MITRE Shield

Ana Valentina López Chacón & Sara Julieth Zuleta Quevedo

Colegio Mayor Nuestra Señora del Rosario. Escuela de Ingeniería, Ciencia y Tecnología.
Matemáticas Aplicadas y Ciencias de la Computación

14 de abril de 2021

Introducción

Introducción

Respond: Desarrollar e implementar las actividades adecuadas para tomar acción ante un evento de ciberseguridad detectado.

Introducción

Respond: Desarrollar e implementar las actividades adecuadas para tomar acción ante un evento de ciberseguridad detectado.

- Planificación de respuesta: Los procesos y procedimientos de respuesta se ejecutan y mantienen para garantizar una respuesta oportuna a los eventos de ciberseguridad detectados.

Introducción

¿Qué es MITRE Shield?

- MITRE Shield es una base de conocimientos de defensa activa que captura y organiza las técnicas de seguridad de manera complementaria a las mitigaciones incluidas en MITRE ATTACK.
- Esta base de conocimientos contiene datos no estructurados y estructurados.
- Este nuevo e importante recurso contiene actualmente 33 técnicas mapeadas para 8 tácticas de defensa activas.
- Shield es una herramienta importante para la industria de la seguridad.

Introducción

¿Qué es Active Defense?

- "El empleo de acciones ofensivas limitadas y contraataques para negar un área o posición en disputa al enemigo".
- Dentro de MITRE Shield, la defensa activa abarca desde capacidades ciberdefensivas básicas hasta operaciones de engaño cibernético y participación adversaria.
- La combinación de estas defensas le permite a una organización no solo contrarrestar los ataques actuales, sino también aprender más sobre ese adversario y prepararse mejor para nuevos ataques en el futuro.
- Un marco de Defensa Activa se podría capturar con una palabra: Velocidad.

Marco Teórico / Antecedentes

1. **Grafo:** Un grafo es una terna que consiste en un conjunto de vértices $V(G)$, un conjunto de aristas $E(G)$ y una relación que asocia a cada arista un par de vértices sin diferenciar a orden.
2. **Grafo Simple:** Un grafo G es simple si no tiene bucles ni aristas paralelas, donde $E(G)$ es un conjunto de parejas no ordenadas.
3. **Grafo Conexo:** Un grafo G es conexo si para cada par de vértices en G existe un camino entre ellos.
4. **Grado de un vértice:** Se define como el numero de aristas incidentes en el vértice, se denota $d(v)$.
5. **Algoritmo de Dijkstra:** El algoritmo de Dijkstra, también llamado algoritmo de caminos mínimos o máximos, es un algoritmo para la determinación del camino más corto o largo, dado un vértice origen, hacia el vértice final en un grafo que tiene pesos en cada arista.

Marco Teórico / Antecedentes

Algorithm 1 Algoritmo de Dijkstra

Input: Un grafo ponderado G con pesos no negativos. Sea $w(u, v)$ el peso de la arista (u, v), definimos $w(u, v) = \infty$ si $(u, v) \notin E(G)$.
Output: $L(z)$ distancia mínima de u a z.

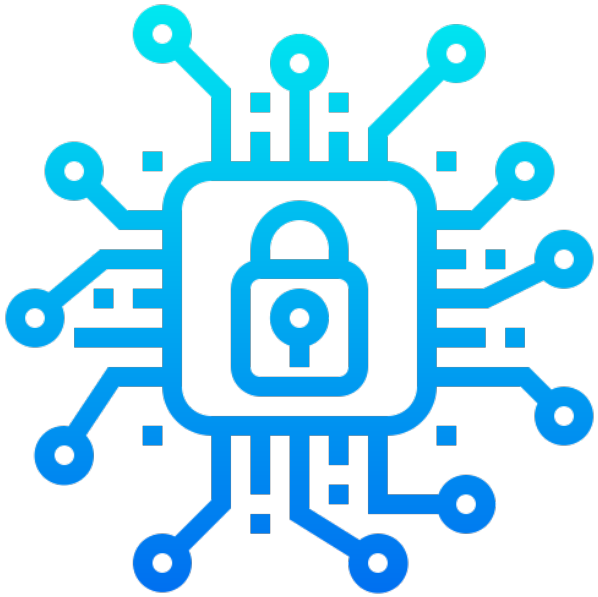
$L(u) = 0$
Para todos los vértices $v \neq u$:
    $L(v) = \infty$
$S = \emptyset$
while $z \notin S$ **do**
  Seleccione un vértice $v \neq u$ con $L(x)$ mínimo
  $S = S \cup \{x\}$
  Para todo $v \notin S$
    $L(v) = min\{L(v), L(x) + w(x, v)\}$
end while

Tácticas

Las tácticas describen el efecto deseado de las actividades de defensa activa y son útiles para describir por qué un defensor elegiría utilizar una técnica de defensa activa específica. Estas tácticas sirven como formas útiles de clasificar las técnicas defensivas individuales.

Tácticas

Channel

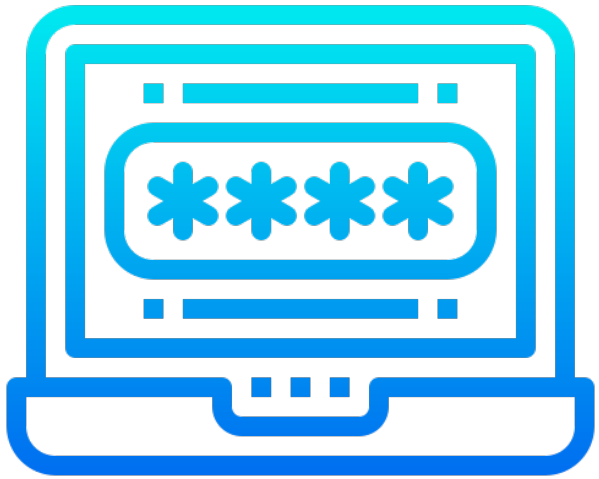


- El canal se usa para guiar a un adversario por un camino específico o en una dirección específica.
- Esta táctica se puede utilizar para desperdiciar el tiempo de un adversario, para hacer que utilice recursos adicionales o para que los defensores estudien sus comportamientos.

Tácticas

Collect

- Recopilar se utiliza para obtener información sobre un adversario o sobre su actividad que pueda informar a otras defensas.



