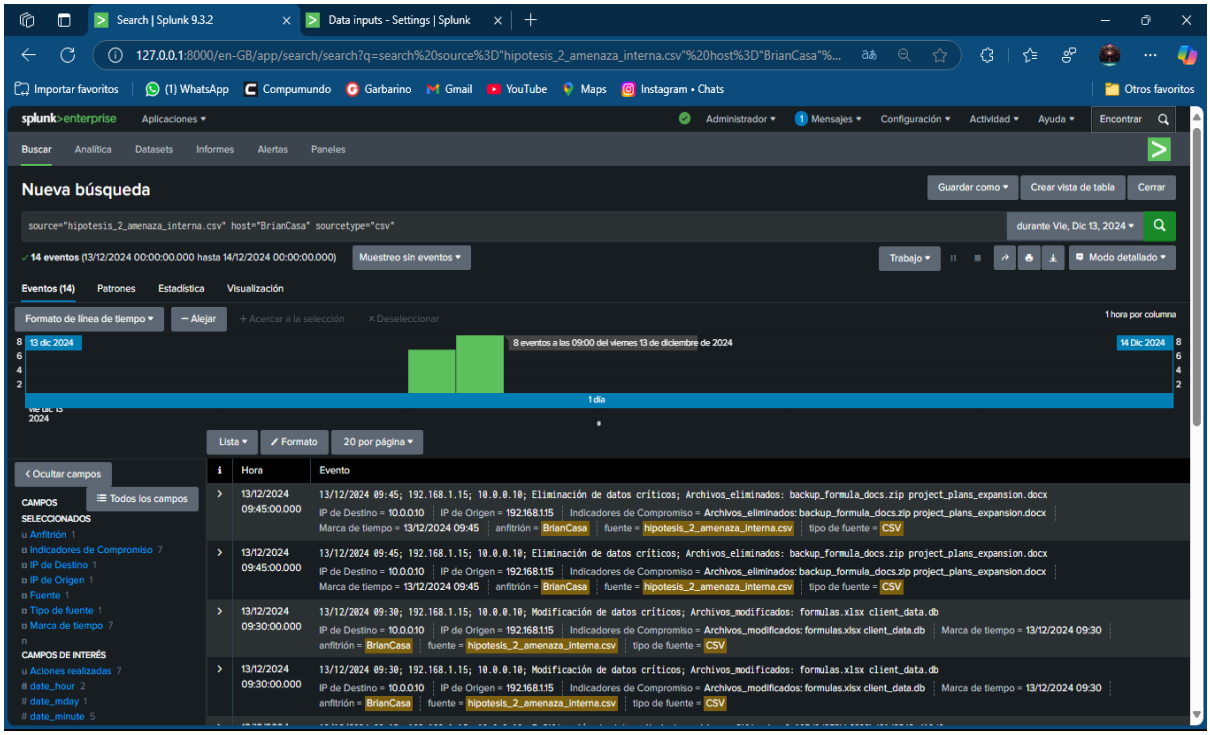


Dataset Hipótesis 2 (Excel)

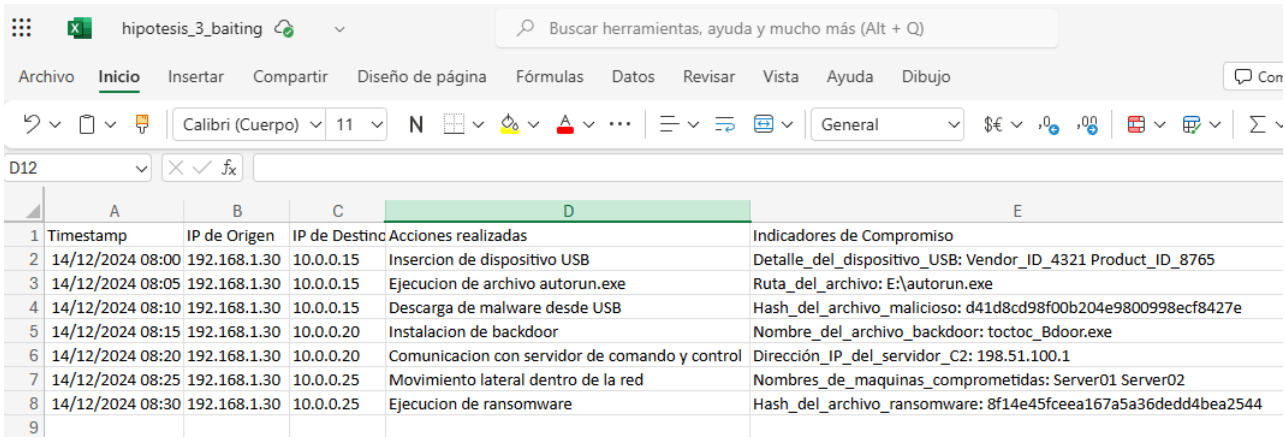


	A	B	C	D	E
1	Timestamp	IP de Origen	IP de Destino	Aciones realizadas	Indicadores de Compromiso
2	13/12/2024 08:00	192.168.1.15	10.0.0.10	Conexion de dispositivo USB	Detalle_del_dispositivo_USB: Vendor_ID_1234 Product_ID_5678
3	13/12/2024 08:05	192.168.1.15	10.0.0.10	Registro de teclas activado	Archivo_de_registro_de_teclas: C:\Logs\keystrokes.log
4	13/12/2024 08:30	192.168.1.15	10.0.0.10	Credenciales elevadas obtenidas	Nombres_de_usuario_comprometidos: admin root
5	13/12/2024 09:00	192.168.1.15	10.0.0.10	Acceso a servidor de datos sensibles	Nombre_del_servidor: DataServer_LongivityCorp
6	13/12/2024 09:15	192.168.1.15	10.0.0.10	Exfiltracion de datos	Hash_de_archivo_exfiltrado: 9e107d9d372bb6826bd81d3542a419d6
7	13/12/2024 09:30	192.168.1.15	10.0.0.10	Modificacion de datos criticos	Archivos_modificados: formulas.xlsx client_data.db
8	13/12/2024 09:45	192.168.1.15	10.0.0.10	Eliminacion de datos criticos	Archivos_eliminados: backup_formula_docs.zip project_plans_expansion.docx

Dataset Hipótesis 2 (Splunk)

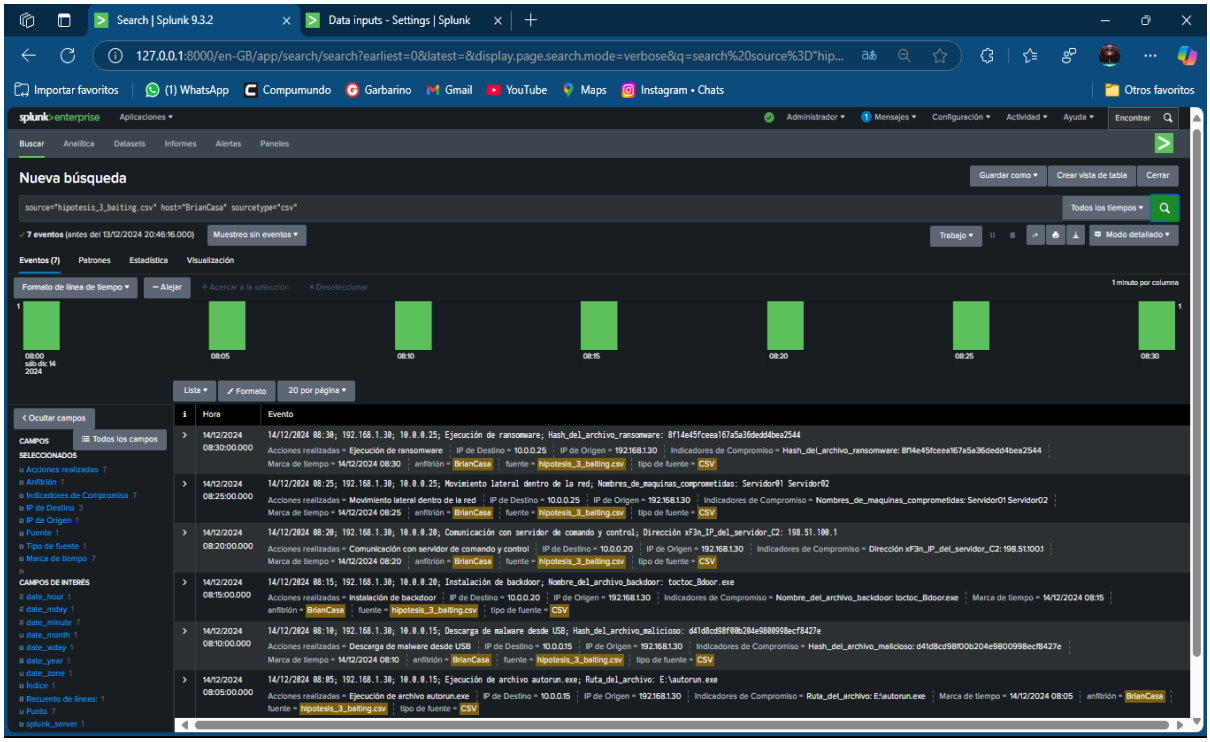


Dataset hipótesis 3 (Excel)

