SOC N1

SOC (Security Operations Center)
Módulo 5 – Herramientas

THREAT INTELLIGENCE - EJERCICIOS

Sheila Fernández Cisneros – 12/07/2024

Tarea 1:

Imagina que eres analista de nivel 1 y tienes que subir un evento para reportar el siguiente incidente al MISP:

Fecha	Descripción	IoC	Ataque detectado
25/06/2024	Phishing	hxxps://bbbva(.)information-cuenta(.)es	Scamming/Phishing

- ¿Qué nivel de amenaza indicarías al subir el evento, teniendo en cuenta que se está reportando únicamente un enlace como phishing y además tiene varios indicios de serlo?

Nivel de amenaza: Medio Alto

Justificación: Dado que se ha detectado un enlace malicioso con indicios de ser phishing, se clasifica el nivel de amenaza como medio alto por las siguientes razones:

1. **Riesgo Humano:** El ser humano es considerado el eslabón más débil en la cadena de seguridad y por tanto un alto riesgo. Los correos electrónicos o mensajes de phishing están diseñados para engañar al personal, aumentando la probabilidad de que alguien cometa un error y haga clic en el enlace.

2. **Campaña dirigida:** El enlace intenta imitar un dominio bancario legítimo, lo cual es un indicador fuerte y dirigido de actividad maliciosa.

3. **Obtención de Credenciales:** El phishing tiene como objetivo principal obtener credenciales de acceso a la organización. Si un empleado proporciona esta información, los atacantes pueden acceder a sistemas internos, lo que representa un riesgo significativo para la seguridad de la organización.

4. **Impacto Potencial:** Si el phishing tiene éxito, puede llevar a compromisos más serios, incluyendo acceso no autorizado a datos sensibles, instalación de malware, y otros tipos de fraude financiero o de identidad.

- ¿Qué información indicarías de este evento como descripción?

Scamming/Phishing.

- De entre las siguientes opciones para Categoría – Tipo del IoC que se debe añadir como atributo, ¿cuál crees que es la que más se ajusta a este incidente?

a) Network activity– URL

b) Financial Fraud– Other

c) External Analysis– Link

d) a) y b) pueden ser adecuadas

Creo que la que mas se ajusta es la d) Network activity-URL y Financial Fraud-Other, a y b son adecuadas.

- **Network activity– URL:** Porque el IoC es una URL que se ha utilizado en una actividad de red maliciosa.
- **Financial Fraud– Other:** Porque el objetivo del phishing es obtener información financiera con fines fraudulentos.

- ¿Qué valor se debería añadir como "atributo"? ¿Habría que hacerle algún cambio a ese atributo para subirlo, o se puede subir tal y como se indica en el incidente?

Valor a añadir como "atributo" en MISP:

- **Category:** Financial fraud
- **Type:** other (seleccionamos "other" porque no aparece la opción de url)
- **Value:** https://bbva.information-cuenta.es

Justificación del cambio:

El cambio realizado al valor es la desanitización del IoC porque se está añadiendo para ser compartido como un Indicador de Compromiso y es necesario proporcionar el valor correcto y completo del enlace malicioso, no una versión sanitizada del mismo.

- De los "tags" que se muestran a continuación, ¿cuál debería añadirse en este evento?

circl: incident-classification="spam"

circl: incident-classification="phishing"

circl: incident-classification="social-engineering"

Tags más adecuados:

- **circl: incident-classification="phishing"**
- **circl: incident-classification="social-engineering"**

Justificación: El incidente descrito implica un enlace malicioso diseñado para obtener credenciales a través de engaños, lo cual clasifica el incidente como phishing. Al mismo

tiempo, el phishing es una forma de ingeniería social, ya que busca manipular a las personas para que realicen acciones específicas (en este caso, proporcionar sus credenciales).

Scam en este caso no es adecuada porque scam suelen ser correos electrónicos enviados en masa que pueden contener enlaces maliciosos o no, no siempre tienen el objetivo de obtener información personal o realizar fraudes como el caso de phishing.

Investiga la matriz de MITRE ATT&CK de Tácticas y Técnicas, ¿cuál crees que puede ser la más indicada/relacionada con este caso?

En este caso, el adversario utiliza un enlace de phishing para obtener acceso inicial a la red de la víctima. Esta actividad se clasifica bajo la táctica **TA0001: Initial Access**, ya que el objetivo es establecer un punto de entrada en el sistema. La técnica utilizada es **T1566: Phishing**, y la subtécnica específica es **T1566.002: Spearphishing Link**, que describe el método exacto empleado: el envío de enlaces personalizados y fraudulentos.