Tácticas

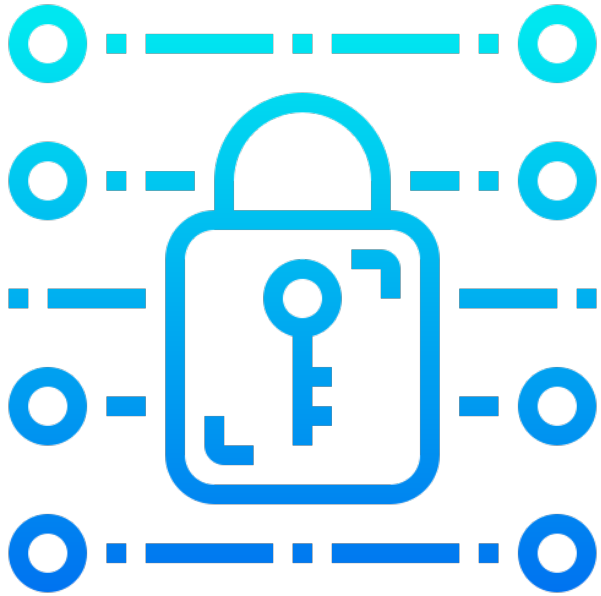
Contain

- Contener se utiliza para evitar que un adversario se mueva fuera de límites o restricciones específicas.

Tácticas

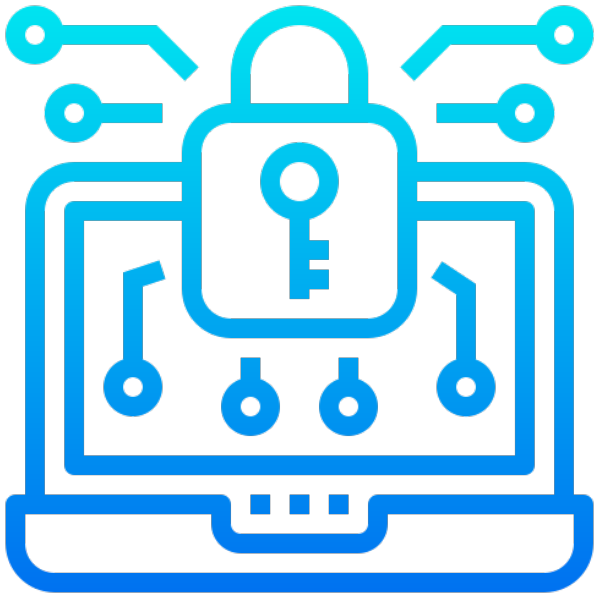
Detect

- Detectar se utiliza para establecer o mantener un seguimiento de lo que está haciendo un adversario.



Tácticas

Disrupt



- Disrupt se utiliza para evitar o disuadir a un adversario de que lleve a cabo una parte o la totalidad de su misión.

Tácticas

Facilitate

- Facilitar se utiliza para permitir que un adversario lleve a cabo parte o toda su misión.

Tácticas

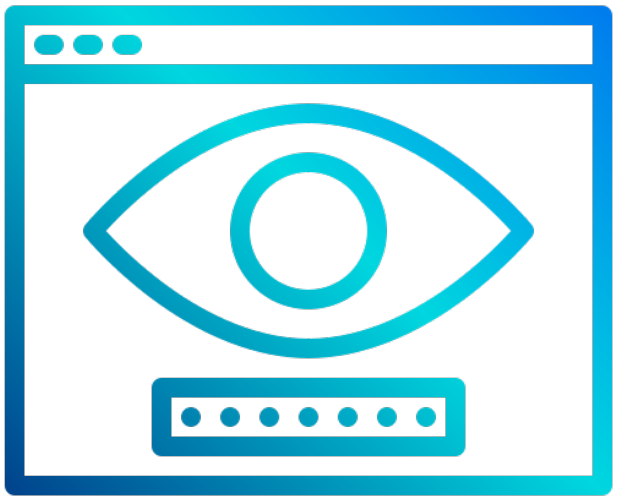
Legitimize

- Legitimar se usa para agregar autenticidad a los componentes engañosos para convencer a un adversario de que algo es real.

Tácticas

Test

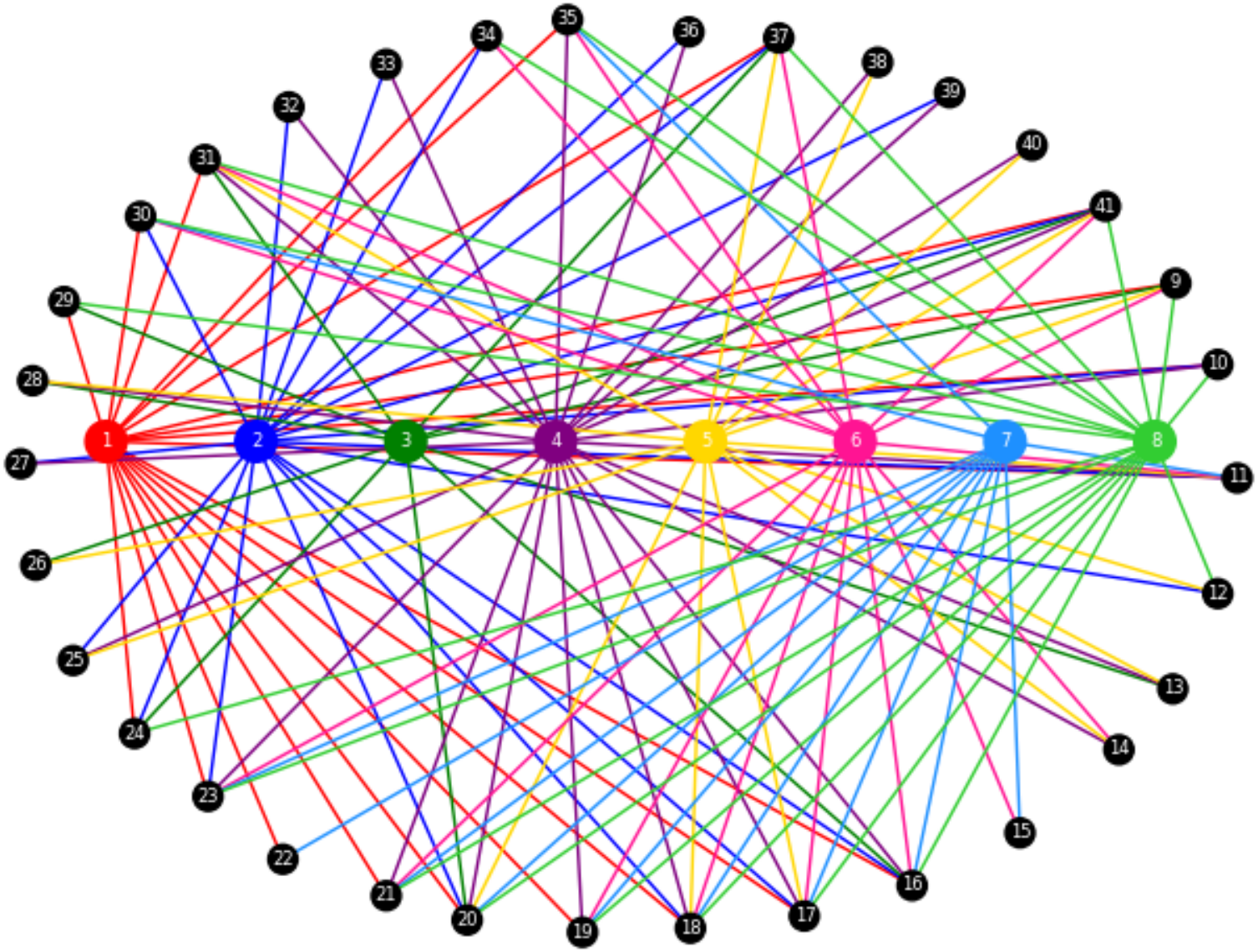
- La prueba se utiliza para determinar los intereses, capacidades, comportamientos, motivaciones y demás de un adversario.