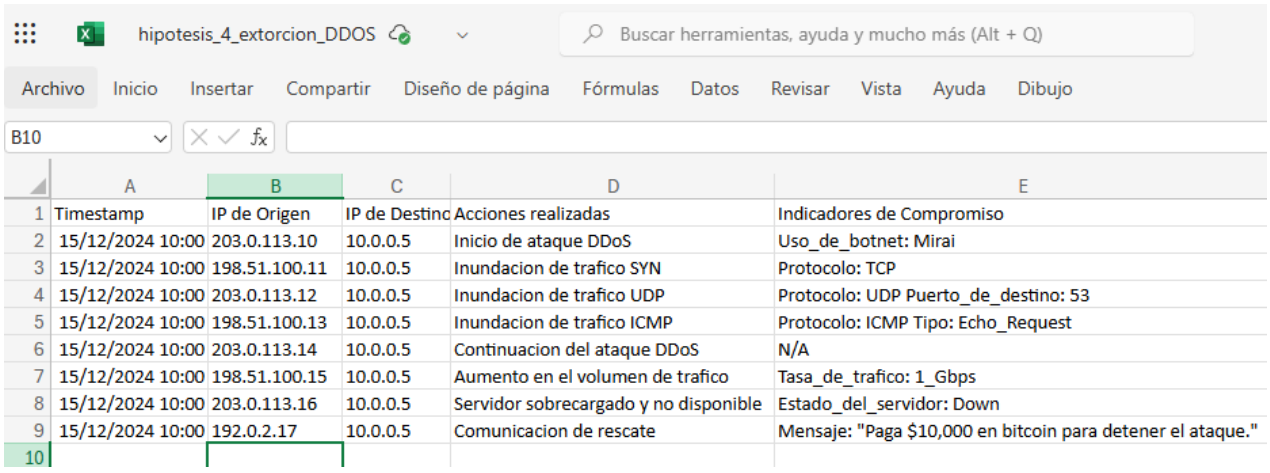


	A	B	C	D	E
1	Timestamp	IP de Origen	IP de Destino	Acciones realizadas	Indicadores de Compromiso
2	14/12/2024 08:00	192.168.1.30	10.0.0.15	Insercion de dispositivo USB	Detalle_del_dispositivo_USB: Vendor_ID_4321 Product_ID_8765
3	14/12/2024 08:05	192.168.1.30	10.0.0.15	Ejecucion de archivo autorun.exe	Ruta_del_archivo: E:\autorun.exe
4	14/12/2024 08:10	192.168.1.30	10.0.0.15	Descarga de malware desde USB	Hash_del_archivo_malicioso: d41d8cd98f00b204e9800998ecf8427e
5	14/12/2024 08:15	192.168.1.30	10.0.0.20	Instalacion de backdoor	Nombre_del_archivo_backdoor: toctoc_Bdoor.exe
6	14/12/2024 08:20	192.168.1.30	10.0.0.20	Comunicacion con servidor de comando y control	Dirección_IP_del_servidor_C2: 198.51.100.1
7	14/12/2024 08:25	192.168.1.30	10.0.0.25	Movimiento lateral dentro de la red	Nombres_de_maquinas_comprometidas: Server01 Server02
8	14/12/2024 08:30	192.168.1.30	10.0.0.25	Ejecucion de ransomware	Hash_del_archivo_ransomware: 8f14e45fceea167a5a36dedd4bea2544
9					

Dataset hipótesis 3 (Splunk)

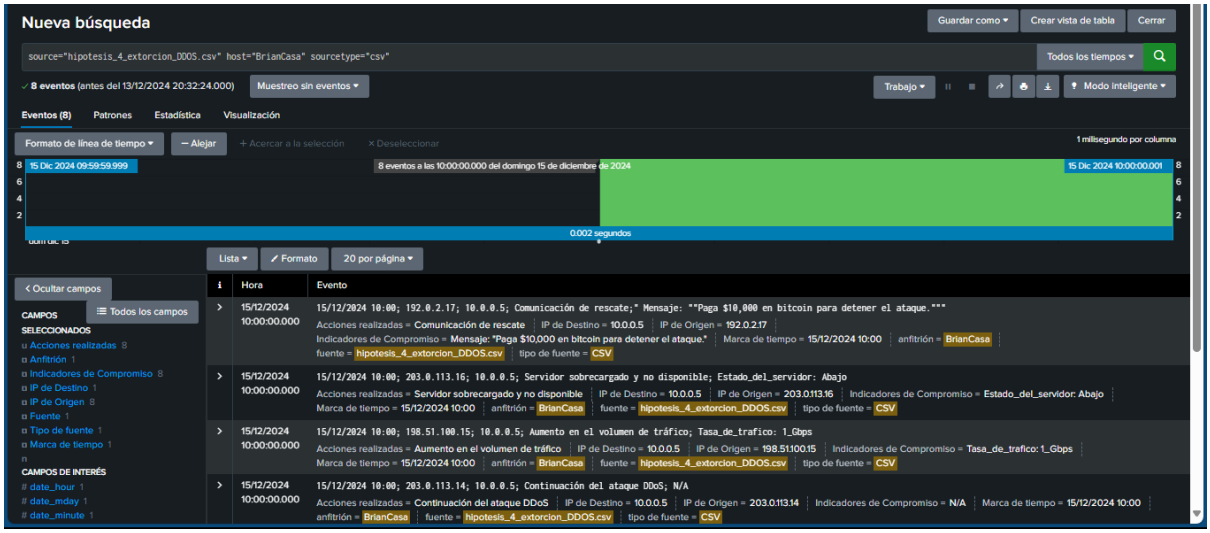


Dataset hipótesis 4 (Excel)

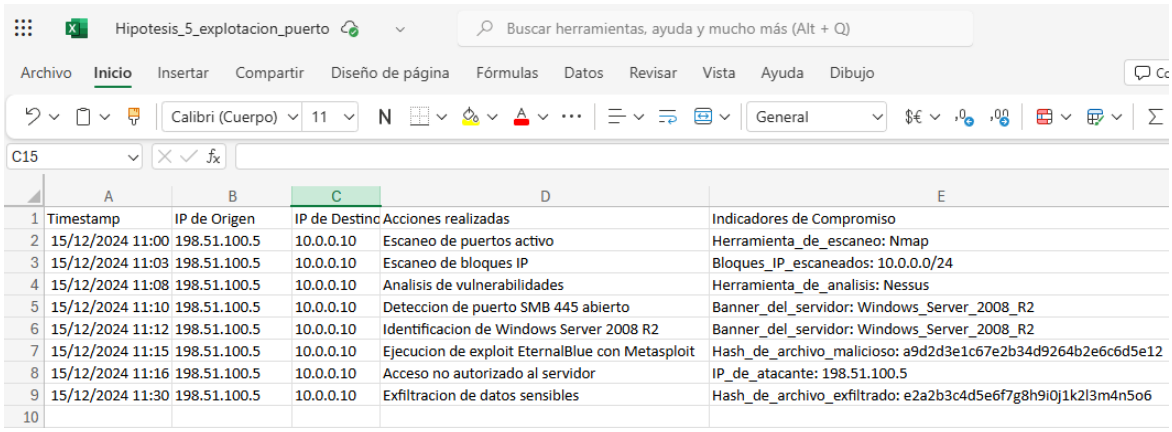


	A	B	C	D	E
1	Timestamp	IP de Origen	IP de Destino	Acciones realizadas	Indicadores de Compromiso
2	15/12/2024 10:00	203.0.113.10	10.0.0.5	Inicio de ataque DDoS	Uso_de_botnet: Mirai
3	15/12/2024 10:00	198.51.100.11	10.0.0.5	Inundacion de trafico SYN	Protocolo: TCP
4	15/12/2024 10:00	203.0.113.12	10.0.0.5	Inundacion de trafico UDP	Protocolo: UDP Puerto_de_destino: 53
5	15/12/2024 10:00	198.51.100.13	10.0.0.5	Inundacion de trafico ICMP	Protocolo: ICMP Tipo: Echo_Request
6	15/12/2024 10:00	203.0.113.14	10.0.0.5	Continuacion del ataque DDoS	N/A
7	15/12/2024 10:00	198.51.100.15	10.0.0.5	Aumento en el volumen de trafico	Tasa_de_trafico: 1_Gbps
8	15/12/2024 10:00	203.0.113.16	10.0.0.5	Servidor sobrecargado y no disponible	Estado_del_servidor: Down
9	15/12/2024 10:00	192.0.2.17	10.0.0.5	Comunicacion de rescate	Mensaje: "Paga $10,000 en bitcoin para detener el ataque."
10					