Tarea 2:

Escenario del Incidente:

Imagina que eres un analista de seguridad y has detectado actividad sospechosa en la red de tu organización. Un atacante parece estar intentando obtener acceso a información sensible.

Detalles del Incidente:

Descripción: Un usuario ha informado de un comportamiento inusual en su equipo. Se han detectado múltiples intentos de inicio de sesión fallidos y la ejecución de comandos desconocidos.

Fecha y Hora: 25 de junio de 2024, 11:00 AM UTC

Indicadores de Compromiso (IoC):

• Múltiples intentos de inicio de sesión fallidos desde la IP interna 10.0.0.5.

• Ejecución de comandos net user y tasklist en el equipo afectado.

Tareas:

- Identificación de Técnicas de Ataque:

Utiliza la matriz MITRE ATT&CK para identificar las técnicas utilizadas por el atacante basándote en los IoCs proporcionados.

Los comandos utilizados son de Windows:

- **net user:** lista las cuentas de usuario en el sistema.

- **tasklist:** lista todos los procesos en ejecución en el sistema.

Responde a las siguientes preguntas:

• ¿Qué técnicas de MITRE ATT&CK corresponden a los intentos de inicio de sesión fallidos?

Esta técnica involucra intentos repetidos de inicio de sesión utilizando diferentes contraseñas. La actividad de múltiples intentos de inicio de sesión fallidos desde una IP interna sugiere que el atacante está tratando de forzar la entrada mediante adivinación de contraseñas.

Esta actividad se clasifica bajo la Táctica **Credential Access – TA0006**, la cual está relacionada con el robo de cuentas y contraseñas. La técnica utilizada es **Brute Force – T1110**, la cual consiste en usar técnicas de fuerza bruta para obtener acceso a cuentas del sistema. Dentro de esta, estaríamos dentro de la subtécnica **Password Guessing – T1110.001**, donde los adversarios sin conocimiento previo de las credenciales intentan adivinarla mediante múltiples intentos de acceso.

• ¿Qué técnicas de MITRE ATT&CK corresponden a la ejecución de los comandos net user y tasklist?

El uso de ambos comandos se engloba dentro de la táctica **Discovery – TA007**, donde el adversario está intentando ganar conocimiento sobre el sistema y red interna.

- El caso del comando “net user”, corresponde a la técnica **Account Discovery – T1087**, ya que se utiliza para listar las cuentas de usuario en el sistema, lo cual corresponde con la técnica de descubrimiento de cuentas. Debido a que la ejecución de dicho comando ha tenido lugar de forma local, ls subtécnica mas adecuada para este caso sería, **Local Account: T1087.001.**

- El uso del comando “tasklist” sin embargo corresponde a la técnica **Proccess Discovery – T1057** de descubrimiento de procesos en ejecución.

- Análisis del Incidente:

Con la información obtenida de MITRE ATT&CK, determina:

• ¿Cuál es el objetivo probable del atacante?

Basado en la información obtenida de MITRE ATT&CK y los indicadores de compromiso proporcionados, el objetivo probable del atacante es: **Obtener acceso no autorizado a información sensible y recursos dentro de la red de la organización.**

El atacante intenta comprometer cuentas de usuario (a través de múltiples intentos de inicio de sesión fallidos) y recolectar información crítica sobre el sistema (utilizando los comandos net user y tasklist). Esto sugiere que el atacante busca identificar cuentas válidas y los procesos en ejecución para preparar un ataque más dirigido y eficaz, como la escalada de privilegios, movimiento lateral, o la ejecución de malware.

• ¿Qué tácticas (categorías generales) están siendo empleadas por el atacante?

Como anteriormente se ha mencionado, las tácticas que han sido empleadas por el atacante en esta ocasión son **Credential Access** (TA0006: intentos de adivinar contraseñas para acceder a cuentas del sistema) y **Discovery** (TA0007: recolección de información sobre cuentas y procesos del sistema).

Tarea 3:

Imagina que eres analista de nivel 1 y tienes que subir un evento para reportar el siguiente incidente al MISP:

Fecha	Descripción	IoC	Ataque detectado
26/06/2024	IP Scan	143.234.122.87, 231.89.76.120, 27.165.88.46, 199.32.154.2	Port Scanning

- ¿Qué nivel de amenaza indicarías al subir el evento, teniendo en cuenta que se están reportando varias IPs y el tipo de incidente que es?

El escenario implica que el Security Operations Center (SOC) ha detectado actividad de escaneo de puertos desde varias IPs externas hacia la red de una empresa.

Nivel de amenaza: Medio.

Justificación:

- **Reconocimiento preliminar:** el escaneo de puertos es una técnica usada para mapear la red y descubrir servicios activos y puertos abiertos, aunque no es un ataque en sí, es precursor de explotación de vulnerabilidades.