Interpretación Gráfica

#	Nombre	#	Nombre	#	Nombre
1	Channel	15	Burn-In	29	Migrate Attack Vector
2	Collect	16	Decoy Account	30	Network Diversity
3	Contain	17	Decoy Content	31	Network Manipulation
4	Detect	18	Decoy Credentials	32	Network Monitoring
5	Disrupt	19	Decoy Diversity	33	PCAP Collection
6	Facilitate	20	Decoy Network	34	Peropheral Management
7	Legitimize	21	Decoy Persona	35	Pocket Litter
8	Test	22	Decoy Process	36	Protocol Decoder
9	Admin Access	23	Decoy System	37	Security Controls
10	API Monitoring	24	Detonate Malware	38	Standard Operating Procedure
11	Application Diversity	25	Email Manipulation	39	System Activity Monitoring
12	Backup and Recovery	26	Hardware Manipulation	40	User Training
13	Baseline	27	Hunting	41	Software Manipulation
14	Behavioral Analytics	28	Isolation		

Interpretación Gráfica



Técnicas

Técnicas describe las cosas que pueden hacer (los defensores) en defensa activa. Para cada una de las técnicas es posible obtener información sobre qué tácticas admite, qué oportunidades están disponibles según los TTP del adversario, así como casos de uso y procedimientos para impulsar las discusiones de implementación.

Técnicas

Admin Access

- Cambiar el sistema de destino para permitir o restringir que los usuarios realicen tareas que requieren permisos de nivel de administrador.

API Monitoring

- La supervisión de API implica capturar una función interna del sistema operativo (SO) para su uso, los argumentos que la acompañan y el resultado.

Técnicas

Application Diversty

- La diversidad de aplicaciones le presenta múltiples objetivos de software para el adversario.

Backup and Recovery

- Utiliza herramientas de imagen, respaldo del sistema o sincronización de archivos para crear copias de datos clave en un repositorio de respaldo protegido.

Técnicas

Baseline

- Identifique elementos de software y configuración elementales para un conjunto de objetivos, defina los valores adecuados y esté preparado para restablecer un sistema en ejecución a su estado esperado.

Behavioral Analytics

- Generar un sistema para recopilar información detallada sobre la ejecución de procesos y la actividad del usuario.

Técnicas

Burn-In

- Ejecutar el sistema para crear artefactos deseados en el sistema, incluyendo la navegación web, el uso del sistema de archivos y demás.

Decoy Account

- Una cuenta señuelo es aquella que se crea específicamente con fines defensivos o engañosos.

Técnicas

Decoy Content

- El contenido señuelo son los datos utilizados para contarle una historia al adversario.

Decoy Credentials

- Desarrolle un sistema de destino con credenciales como nombre de usuario, contraseña y otras formas de datos de autenticación, con el fin de generar una interacción.

Técnicas

Decoy Diversity

- La diversidad de señuelos es el despliegue de sistemas señuelo con diferentes sistemas operativos y configuraciones de software.

Decoy Network

- Las redes señuelo están compuestas de múltiples recursos informáticos que se pueden utilizar con fines defensivos o engañosos.

Técnicas

Decoy Persona

- Una persona señuelo se utiliza para establecer antecedentes sobre un usuario.

Decoy Process

- La ejecución de software creará un proceso de sistema en el sistema de destino, el cual se puede utilizar para influir en la percepción o reacción de un adversario.

Técnicas

Decoy System

- Un sistema de señuelo es un recurso informático presentado al adversario en apoyo de la defensa activa.

Detonate Malware

- Un entorno de ejecución puede variar desde un dispositivo de ejecución de malware comercial algo estéril hasta un sistema a medida diseñado para cumplir los objetivos de participación.

Técnicas

Email Manipulation

- La manipulación del contenido del correo electrónico se refiere a la alteración de un mensaje de correo electrónico.

Hardware Manipulation

- La manipulación de hardware puede consistir en realizar cambios físicos o de configuración, incluyendo la eliminación física del micrófono, la cámara, el adaptador Wi-Fi integrado, entre otros de un sistema o el uso de otros controles para desactivar estos dispositivos.

Técnicas

Hunting

- Dentro del entorno del defensor, hunting asume una falla en la prevención o detección inicial y que un adversario ha penetrado exitosamente en el sistema.
- La búsqueda se basa en inteligencia sobre las TTP e infraestructura del adversario.
- La información sobre el adversario se puede utilizar para mejorar las defensas.
- Investigar activamente la exposición de la organización o la inclusión en volcados de contraseñas, filtraciones y demás ayuda a los defensores a centrarse en detecciones específicas y contramedidas proactivas.

Técnicas

Isolation

- Al usar el aislamiento, un defensor puede prevenir una actividad potencialmente maliciosa antes de que comience o limitar su efectividad y alcance.

Migrate Attack Vector

- Migrate Attack Vector permite que un defensor acceder a un elemento malicioso interceptado y que lo analice en un entorno seguro o que lleve a cabo un enfrentamiento con el adversario dentro de una red de señuelos.

Técnicas

Network Diversity

- La diversidad de la red implica el uso de una colección diversa de elementos de la red para hacer que una red señuelo parezca más realista.

Network Manipulation

- La manipulación de red permite que un defensor modifique las velocidades de la red, segmente la red, mantenga un esquema de direccionamiento IP único o agregue un interruptor para cortar el acceso a la red si es necesario.

Técnicas

Network Monitoring

- El monitoreo de la red se refiere a capturar datos sobre la actividad de la red, incluida la captura del registro en el servidor, el firewall y otros registros relevantes.