Dataset hipótesis 4 (Splunk)

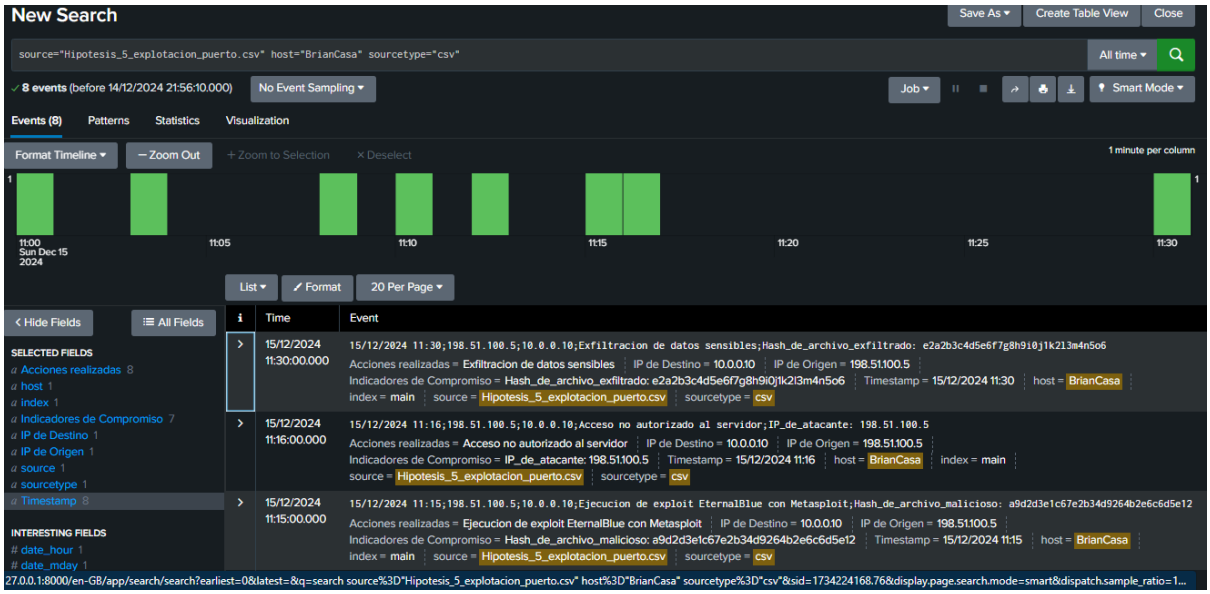


Dataset hipótesis 5 (Excel)



	A	B	C	D	E
1	Timestamp	IP de Origen	IP de Destino	Acciones realizadas	Indicadores de Compromiso
2	15/12/2024 11:00	198.51.100.5	10.0.0.10	Escaneo de puertos activo	Herramienta_de_escaneo: Nmap
3	15/12/2024 11:03	198.51.100.5	10.0.0.10	Escaneo de bloques IP	Bloques_IP_escaneados: 10.0.0.0/24
4	15/12/2024 11:08	198.51.100.5	10.0.0.10	Analisis de vulnerabilidades	Herramienta_de_analisis: Nessus
5	15/12/2024 11:10	198.51.100.5	10.0.0.10	Deteccion de puerto SMB 445 abierto	Banner_del_servidor: Windows_Server_2008_R2
6	15/12/2024 11:12	198.51.100.5	10.0.0.10	Identificacion de Windows Server 2008 R2	Banner_del_servidor: Windows_Server_2008_R2
7	15/12/2024 11:15	198.51.100.5	10.0.0.10	Ejecucion de exploit EternalBlue con Metasploit	Hash_de_archivo_malicioso: a9d2d3e1c67e2b34d9264b2e6c6d5e12
8	15/12/2024 11:16	198.51.100.5	10.0.0.10	Acceso no autorizado al servidor	IP_de_atacante: 198.51.100.5
9	15/12/2024 11:30	198.51.100.5	10.0.0.10	Exfiltracion de datos sensibles	Hash_de_archivo_exfiltrado: e2a2b3c4d5e6f7g8h9i0j1k2l3m4n5o6
10					

Dataset hipótesis 5 (Splunk)



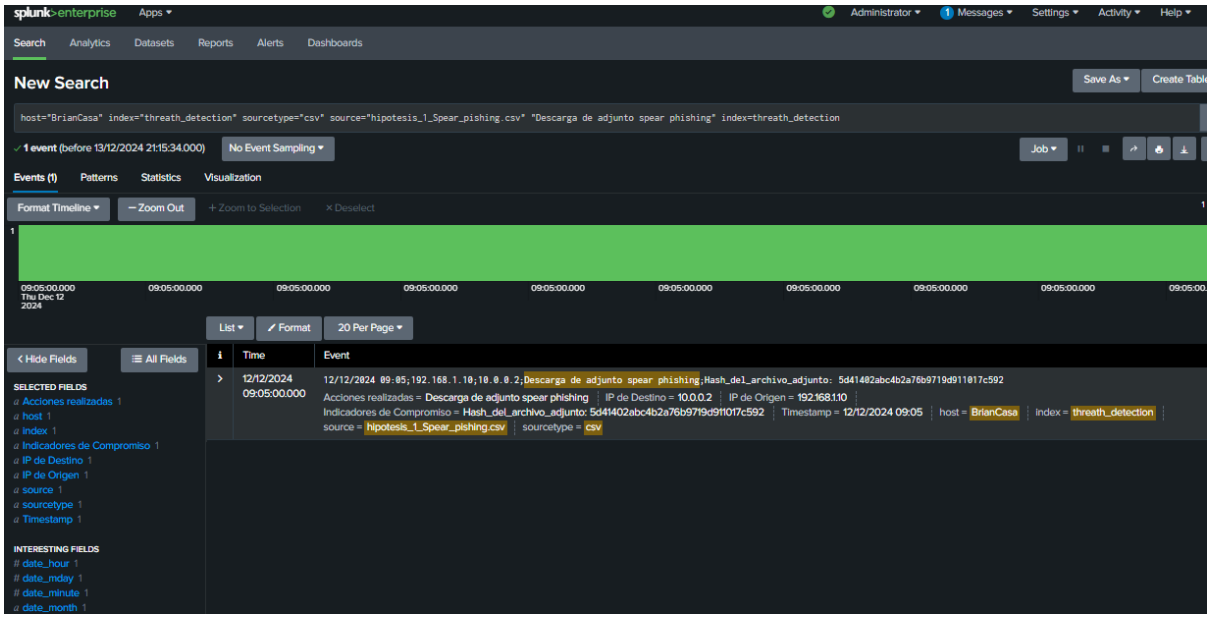
Parte 3

Introducción de la parte 3

En la parte 3 de la prueba la trabaje sobre la detección de una amenaza de la hipótesis 1, 2, 3, 4, 5.

Reporte de la amenaza de la hipótesis 1

Captura de pantalla de la amenaza en Splunk.



Análisis del incidente detectado en Splunk.

Detalles del evento:

- Descripción del evento: Descarga de adjunto spear-phishing.
- Fecha y Hora: 12/12/2024 09:05:00.
- IP de Destino: 10.0.0.2.
- IP de Origen: 192.168.1.10.
- Hash del Archivo Adjunto: 5d41402abc4b2a76b9719d911017c592.
- Fuente del Archivo: 18ipótesis_1_Spear_phishing.csv.
- Host: BrianCasa.
- Índice: threath_detection

Descripción del Ataque:

Este evento muestra que un correo spear-phishing ha sido exitosamente descargado por el usuario con la IP de destino 10.0.0.2. El correo contenía un archivo adjunto con el hash indicado, el cual probablemente sea un archivo malicioso.

Indicadores de Compromiso (IoCs):

- IP de Origen: 192.168.1.10 (Atacante).
- IP de Destino: 10.0.0.2 (Usuario comprometido).
- Hash del Archivo Malicioso: 5d41402abc4b2a76b9719d911017c592.