- **Múltiples IPs involucradas:** La presencia de múltiples IPs sugiere una operación más coordinada y organizada, posiblemente automatizada aumentando el riesgo potencial.

- **Potencial de Escalación:** Aunque el escaneo en sí no compromete directamente los sistemas, identifica posibles puntos de entrada para ataques futuros específicos y personalizados. La detección temprana y la mitigación son esenciales para evitar la escalación de la amenaza.

Tipo de Incidente: Escaneo de puertos (Port Scanning)

El escaneo de puertos es una técnica utilizada para detectar los puertos abiertos en una red y los servicios que están activos en esos puertos. Es una técnica de reconocimiento que permite a los atacantes mapear la red y encontrar puntos de entrada potenciales.

- ¿Qué información indicarías de este evento como descripción?

Port Scanning.

- De entre las siguientes opciones para Categoría – Tipo del IoC que se debe añadir como atributo, ¿cuál crees que es la que más se ajusta a este incidente?

a) Network activity – IP src

b) Network activity – IP dst

c) Other - Port

d) Ninguna de las anteriores es correcta

a) Network activity – IP src: este tipo de categoría "ip-scr" sería la mas adecuada ya que el ataque captado de escaneo de puertos se ha realizado a partir de las IPs fuente identificadas: 143.234.122.87, 231.89.76.120, 27.165.88.46 y 199.32.154.2.

- ¿Qué valor/es se debería/n añadir como "atributo"?

Para este tipo de incidente, se deben añadir los valores de las direcciones IP detectadas en el escaneo. Los atributos a incluir serían las direcciones IP de origen que participaron en el escaneo:

- IP src: 143.234.122.87
- IP src: 231.89.76.120
- IP src: 27.165.88.46
- IP src: 199.32.154.2

- De los "tags" que se muestran a continuación, ¿cuál/es debería/n añadirse en este evento?

circl: incident-classification="scan"

circl: incident-classification="scam"

circl: incident-classification="denial-of-service"

circl: incident-classification="system-compromise"

El "tag" mas adecuado en este caso es:

- **circl: incident-classification="scan"**

Este "tag" es indicativo de un escaneo de puertos que es exactamente el evento que ha sido detectado.

- Investiga la matriz de MITRE ATT&CK de Tácticas y Técnicas, ¿cuál crees que puede ser la más indicada/relacionada con este caso?

Táctica: Reconnaissance TA0043: El adversario intenta obtener información que puede usar para planear ataques futuros.

Técnica: Active Scanning T1595: El adversario realiza escaneos activos de reconocimiento para obtener información que puede ser usada como objetivo.

Tarea 4:

Imagina que eres analista de nivel 1 y tienes que subir un evento para reportar el siguiente incidente al MISP:

Fecha	Descripción	IoC	Ataque detectado
26/06/2024	Attempted SQL Injection detected	222.134.54.12	SQL Injection

- ¿Qué nivel de amenaza indicarías al subir el evento, teniendo en cuenta el tipo de incidente que es?

Nivel de amenaza: Alto

Considero que el nivel **Alto** es adecuado debido a la severidad del ataque y la necesidad de una respuesta rápida. Sin embargo, si el sistema comprometido es crítico para la operación de la organización (por ejemplo, bases de datos de clientes, sistemas financieros, etc.), se consideraría el nivel **Crítico** apropiado para reflejar la urgencia y el potencial impacto devastador del ataque.

Justificación:

- **Naturaleza del ataque**: La inyección SQL es una técnica extremadamente peligrosa que permite a los atacantes ejecutar comandos SQL maliciosos en una base de datos. Esto puede resultar en la filtración de datos sensibles, modificación de datos críticos, o incluso en la obtención del control total del sistema afectado.

- **Impacto**: Una inyección SQL exitosa puede comprometer la confidencialidad, integridad y disponibilidad de los datos. Además, puede permitir a los atacantes acceder a otros sistemas internos, facilitando ataques adicionales y potencialmente más graves.

- **Contexto**: La detección de este ataque indica que hay un ataque activo en la aplicación. Dado que el ataque ya ha ocurrido, es fundamental iniciar una investigación inmediata para determinar las consecuencias y mitigar cualquier daño adicional.

- ¿Qué información indicarías de este evento como descripción?

SQL Injection.

- De entre las siguientes opciones para Categoría – Tipo del IoC que se debe añadir como atributo, ¿cuál crees que es la que más se ajusta a este incidente?

a) Network activity– IP src

b) Network activity– IP dst

c) Payload Installation– Vulnerability

d) Ninguna de las anteriores es correcta

a) **Network activity – IP src**: Este tipo de categoría "ip-src" sería la más adecuada ya que el intento de inyección SQL fue detectado desde la IP fuente 222.134.54.12.