PCAP Collection

- La recopilación de PCAP permite a los defensores utilizar los datos para examinar el tráfico de red del adversario más de cerca, incluyendo el estudio de si está codificado y/o encriptado.

Técnicas

Peripheral Management

- La gestión de periféricos es la administración de dispositivos periféricos utilizados en sistemas dentro de la red con fines defensivos o engañosos.

Pocket Litter

- Pocket Litter son datos que se colocan en un sistema para convencer a un adversario de que el sistema y los usuarios son reales.

Técnicas

Protocol Decoder

- Los decodificadores de protocolo están diseñados para leer el tráfico de la red y contextualizar toda la actividad entre el operador y el implante.

Security Controls

- La manipulación de los controles de seguridad implica realizar cambios de configuración en la configuración de seguridad de un sistema.

Técnicas

Standard Operating Procedure

- Los procedimientos operativos estándar (SOP) establecen una forma estructurada de interactuar con sistemas y servicios.

System Activity Monitoring

- La captura de registros del sistema puede mostrar inicios de sesión, eventos del sistema y del usuario.

Técnicas

Software Manipulation

- La manipulación de software le permite al defensor alterar o reemplazar elementos del sistema operativo, sistema de archivos o cualquier otro software instalado y ejecutado en el sistema.

User Training

- La formación de usuarios implica enseñar a los usuarios finales a ser sensores humanos que saben cómo reconocer las amenazas cibernéticas y los procedimientos para reportarlas.

Attack Mapping Overview

Como defensores, vemos el valor de mapear técnicas de defensa activa. En esta sección del sitio, cada táctica en el marco de ATTACK se muestra individualmente. Dependiendo de sus necesidades, es posible aplicar múltiples técnicas de defensa activa. A continuación veamos el mapeo ATTACK desglosado por táctica ATTACK.

Attack Mapping Overview

Reconocimiento:

El adversario está tratando de recopilar información que pueda utilizar para planificar operaciones futuras.

Desarrollo de recursos:

El adversario está tratando de establecer recursos que puedan utilizar para respaldar las operaciones.

Acceso inicial:

El adversario está intentando ingresar a su red.

Ejecución:

El adversario está intentando ejecutar un código malicioso.

Persistencia:

El adversario está tratando de mantenerse firme.

Attack Mapping Overview

Escala de privilegios:

El adversario está intentando obtener permisos de nivel superior.

Evasión de defensa:

El adversario está tratando de evitar ser detectado.

Acceso a credenciales:

El adversario está intentando robar nombres de cuentas y contraseñas.

Descubrimiento:

El adversario está tratando de descubrir su entorno.

Movimiento lateral:

El adversario está tratando de moverse a través de su entorno.

Attack Mapping Overview

Recopilación:

El adversario está tratando de recopilar datos de interés para su objetivo.

Exfiltración:

El adversario está intentando robar datos.

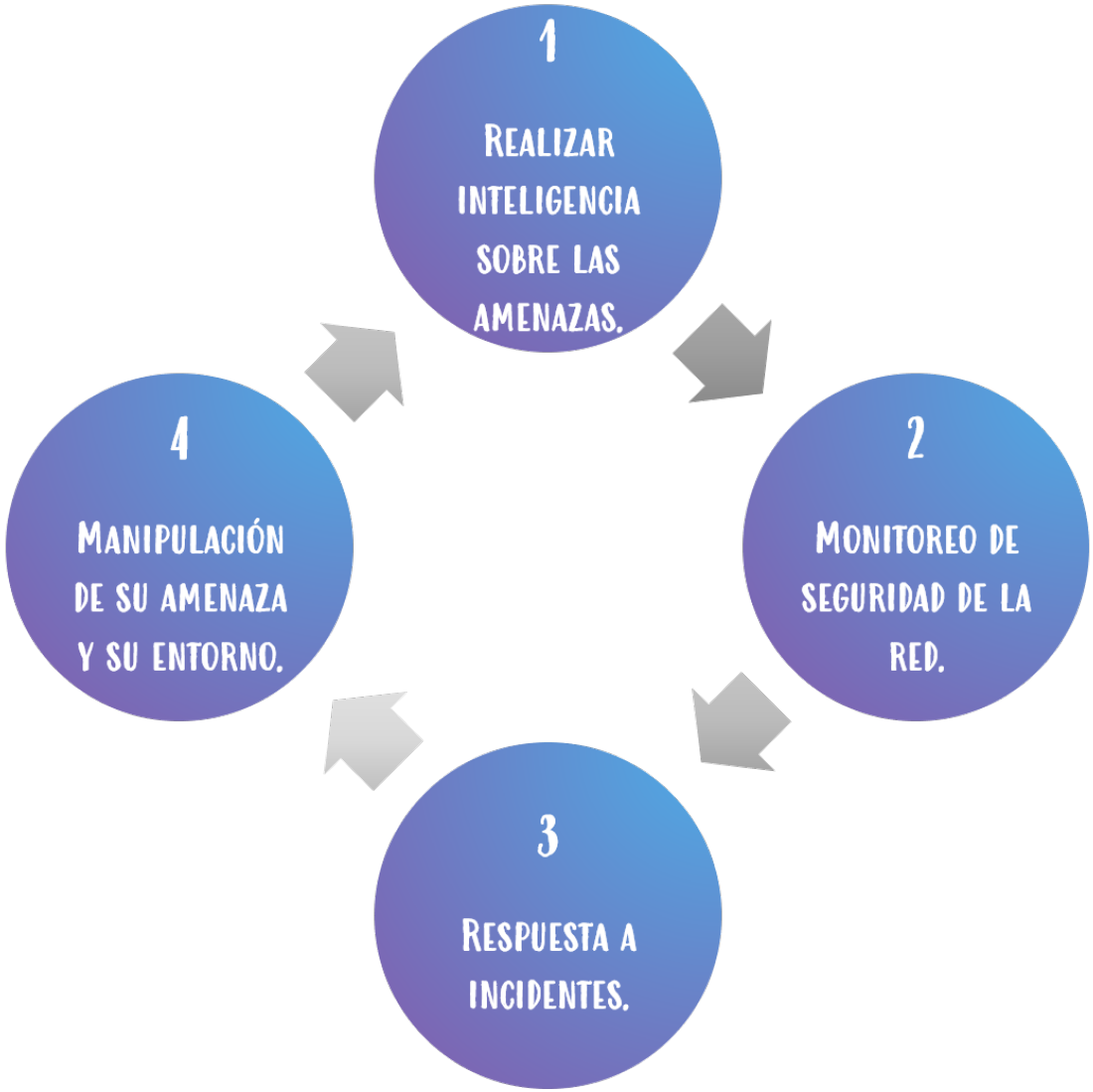
Mando y Control:

El adversario está tratando de comunicarse con los sistemas comprometidos para controlarlos.