Impacto potencial:

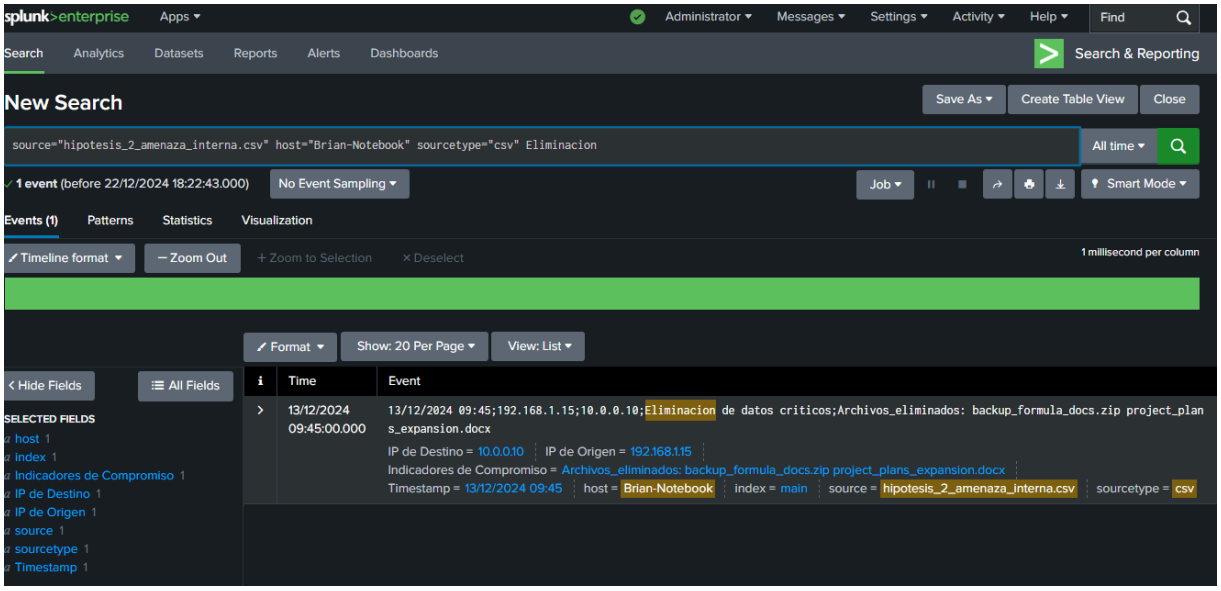
- **Acceso No Autorizado**: Si el archivo adjunto fue ejecutado, podría haber dado al atacante acceso a la red interna.
- **Robo de Información Confidencial**: Posible exfiltración de datos sensibles.
- **Interrupción de Operaciones**: El atacante podría usar el acceso para interrumpir operaciones críticas.

Recomendaciones para Mitigar la Amenaza:

1. **Implementación de Políticas de Seguridad de Correo Electrónico**:
   - Usar soluciones de correo electrónico seguro que escaneen y filtren correos sospechosos antes de que lleguen a los usuarios.
2. **Autenticación Multifactor** (MFA):
   - Implementar MFA para accesos críticos, lo cual añadiría una capa adicional de seguridad.
3. **Capacitación de Empleados**:
   - Hacer capacitaciones periódicas para que los empleados puedan identificar y reportar correos de phishing.
4. **Monitorización Continua**:
   - Usar herramientas de monitoreo continuo para detectar accesos no autorizados y responder rápidamente.
5. **Análisis Forenses**:
   - Hacer un análisis forense del hash del archivo malicioso y cualquier otra actividad inusual desde la IP comprometida.

Reporte de la Amenaza de la Hipótesis 2

Captura de pantalla de la amenaza de la amenaza en Splunk.



Análisis del Incidente Detectado

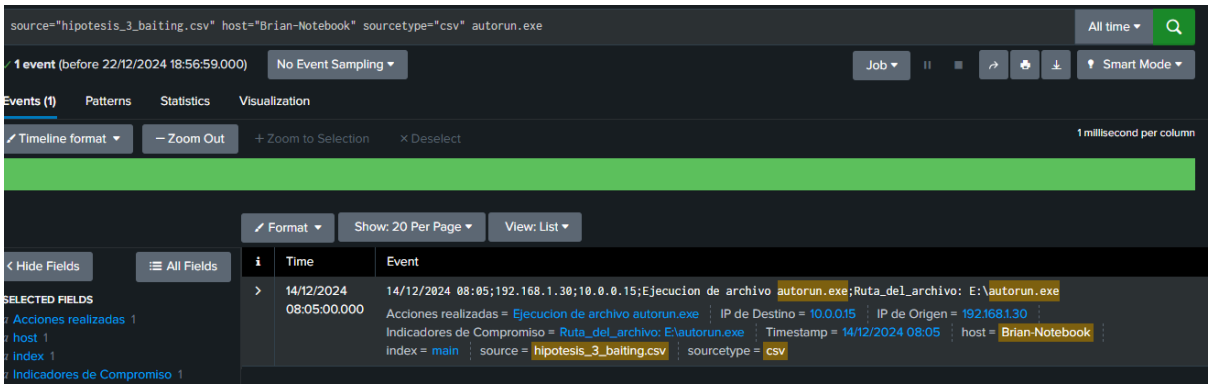
- **Descripción**: El incidente detectado involucra la eliminación de archivos críticos el sistema. Esta acción podría ser un intento de sabotaje o un error humano que resulta en la pérdida de datos importantes.
- **Impacto Potencial**: La eliminación de archivos críticos puede llevar a la pérdida de información valiosa, interrupción de operaciones y potencial daño a la reputación de la empresa si los datos son irrecuperables.
- **Fuentes**: El evento se originó desde la IP 192.168.1.15, que podría ser una estación de trabajo comprometida o un empleado interno con intenciones maliciosas.

Recomendaciones para Mitigar la Amenaza

- **Implementar Políticas de Acceso y Control**: Restringir el acceso a archivos críticos al personal autorizado y usar controles de acceso basados en roles.
- **Monitoreo y Registro de Actividades**: Configurar sistemas de monitoreo continuo para registrar todas las actividades de acceso y modificación de archivos críticos.

- **Capacitación**: Proveer capacitación continua a los empleados sobre la importancia de la seguridad de los datos y como reconocer intentos de sabotaje.
- **Implementar Copias de Seguridad Regulares**: Asegurarse que haya copias de seguridad regulares y verificadas de todos los datos críticos para facilitar la recuperación en caso de eliminación accidental o intencional.

Reporte de la Amenaza de la Hipótesis 3



Análisis del Incidente Detectado

- **Descripción**: El incidente detectado involucra la ejecución de un archivo autorun.exe desde un dispositivo USB. Esto indica un posible caso de Baiting, donde un empleado curioso usa un USB infectado que encontró introduciendo sin darse cuenta un malware en el sistema.
- **Impacto Potencial**:
  - **Instalación de Programa Malicioso**: La ejecución de archivos autorun.exe desde dispositivos USB puede llevar a la instalación de malware, robo de datos, y comprometer la seguridad del sistema.
  - **Exposición de la Red Interna**: Si el malware instala puertas traseras, puede permitir al atacante acceder a la red interna de la organización.
  - **Futuros Ataques**: La red interna comprometida puede ser vulnerable a futuros ataques, como ransomware, una vez que las puertas traseras están instaladas.
- **Fuentes**: El ataque se originó desde la IP 192.168.1.30, lo que sugiere que el dispositivo USB infectado fue conectado a esa estación de trabajo.

Recomendaciones para Mitigar la Amenaza

- **Deshabilitar Autorun**: Configurar los sistemas para deshabilitar la ejecución automática de archivos desde dispositivos USB. Ej: usando la política de grupo de Windows
- **Implementar Políticas de Uso de Dispositivos USB**: Restringir el uso de dispositivos USB no autorizados y proporcionar dispositivos USB seguros y verificados para el personal. Ej: Endpoint Protector es una solución DLP que permite controlar y monitorear el uso de dispositivos USB. Otra solución es McAfee Device Control que gestiona y controla el acceso a dispositivos extraíbles y de almacenamiento, asegurando que solo dispositivos autorizados puedan conectarse.
- **Escaneo y Monitoreo de Dispositivos USB**: Usar software de seguridad que escanee automáticamente los dispositivos USB al ser conectados y monitoree la actividad en tiempo real para detectar comportamientos sospechosos. Ej: Symantec EndPoint Protection es una solución que da protección avanzada contra malware y escanea automáticamente dispositivos USB cuando se conectan al sistema. Sophos Intercept X es otra solución que detecta y bloquea amenazas provenientes de dispositivos USB y da reportes detallados de las actividades de los dispositivos conectados.
- Capacitación: Proveer capacitación a los empleados sobre los riesgos del uso de dispositivos USB no verificados y cómo manejarlos de manera segura.

Reporte de la Amenaza de la Hipótesis 4

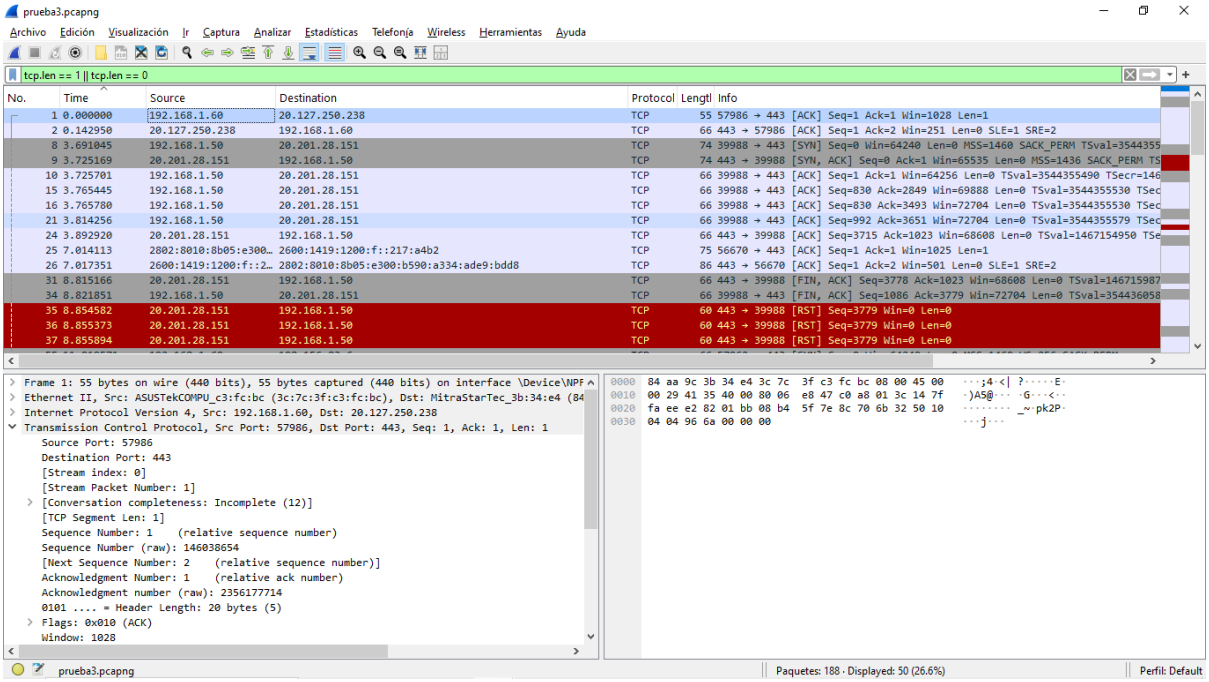
Introducción del reporte:

Si bien esta hipótesis tiene su propio Dataset cargado en Splunk (visto en la parte 2 de esta prueba), solo para hacer un reporte más gráfico simulé un ataque DoS usando Slowloris en un entorno controlado tomando una de las técnicas conocida como TCP flood lo cual, en resumen, trata de inundar el servidor con paquetes tcp muy pequeños con conexiones incompletas con el propósito de dejarlas abiertas y así denegar el servicio, todo lo capturé en vivo con Wireshark. Para lograr dicha simulación use una

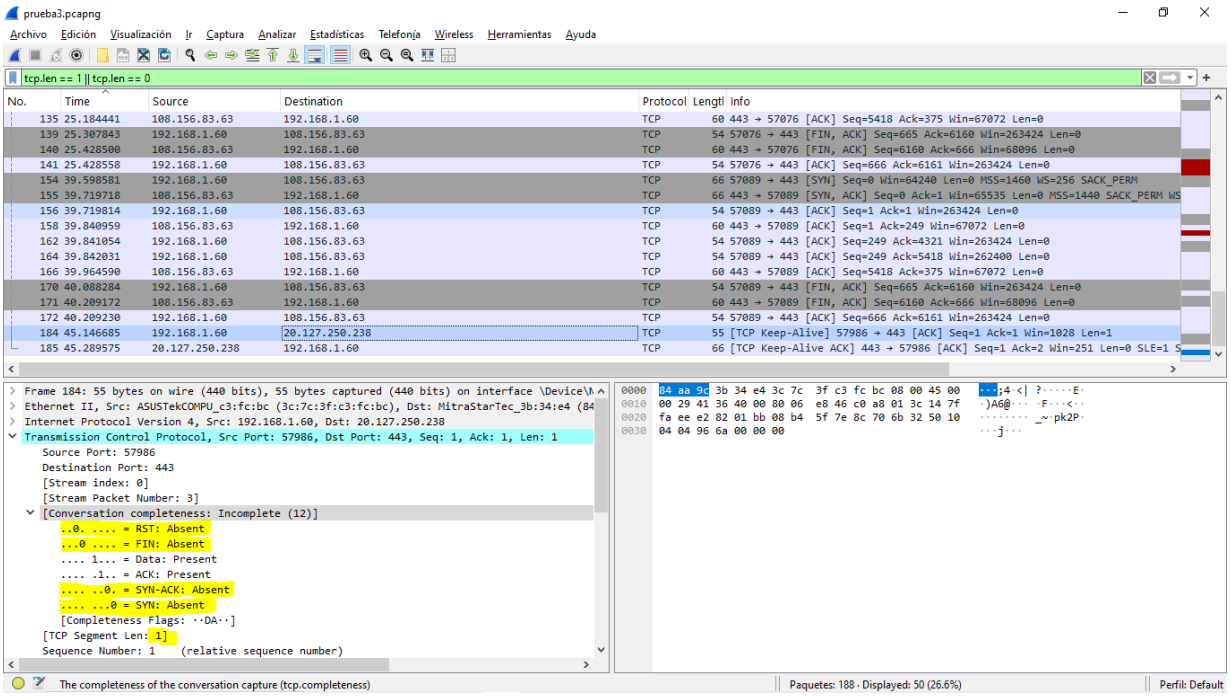
máquina virtual con Sistema Operativo Kali Linux (rol de adversario) y mi maquina host windows 11 (rol de servidor) usando DVWA con XAMPP.

Capturas de la amenaza DoS en Wireshark.

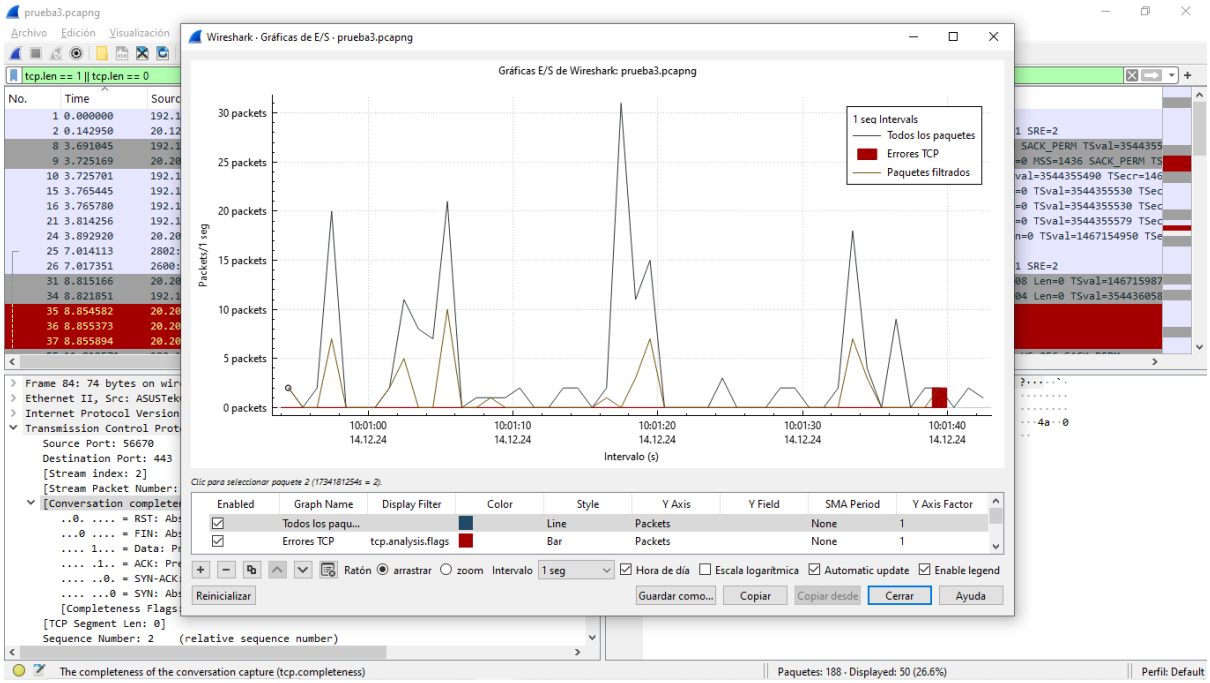
Captura A: Paquetes con longitud de segmento TCP inusual