Impacto:

El adversario está intentando manipular, interrumpir o destruir sus sistemas y datos.

Ciclo de Defensa Activa



Preguntas a responder

Para llevar a cabo nuestra investigación y proyecto es necesario plantearse los siguientes interrogantes:

1. ¿Cómo podemos usar el ciclo de defensa activa para clasificar nuestras tácticas y técnicas?
2. Dependiendo de un determinado tipo de ataque, ¿Que clase de tácticas y técnicas son eficientes para contra-restar esa amenaza?
3. ¿Cómo podemos adaptar el Algoritmo de Dijkstra para nuestras necesidades?
4. ¿Se necesitan implementar otros algoritmos para complementar la búsqueda de caminos?

Metodología

Veamos los pasos a seguir para nuestra investigación y desarrollo del proyecto:

1. Clasificar las técnicas dentro de los cuatro estados del ciclo de defensa activa.
2. Seleccionar 8 de los 14 ataques que tengan mayor complejidad y casos de uso.
3. Determinar que técnicas son eficientes para combatir cada ataque.
4. Generar subgrafos que incluyan los vértices de las técnicas convenientes para cada de ataque.
5. Modificar el algoritmo de Dijkstra para que encuentre caminos que cumplen con el ciclo de defensa activa.
6. Finalizar los últimos detalles de cuestiones estéticas y computacionales para tener una implementación apropiada.

Descripción de los pasos a seguir

Paso 1: Determinar la clasificación de las 33 técnicas dentro del ciclo de defensa activa, es decir, estudiar los objetivos y procedimientos de cada técnica para luego clasificarla dentro de uno de los cuatro estados del ciclo de defensa activa. Para los propósitos de la implementación una técnica no puede pertenecer a dos estados diferentes del ciclo de defensa activa.

Descripción de los pasos a seguir

Paso 2: Para los propósitos de la implementación queremos tener control sobre los tipos de ataques disponibles para ofrecer todas las opciones de respuesta. De los 14 ataques presentados anteriormente tomaremos los 8 ataques que tienen mayor complejidad y casos de uso, luego partiendo de esto podremos generar una respuesta más acertada, sin embargo el proceso para cada uno de los ataque no escogidos es completamente análogo.

Descripción de los pasos a seguir

Paso 3: Basándonos en la información proporcionada por la pagina oficial de Mitre SHIELD [2] en la sección de ATTACK Mapping buscamos que dado el tipo de ataque ingresado por el usuario se encontraran los caminos teniendo en cuenta las técnicas que si son eficientes para combatir el ataque especificado, el cual estar entre los 8 ataques seleccionados en el paso anterior.

Descripción de los pasos a seguir

Paso 4: Con la información obtenida en el **Paso 2** podemos generar subgrafos del grafo original que solo incluyan los vértices que representan las técnicas útiles para el tipo de ataque con sus respectivas aristas. También se incluyen los vértices de las tácticas que aun tengan conexiones con los vértices resultantes.

Descripción de los pasos a seguir

Paso 5: Basándonos en el Algoritmo de Dijkstra y la información obtenida en el **Paso 1** buscamos extrapolar la idea del algoritmo donde en lugar de buscar los caminos de peso mínimo retorne todos los caminos que cumplen con el ciclo de defensa activa para un ataque determinado, es decir, que cada camino contenga un vértice de cada estado del ciclo de defensa activa, esto se podría lograr implementando Dijkstra con otros algoritmos de búsqueda, como Backtracking.

Descripción de los pasos a seguir

Paso 6: Finalmente, se le mostrará al usuario cada una de las posibilidades por las que puede optar para responder al ataque ingresado, es decir, obtendrá cada uno de los caminos que puede tomar representado en forma gráfica, en términos de teoría de grafos y el orden y nombre de las técnicas que debe ejecutar para obtener una defensa activa.

Cronograma

Fecha	Actividad
7 de abril de 2021	Clasificar las técnicas dentro de los cuatro estados del ciclo de defensa activa.
10 de abril de 2021	Seleccionar 8 de los 14 ataques que tengan mayor complejidad y casos de uso.
12 de abril de 2021	Determinar que técnicas son eficientes para combatir cada ataque.
21 de abril de 2021	Generar subgrafos que incluyan los vértices de las técnicas convenientes para cada de ataque.
26 de abril de 2021	Modificar el algoritmo de Dijkstra para que encuentre caminos que cumplen con el ciclo de defensa activa.
1 de mayo de 2021	Finalizar los últimos detalles de cuestiones estéticas y computacionales para tener una implementación apropiada.

Ciclo de Defensa Activa (Paso 1)

Para completar el **Paso 1**, vamos a clasificar las 33 técnicas en cada una de las cuatro instancias del ciclo de defensa activa explicado anteriormente. Esta clasificación se hace de acuerdo a los propósitos de cada técnica y sus casos de uso.

1. Realizar inteligencia sobre amenazas

- Baseline
- Behavioral Analytics
- Decoy Credentials
- Decoy Process
- Isolation
- PCAP Collection
- Protocol Decoder

Ciclo de Defensa Activa (Paso 1)

2. Monitoreo de seguridad de la red

- API Monitoring
- Decoy Network
- Migrate Attack Vector
- Network Diversity
- Network Monitoring
- Peripherial Management
- Standard Operating Procedure
- System Activity Monitoring

3. Respuesta a incidentes

- Backup and Recovery
- Burn-In
- Decoy Account
- Decoy Diversity
- Detonate Malware
- Hunting
- Software Manipulation

Ciclo de Defensa Activa (Paso 1)

4. Manipulación de su amenaza y su entorno

- Admin Access
- Application Diversity
- Decoy Content
- Decoy Persona
- Decoy System
- Email Manipulation
- Hardware Manipulation
- Network Manipulation
- Pocket Litter
- Security Controls
- User Training

Ataques Seleccionados (Paso 2)

Para completar el **Paso 2** seleccionamos los siguientes ataques explicados anteriormente:

1. Acceso inicial
2. Ejecución
3. Escalada de privilegios
4. Evasión de defensa
5. Acceso a credenciales
6. Exfiltración
7. Mando y control
8. Impacto

Técnicas para cada ataque(Paso 3)

Para completar el **Paso 3**, vamos a clasificar en cada ataque seleccionado en el paso anterior, las técnicas que sean eficientes para responder al ataque.