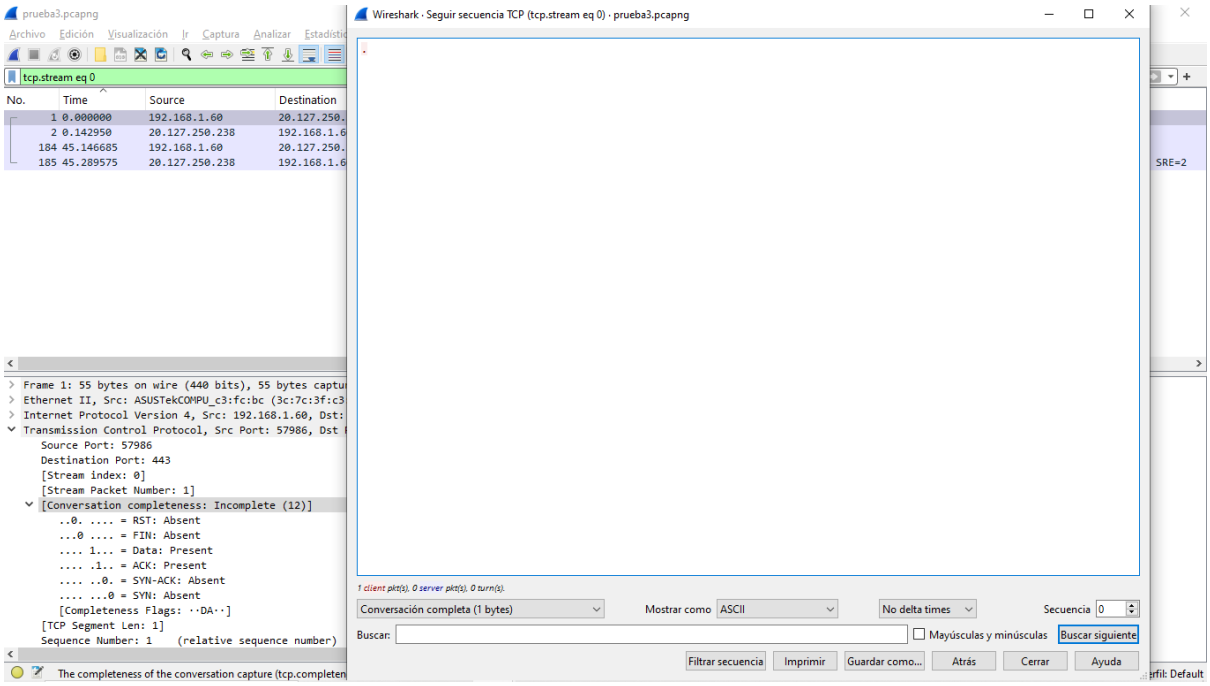
Captura B: paquetes con conexiones incompletas



Captura C: Gráfico



Captura D: paquetes de conexión incompleta sin conversación entre cliente y servidor.



Análisis del Ataque Slowloris en Wireshark

Detalles del ataque:

1. **Paquetes Pequeños y Múltiples Conexiones**:
   - Filtro aplicado: tcp.leng == 1 || tcp.leng == 0.
   - Identifica los paquetes TCP con longitudes de 1 o 0 bytes, que son característicos de Slowloris.
   - Paquete 184: Tiene un mensaje clave de “TCP Keep-Alive” y longitud de segmento de 1 byte.
2. **Gráfico de E/S**:
   - Picos de actividad en el número de paquetes por segundo y errores TCP, indicando sobrecarga del servidor.
   - La gráfica confirma la presencia de una alta carga de tráfico y errores durante el ataque
3. **Seguimiento de la Secuencia TCP**:
   - Las conexiones seguidas (como la del paquete 184) muestran que las conversaciones están vacías, lo que es típico de Slowloris, donde las conexiones se mantienen abiertas, pero no transfieren datos completos.

Impacto del Ataque:

- **Inaccesibilidad del Servidor Web**: El ataque puede dejar el servidor web de LongevityCorp inaccesible debido a la sobrecargar de conexiones.
- **Recursos del Servidor Agotados**: El servidor intenta mantener múltiples conexiones incompletas, consumiendo sus recursos y degradando su rendimiento.

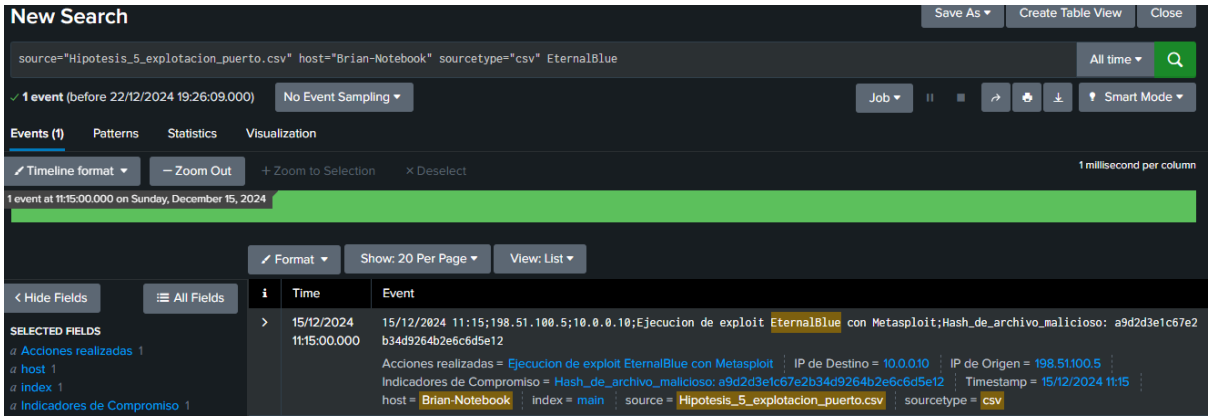
Recomendaciones para Mitigar el Ataque Slowloris:

1. **Configuración de Limites de Conexión**:
   - Ajustar los límites de tiempo de espera para conexiones incompletas.
   - Implementar límites en el número de conexiones simultáneas desde una misma IP.
2. **Uso de Herramientas de Mitigación DoS**:

- Implementar soluciones que puedan identificar y bloquear tráfico característico de ataques Slowloris.

3. **Monitorización y Alerta**:
   - Implementar sistemas de monitoreo continuo que detecten patrones de tráfico inusuales y generen alertas tempranas.
   - Usar herramientas como Wireshark para análisis forenses continuo y para identificar potenciales amenazas.
4. **Fortalecer la Seguridad del Servidor Web**:
   - Asegurarse de que todas las aplicaciones web y servidores estén actualizados con los últimos parches de seguridad.
   - Configurar las reglas de firewall adecuadas para bloquear tráfico malicioso.

Reporte de la Amenaza de la Hipótesis 5



Análisis del Incidente Detectado

- **Descripción**: El incidente detectado involucra la explotación de la vulnerabilidad **EternalBlue** en un servidor Windows Server R2 2008 con el puerto SMB 445 abierto. Esto indica que el atacante usó Metasploit para ejecutar el exploit y obtener acceso no autorizado al servidor.

Impacto Potencial:

- **Compromiso de Información Sensible**: El atacante podría acceder a información crítica y confidencial almacenada en el servidor.

- **Control Total del Servidor**: El atacante podría tomar control completo del servidor afectado, permitiendo movimiento lateral y acceso a otros sistemas en la red.
- **Violación de la Triada CIA** (Confidencialidad, Integridad y Disponibilidad): El compromiso del servidor afectaría la confidencialidad, disponibilidad e integridad de los datos y sistemas de LongevityCorp.
- **Impacto Monetario y Legal**: Las pérdidas monetarias y los problemas legales asociados con la violación de datos podrían ser significativos.
- **Daño a la Reputación**: La exposición de datos sensibles y la falta de seguridad podría dañar la reputación de LongevityCorp, afectando la confianza de clientes y socios comerciales.

Recomendaciones para Mitigar la Amenaza

- **Actualizar y Parchear Sistemas**: Asegurarse de que todos los sistemas y software estén actualizados con los últimos parches de seguridad para evitar la explotación de vulnerabilidades conocidas como EternalBlue.
- **Deshabilitar Servicios Innecesarios**: Deshabilitar servicios no esenciales, como SMB, en los servidores que no los requieran, para reducir la superficie de ataque.
- **Implementar Firewalls y Filtrado de Tráfico**: Configurar firewalls y sistemas de prevención de intrusos (IPS) para filtrar tráfico y bloquear intentos de escaneo y explotación de puertos.
- **Escaneo Regular de Vulnerabilidades**: Usar herramientas como Nessus o OpenVas para hacer escaneos regulares de vulnerabilidades y corregir fallos de seguridad.
- **Monitoreo Continuo de la Red**: Implementar soluciones de monitoreo continuo, como Splunk o ELK Stack, para detectar y responder rápidamente a actividades sospechosas y posibles intrusiones.

Parte 4

INFORME

Introducción

En esta última parte de la prueba haré un informe donde menciono las hipótesis presentadas y cómo fueron desarrolladas. Para evitar ser repetitivo, todas las hipótesis las pensé en las características de LongevityCorp y lo que ofrece. Estas hipótesis están diseñadas para analizar proactivamente posibles amenazas en ciberseguridad y mejorar la postura de seguridad de la organización.

1-Hipótesis presentadas y su desarrollo:

Las hipótesis presentadas son cinco (5):

- **Hipótesis 1 Phishing**:
  - ❖ Esta hipótesis está basada en la probabilidad de que los empleados pueden cometer descuidos de mostrar su lugar de trabajo, rol dentro de la organización e instalaciones de la organización en redes sociales siendo un buen objetivo de phishing dirigido. De esta manera, investigando, fue que he creado esta hipótesis considerando el impacto potencial y las tácticas/técnicas del marco MITRE ATT&CK.
- **Hipótesis 2 Amenaza Interna**:
  - ❖ Esta hipótesis la trabaje basándome en dos situaciones:
    1. Un empleado insatisfecho con la organización podría abusar de la confianza y robar información sensible como “venganza”.
    2. Un mal manejo de la desvinculación laboral podría resultar en un empleado disconforme que busque hacer daño a la organización. Investigando en el marco MITRE ATT&CK, encontré tácticas para instalar hardware de registro de teclas (keylogger) y examinar las posibles consecuencias.
- **Hipótesis 3 Baiting**:
  - ❖ Esta hipótesis la elaboré pensando más en la posibilidad de que el atacante quiera sacar provecho a la curiosidad de las personas colocando

estratégicamente un dispositivo USB cerca de la organización para comprometer la seguridad de la red misma.

- **Hipótesis 4 Extorsión DDoS**:
  - ❖ Esta hipótesis la elaboré pensando en que siendo una empresa innovadora que trabaja con proveedores y depende de la disponibilidad de su sitio web, una posible amenaza es un ataque DDoS que comprometa la disponibilidad del servicio, aprovechando una postura de seguridad débil para extorsionar a la organización por una buena cantidad de dinero.
- **Hipótesis 5 Explotación de Puertos**:
  - ❖ Esta hipótesis la hice evaluando el supuesto caso que la organización tuviera una postura débil de seguridad informática, sistemas operativos antiguos los cuales con un escaneo de puertos se puede llegar a la explotación de vulnerabilidades conocidas como EternalBlue en Windows Server 2008 R2

2-Detalles sobre el Dataset creado y su Relación con las Hipótesis

Introducción

En esta sección se presentan los detalles sobre los datasets simulados que fueron creados para apoyar el análisis de cada hipótesis. Cada Dataset incluye información relevante como Timestamp, IP de origen, IP de destino, acciones realizadas e indicadores de compromiso (IoCs). Estos datos se relacionan directamente con los eventos descritos en las hipótesis y ayudan a identificar y analizar las amenazas potenciales.

Estructura Común de los Datasets

Todos los Datasets creados para las cinco hipótesis comparten la misma estructura. Esto permite una consistencia en el análisis y facilita la comparación de los diferentes escenarios de amenaza. La estructura común incluye los siguientes campos:

- Timestamp: Fecha y hora en que ocurrieron los eventos.
- IP de Origen: Dirección IP del atacante o dispositivo comprometido.

- IP de Destino: Dirección IP del objetivo dentro de la organización.
- Acciones Realizadas: Descripción de las acciones realizadas durante el evento.
- Indicadores de Compromiso: Identificadores clave como hashes de archivos maliciosos, direcciones de correo usadas y vulnerabilidades explotadas.

Hipótesis 1: Phishing

Archivo: Hipótesis_1_spear_phishing.csv

- Descripción del Dataset: Este Dataset refleja los eventos y actividades relacionados con un ataque de spear-phishing, incluyendo la apertura del correo y la ejecución del archivo malicioso.
- Relación con la Hipótesis: Ayuda a analizar el patrón de ataque y las tácticas usadas en un escenario de spear-phishing dirigido a empleados específicos.

Hipótesis 2: Amenaza Interna

Archivo: Hipótesis_2_Amenaza_Interna.csv

- Descripción del Dataset: simula eventos internos no autorizados donde un empleado disconforme instala un keylogger y accede a información sensible.
- Relación con la Hipótesis: Permite analizar las acciones del empleado insatisfecho y su impacto en la seguridad de la organización.

Hipótesis 3: Baiting

Archivo: Hipótesis_3_Baiting.csv

- Descripción del Dataset: Refleja los eventos y actividades relacionadas con la técnica de Baiting usando un dispositivo USB malicioso.
- Relación con la Hipótesis: Ayuda a analizar cómo el programa malicioso se propaga y afecta la red interna.

Hipótesis 4: Extorsión DDoS

Archivo: Hipotesis_4_Extorsión_DdoS.csv

- Descripción del Dataset: Captura el tráfico anómalo durante un ataque DDoS simulado, incluyendo las fuentes del tráfico malicioso.

- Relación con la Hipótesis: Permite analizar la efectividad del ataque DDoS y las posibles medidas de mitigación.

Hipótesis 5: Explotación de Puertos

Archivo: Hipótesis_5_Explotacion_puertos.csv

- Descripción del Dataset: Refleja los eventos relacionados con el escaneo de puertos y la explotación de vulnerabilidades.
- Relación con la hipótesis: Ayuda a analizar cómo un atacante puede identificar y explotar puntos débiles en la red de LongevityCorp.

3-Resultados del Análisis y Conclusiones

Hipótesis 1: Phishing

Resultados del Análisis:

- Detección en Splunk: Se identificó un evento de spear-phishing donde un correo malicioso fue enviado a un empleado específico. El análisis mostró la apertura del correo y la ejecución del archivo adjunto, confirmando un compromiso inicial.
- Indicadores de Compromiso (IoCs):
  - ❖ IP de Origen: 192.168.1.10 (atacante).
  - ❖ IP de Destino: 10.0.0.2 (usuario comprometido).
  - ❖ Hash del archivo Malicioso: 5d41402abc4b2a76b9719d911017c592

Conclusiones

Este análisis confirmó que los empleados de LongevityCorp son vulnerables a ataques de spear-phishing debido a la falta de concienciación sobre la seguridad. Es importante implementar medidas de capacitación y usar herramientas de detección/prevención de phishing para mitigar esta amenaza

Hipótesis 2: Amenaza interna

Resultados del Análisis:

- Detección en Splunk: Los eventos simulados mostraron que un empleado insatisfecho podría instalar un keylogger y capturar credenciales críticas. Este análisis revela accesos no autorizados a sistemas internos usando dichas credenciales.

- Indicadores de Compromiso (IoCs):
  - ❖ IP de Origen: 192.168.2.15 (empleado disconforme).
  - ❖ IP de Destino: 10.0.0.3 (sistema interno).
  - ❖ Credenciales robadas: Usuario y Contraseñas capturadas por el keylogger.

Conclusiones

Las amenazas internas son un riesgo importante para la organización. Es muy importante implementar políticas de supervisión y detección de anomalías, además de gestionar adecuadamente la desvinculación de empleados para evitar incidentes de este tipo.

Hipótesis 3: Baiting

Resultados del Análisis:

- Detección en Splunk: Los eventos muestran la inserción de un dispositivo USB malicioso en un sistema de la organización. El programa malicioso se ejecutó automáticamente, comprometiendo el dispositivo y propagándose a otros sistemas en la red.
- Indicadores de Compromiso (IoCs):
  - ❖ IP de Origen: 192.168.3.20 (dispositivo comprometido).
  - ❖ IP de Destino: 10.0.0.4 (sistemas afectados).
  - ❖ Hash del Programa Malicioso: 9e107d9d372bb6826bd81d3542a419d6

Conclusiones

La curiosidad de los empleados puede ser explotada vía técnicas de Baiting. Es muy importante poner políticas de ejecución restringida y herramientas de escaneo de dispositivos USB para prevenir la ejecución de programas maliciosos.