1. Acceso Inicial

- Decoy Account
- Decoy Credentials
- Burn-In
- System Activity Monitoring
- Security Controls
- Migrate Attack Vector
- Isolation
- Decoy System
- Decoy Network
- Decoy Diversity
- Email Manipulation
- User Training
- Decoy Persona

Técnicas para cada ataque(Paso 3)

2. Execution

- Admin Access
- Security Controls
- Decoy System
- System Activity Monitoring
- Software Manipulation
- API Monitoring
- Application Diversity
- Detonate Malware
- Standard Operating Procedure

3. Privilege Escaletion

- Baseline
- Admin Access
- Decoy System
- System Activity Monitoring
- Security Controls
- Decoy Account
- Decoy Credentials
- Burn-In
- Software Manipulation
- Behavioral Analytics

Técnicas para cada ataque(Paso 3)

4. Defense evasion

- Software Manipulation
- Admin Access
- Security Controls
- Decoy System
- Behavioral Analytics
- Decoy Account
- Decoy Credentials
- Burn-In
- Baseline
- System Activity Monitoring
- API Monitoring
- Network Monitoring
- Application Diversity
- Detonate Malware
- Pocket Litter
- Decoy Content
- Satandard Operating Procedure
- Decoy Diversity

Técnicas para cada ataque(Paso 3)

5. Credentials Access

- Decoy Credentials
- Software Manipulation
- Decoy Process
- Network Diversity
- Decoy Content
- System Activity Monitoring
- Security Controls
- Standard Operating Procedure
- Network Manipulation
- Application Diversity
- User Training
- Burn-In
- Network Monitoring

6. Exfiltration

- Security Controls
- PCAP Collection
- Protocol Decoder
- Network Monitoring
- Network Manipulation
- Peripheral Management
- Behavioral Analytics

Técnicas para cada ataque(Paso 3)

7. Command and Control

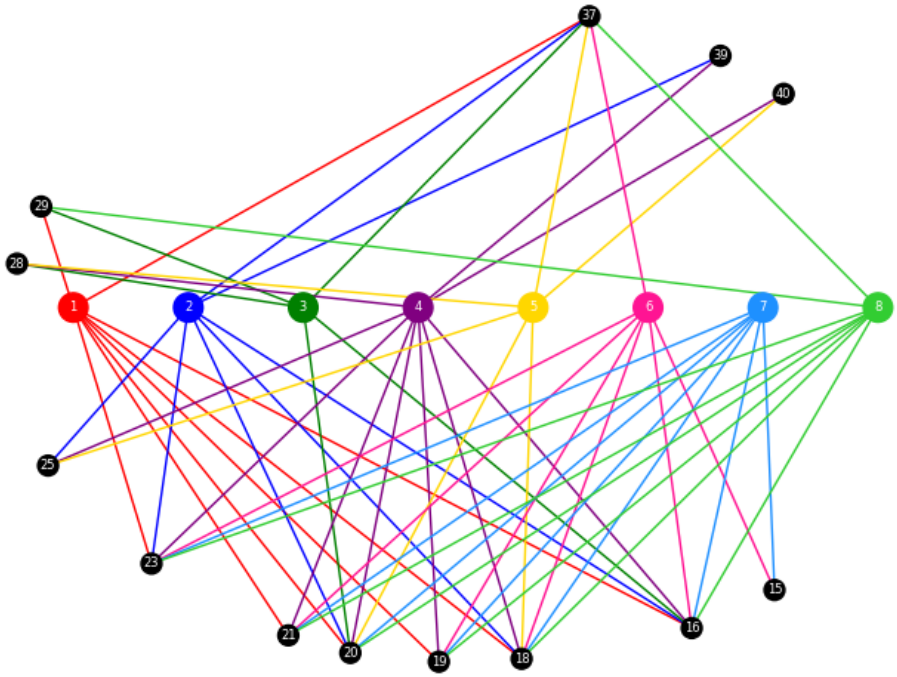
- PCAP Collection
- Protocol Decoder
- Network Manipulation
- Network Monitoring
- Peripheral Management
- Migrate Attack Vector
- Behavioral Analytics
- Isolation
- Decoy System
- Hunting

8. Impact

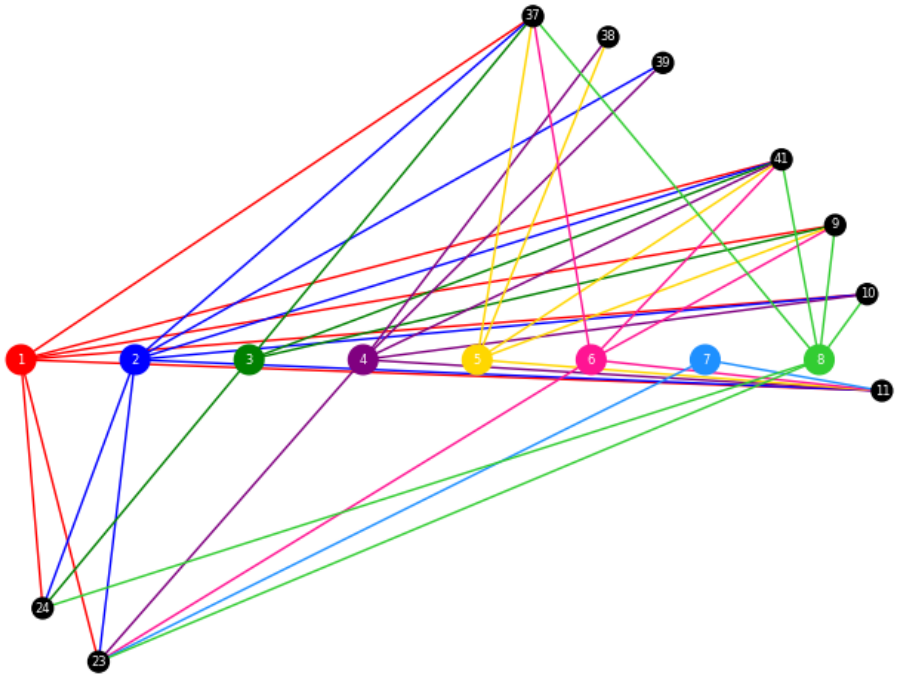
- Backup and Recovery
- Software Manipulation
- System Activity Monitoring
- Behavioral Analytics
- Network Manipulation
- Security Controls
- Decoy System
- Decoy Content

Implementación (Paso 4)

Para completar el **Paso 4** veamos el subgrafo resultante para cada uno de los ataque tomando en cuenta a información obtenida en el paso anterior:

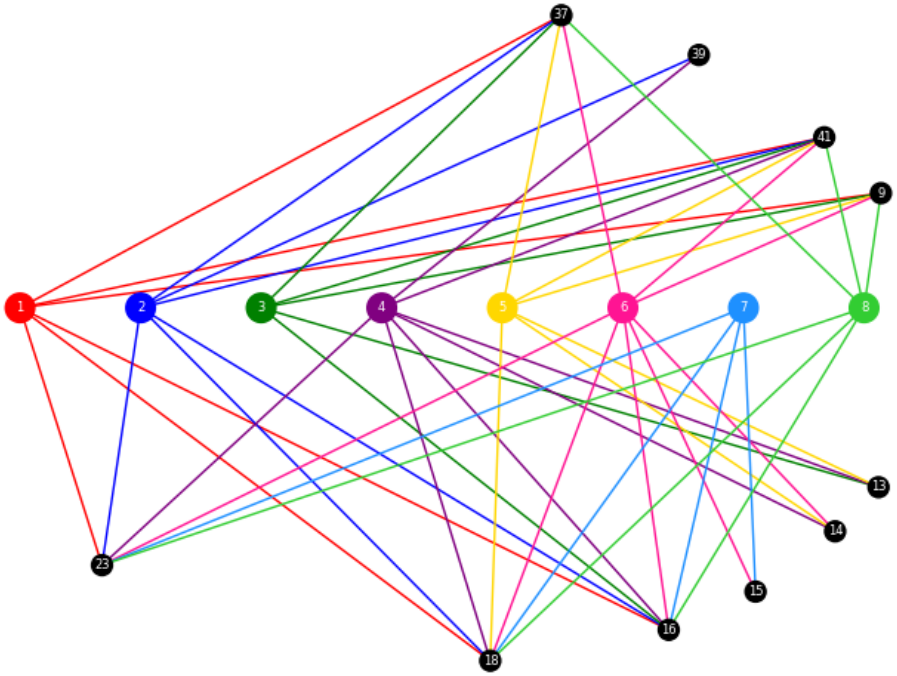


Ataque *Initial Access*

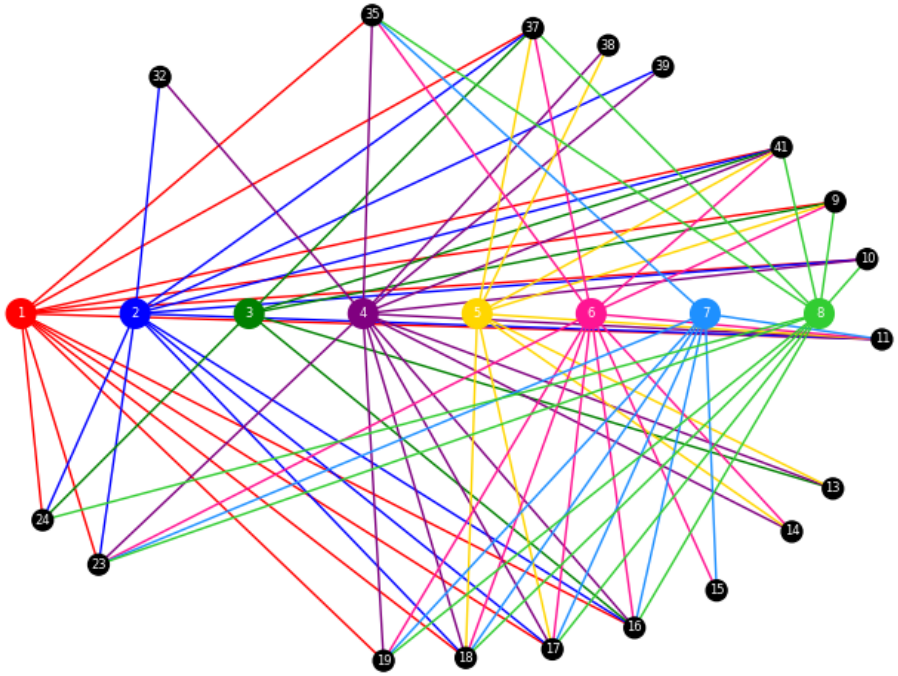


Ataque *Execution*

Implementación (Paso 4)

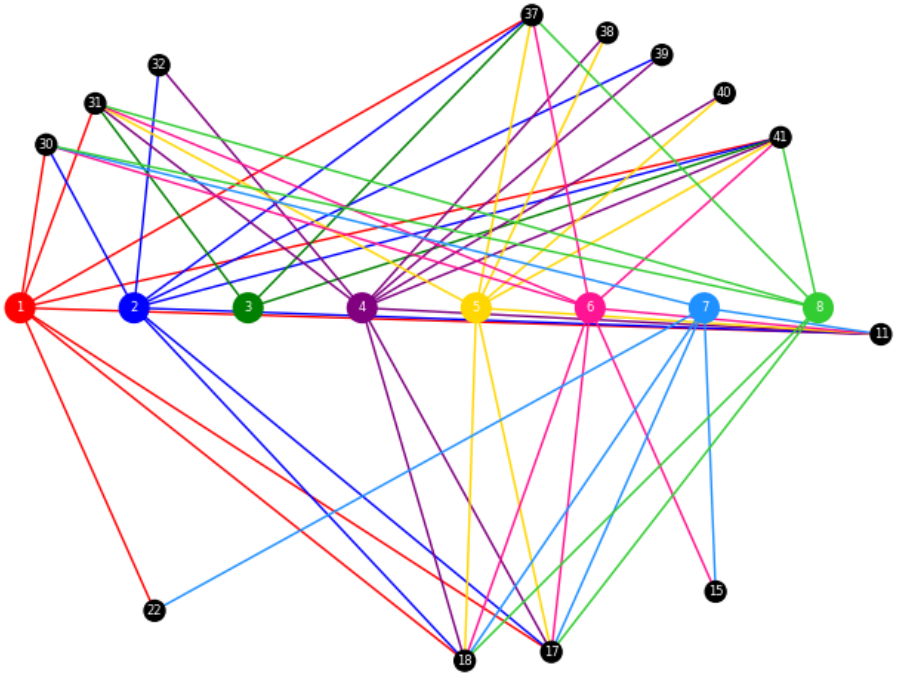


Ataque *Privilege Escaletion*

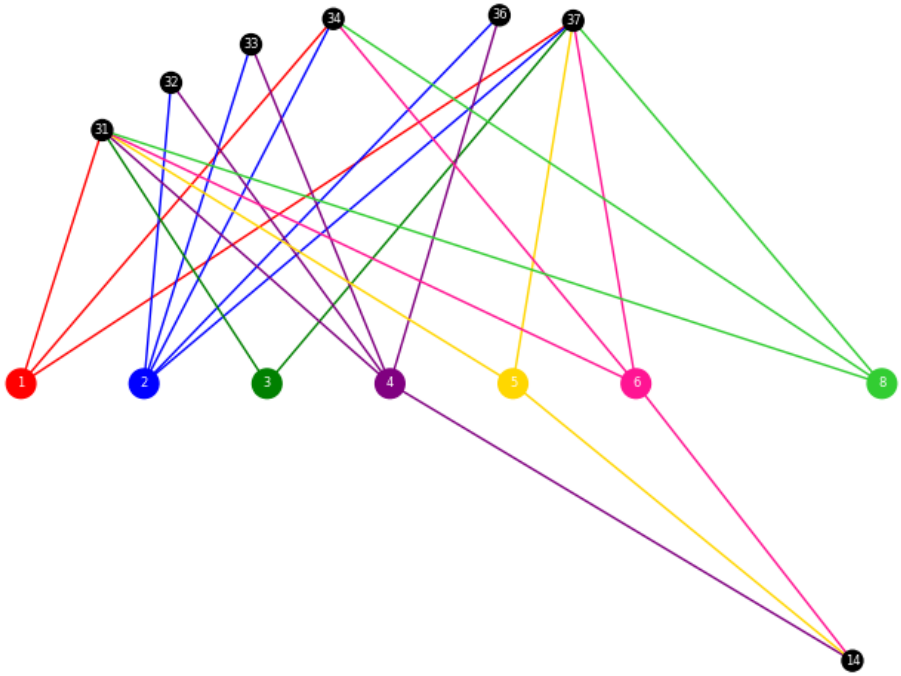


Ataque *Defense Evasion*

Implementación (Paso 4)

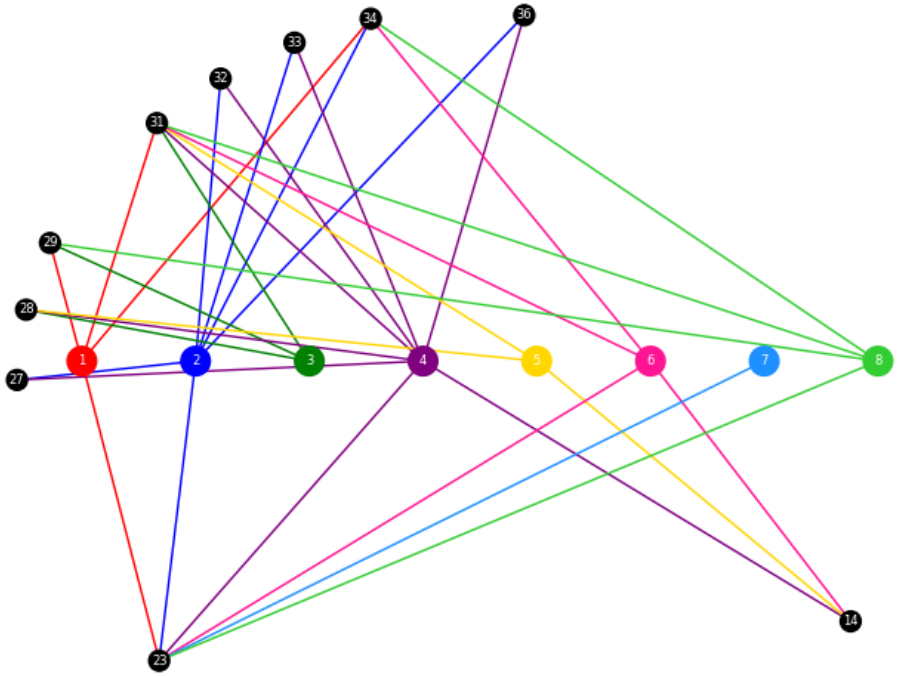


Ataque *Credential Access*

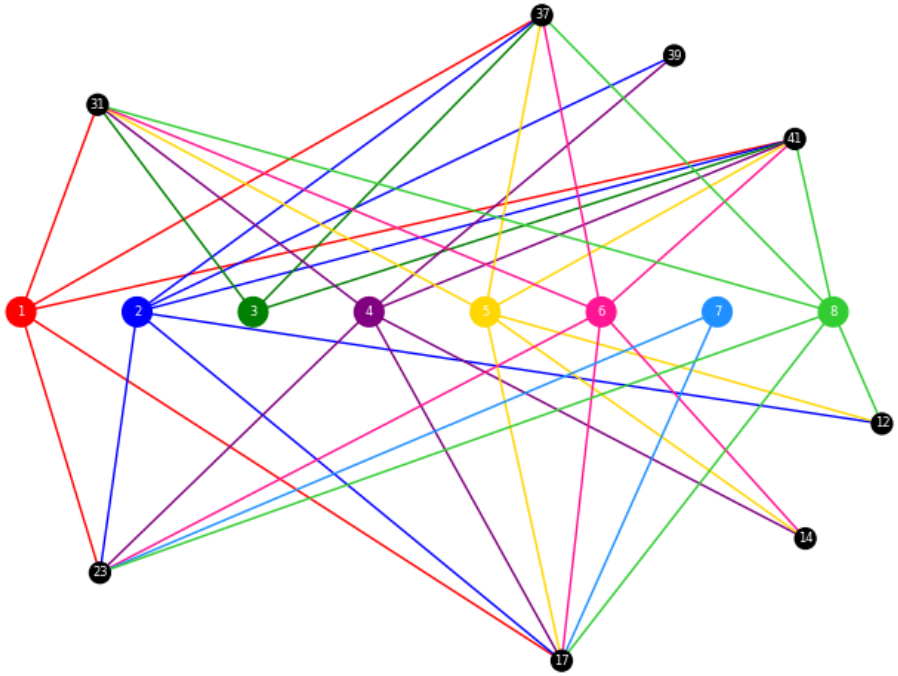


Ataque *Exfiltration*

Implementación (Paso 4)



Ataque *Command and Control*



Ataque Impact

Referencias

- Goffin, M. (2020). *Introducing MITRE Shield Adversary Group Mappings - MITRE Shield.* Medium. https://medium.com/mitre-shield/introducing-mitre-shield-adversary-group-mappings-b1e095381dae
- The MITRE Corporation. (2020). *MITRE Shield*. MITRE Shield. https://shield.mitre.org/
- Preston, S., SVP Strategy Growth, TrapX Security. (2021). *MITRE Shield: A Framework for Agile Cyber Security.* The First Global Cybersecurity Observatory. https://cyberstartupobservatory.com/mitre-shield-a-framework-for-agile-cyber-security/