Hipótesis 4: Extorsión DDoS

Resultados del Análisis:

- Simulación en Wireshark: Se observó tráfico anómalo durante la simulación del ataque DDoS con Slowloris. Los datos mostraron un volumen elevado de paquetes pequeños y múltiples conexiones incompletas, característicos de este tipo de ataque.
- Indicadores de Compromiso (IoCs):
  - ❖ IP de Origen: Varias IPs involucradas en el ataque.
  - ❖ IP de Destino: 20.127.250.238.
  - ❖ Errores de Conexión: Aumento significativo de errores TCP

Conclusiones

El ataque DDoS demostró la vulnerabilidad del servidor web de LongevityCorp ante este tipo de amenazas. Es crucial implementar soluciones de mitigación DDoS, ajustar límites de conexión y hacer monitoreo continuo para detectar y responder rápidamente a estos ataques.

Hipótesis 5: Explotación de Puertos

Resultados del Análisis:

- Detección en Splunk: Los eventos muestran que un atacante hizo un escaneo de puertos y explotó vulnerabilidades conocidas en un servidor Windows Server 2008 R2. El análisis confirmó la explotación de la Vulnerabilidad EternalBlue.
- Indicadores de Compromiso (IoCs):
  - ❖ IP de Origen: 192.168.4.25 (atacante).
  - ❖ IP de Destino: 10.0.0.5 (servidor vulnerable).
  - ❖ Vulnerabilidad: EternalBlue (**CVE-2017-0144**).

Conclusiones

La explotación de puertos y vulnerabilidades conocidas puede comprometer gravemente la seguridad de la red. Es esencial mantener los sistemas actualizados con los últimos parches de seguridad, usar firewalls y sistemas IPS.

Contenido del Video

Nota: Esta es la versión física de lo presentado en el video

❖ ¿Cómo usé las herramientas para analizar los datos?

➢ **SPLUNK**:

- Para todas las hipótesis, cargué los datasets en formato CSV usando la opción de cargar archivo en Splunk. Verifiqué los valores para asegurarme de que fueran correctos.
- Con los archivos cargados, pude visualizar todas las amenazas presentes en el Dataset.
- Ejemplo: Para detectar una amaneza específica en el Dataset de pishing, usé un filtro, source="hipotesis_1_Spear_pishing.csv" host="BrianCasa" index="threat_detection" sourcetype="csv" Acciones_realizadas = Descarga_de_adjunto_spear_phishing, que me permitió identificar eventos de “descarga de adjuntos Spear-pishing”. De manera similar, apliqué filtros específicos para cada hipótesis para identificar amenazas relevantes.

➢ **Wireshark**:

- En el caso de la amenaza DDoS, usé wireshark para capturar paquetes en vivo durante el ataque.
- Exporté el archivo de captura como pcap para hacer un análisis más detallado.
- Revisé los paquetes TCP en busca de anomalías y descubrí una cadena de paquetes con conexiones incompletas. Este comportamiento es típico de un ataque DDoS, donde se mantienen abiertas múltiples conexiones sin completarlas.

❖ ¿Cómo identifiqué la amenaza?

➢ **SPLUNK**:

- Usé filtros específicos para identificar eventos relacionados con las hipótesis.
- Las amenazas se identificaron mediante la detección de indicadores de compromiso, como la IP del atacante y el hash del archivo

malicioso (en algunos casos). De manera similar apliqué filtros y búsquedas para las demás hipótesis.

- **Wireshark**:
  - Identifiqué la amenaza DDoS al observar un volumen elevado de paquetes pequeños con conexiones incompletas.
  - La falta de una conversación (entre cliente-servidor) significativa y la longitud anormal de los paquetes confirmaron que se trataba de un ataque Slowloris.

- Explicación para el equipo de LongevityCorp sobre cómo prevenir incidentes similares en el futuro.
  - Phishing-Hipótesis 1:
    - **Capacitación a Empleados**: Implementar programas de capacitación continua para que los empleados puedan reconocer y evitar correos de pishing.
    - **Autenticación Multifactor** (MFA): Implementar MFA para añadir una capa adicional de seguridad en los accesos. EJ: Contraseña + Código de Verificación esto es para que luego de que el usuario ingrese la contraseña recibirán un código a su móvil o un correo electrónico que deben ingresar para completar el inicio de sesión.
    - **Soluciones de Correo Seguro**: Usar herramientas que escaneen y filtren correos sospechosos antes de que lleguen a los empleados. Ej: SpamTitan que es un software potenciado por IA que bloquea spam, phishing y malware, protegiendo los correos electrónicos de la empresa. Otra opción es Tutanota que da cifrado de extremo a extremo y es fácil de usar. No requiere de conocimiento técnico para configurarlo.
  - Amenaza Interna-Hipótesis 2:
    - **Supervisión y Detección de Anomalías**: Implementar políticas de supervisión y detección de anomalías para identificar comportamientos inusuales.

- **Gestión de Desvinculación**: Manejar adecuadamente la desvinculación de empleados para evitar incidentes.
- **Políticas de Acceso y Control**: Restringir el acceso a información sensible y usar controles de acceso basados en roles.

- Baiting-Hipótesis 3:
  - **Deshabilitar Autorun**: Configurar los sistemas para deshabilitar la ejecución automática de archivos desde dispositivos USB.
  - **Políticas de Uso aceptable de Dispositivos USB**: Restringir el uso de dispositivos USB no autorizados y proporcionar dispositivos USB seguros y verificados.
  - **Escaneo y Monitoreo de Dispositivos USB**: Usar software de seguridad que escanee automáticamente los dispositivos USB al ser conectados.
- Ataques DDoS-Hipótesis 4:
  - **Configuración de Límites de conexión**: Ajustar los tiempos de espera y limitar el número de conexiones simultáneas desde una misma IP para prevenir la sobrecarga de servidor. Ej: Limitar el ancho de banda en el enrutador para controlar la cantidad de tráfico de datos permitido.
  - **Herramientas de mitigación DDoS**: Implementar soluciones específicas que puedan identificar y bloquear tráfico malicioso antes de que alcance el servidor. Ej: SolarWinds detecta y previene ataques DDoS supervisando los registros de eventos de varias fuentes y puede responder automáticamente a amenazas.
  - **Monitorización Continua**: Usar herramientas de monitoreo continuo para detectar patrones de tráfico inusuales y responder rápidamente a posibles amenazas. Ej: Wireshark para capturar y analizar el tráfico de red. Otra opción es SolarWinds Network Performance Monitor la cual es para monitorear el rendimiento de la red en tiempo real y detectar cualquier anomalía.
- Explotación de Puertos-Hipótesis 5:

- **Actualizar y Parchear Sistemas**: Asegurarse de que todos los sistemas y software estén actualizados con los últimos parches de seguridad.
- **Deshabilitar Servicios Innecesarios**: Deshabilitar servicios no esenciales en los servidores.
- **Firewalls y Filtrado de Tráfico**: Configurar firewalls y sistemas de prevención de intrusiones (IPS) para filtrar el tráfico y bloquear intentos de escaneo y explotación de puertos.

❖ Glosario Técnico

➢ Referencias a las Técnicas del marco MITRE ATT&CK citadas en este documento.

- Phishing (T1566).
- Spearphishing (T1566.001).
- Recopilar información de la organización víctima (T1591).
- Recopilar información de la organización de la víctima: Relaciones Comerciales (T1591.002).
- Cuentas válidas (T1078).
- Adición de hardware (T1200).
- Registro de teclas (T1056.001).
- Replicación a través de medios extraíbles (T1091)
- Denegación de Servicio de la Red (T1498)
- Inundación Directa a la Red (T1498.001)
- Escaneo Activo (T1595).
- Escaneo de Bloques de IP (T1595.001).
- Análisis de Vulnerabilidades (T1595.002).

➢ Referencias a las Tácticas del marco MITRE ATT&CK citadas en este documento.

- Acceso Inicial (TA0001).
- Ejecución (TA0002).
- Persistencia (TA0003).
- Movimiento Lateral (TA0008).

- Impacto (TA0040).
- Reconocimiento (TA0043)

➢ EternalBlue

- CVE-2017.0144

➢ ¿Qué es DVWA (Damm Vulnerable Web Application)?

- Es una herramienta que se usa para practicar y aprender sobre la seguridad de aplicaciones web de manera segura y legal. https://github.com/digininja/DVWA .

➢ ¿Qué es XAMPP?

- Es una caja de herramientas versátil de fácil uso en Sistemas Operativos windows es ideal para desarrollar sitios web y aplicaciones. Este incluye apache, MySQL, PHP, phpMyAdmin, Perl lo que la hace ideal para hacer pruebas locales sin tener un servidor en línea lo que permite experimentar sin riesgos. Combinando XAMPP con DVWA se crea un laboratorio perfecto para entender ataques en aplicaciones web como, Ej, DDoS con Slowloris. https://www.apachefriends.org/es/index.html