- ¿Qué valor/es se debería/n añadir como "atributo"?

Para este tipo de incidente, se deben añadir los valores de la dirección IP detectada en el intento de inyección SQL:

- IP src: 222.134.54.12

- De los "tags" que se muestran a continuación, ¿cuál/es debería/n añadirse en este evento?

circl: incident-classification="scan"

circl: incident-classification="system-compromise"

circl: incident-classification="vulnerability"

circl: incident-classification="sql-injection"

El tag más adecuado en este caso es:

- **circl: incident-classification="sql-injection"**

Este tag es específico para la clasificación del incidente de inyección SQL detectado en la red.

- Investiga la matriz de MITRE ATT&CK de Tácticas y Técnicas, ¿cuál crees que puede ser la más indicada/relacionada con este caso?

- **Táctica: Initial Access TA0001:** son técnicas usadas como vector de entrada en la organización.
- **Técnica: Exploit Public-Facing Application T1190:** En este caso la aplicación explotada es una base de datos SQL.
- **T1059.007, execution**

Tarea 5:

Escenario del Incidente:

Imagina que eres un analista de seguridad y has detectado que la web de tu organización no funciona correctamente. Un atacante parece estar realizando una denegación de servicio.

Detalles del Incidente:

Descripción: Se ha detectado una caída significativa del rendimiento y disponibilidad del sitio web de la empresa. Se observó un aumento repentino del tráfico entrante que saturó los recursos del sistema dejando la web inaccesible para usuarios legítimos.

Fecha y Hora: 29 de junio de 2024, 02:00 AM UTC

Indicadores de Compromiso (IoC):

• Picos de tráfico entrante superior al 500% del promedio hacia los puertos 80 y 443 del servidor web

• Múltiples solicitudes HTTP/HTTPS desde un gran número de IPs diferentes, en su mayoría provenientes de países como China, Rusia y Corea del Norte

• Uso anormal del 100% de CPU y memoria en los servidores web

Tareas:

- ¿A qué técnica del marco MITRE ATT&CK corresponde el ataque de denegación de servicio descrito en el ejemplo?

- **Técnica: Endpoint Denial of Service T1499:** Esta técnica es usada por los atacantes cuando realizan ataques de denegación de servicio en los endpoints para degradar o

bloquear la disponibilidad de servicios para los usuarios. Este ataque puede llevarse a cabo agotando los recursos del sistema en los que se alojan esos servicios o explotando el sistema para causar una condición de falla persistente.

- **Subtécnica: Service Exhaustion Flood T1499.002**: Este tipo se refiere a la saturación de los recursos del servicio web específico, que en este caso son los servidores web que están recibiendo un tráfico masivo y anómalo, resultando en un uso anormal del 100% de CPU y memoria.

- ¿Qué otros tipos de técnicas de MITRE ATT&CK podrían estar relacionadas con un incidente de denegación de servicio?

Además de la técnica T1499, otras técnicas relacionadas serían:

- **Network Denial of Service T1498:** La denegación de servicio en la red se lleva a cabo agotando el ancho de banda de la red del que dependen los servicios.
    - **Reflection Amplification T1498.002**: Utiliza servidores intermedios para amplificar el ataque.
- **Application Layer Protocol T1071:** Esta técnica puede involucrar el uso de protocolos de aplicación, como HTTP/HTTPS, para enviar tráfico malicioso que forma parte de un ataque de denegación de servicio. Los atacantes pueden abusar de estos protocolos para disfrazar su tráfico como tráfico legítimo.
- **Resource Hijacking T1496:** Los atacantes pueden intentar secuestrar recursos del sistema, como CPU, memoria o ancho de banda, para llevar a cabo ataques de denegación de servicio.

- ¿Cómo se podría utilizar el marco MITRE ATT&CK para mejorar la preparación y respuesta ante futuros ataques de denegación de servicio?

El marco MITRE ATT&CK puede ser una herramienta poderosa para mejorar la preparación y respuesta ante futuros ataques de denegación de servicio (DoS) desde varios enfoques.

1. **Identificación y Catalogación de Técnicas de Ataque**:
    - **Mapeo de Técnicas**: Utilizar el marco para identificar y mapear todas las técnicas de ataque conocidas relacionadas con DoS, como T1499 (Denial of Service), T1498 (Network Denial of Service), y otras técnicas asociadas.
    - **Actualización Continua**: Mantenerse al día con las últimas técnicas y tácticas documentadas en MITRE ATT&CK para ajustar las defensas y estrategias de respuesta.
2. **Evaluación y Fortalecimiento de Defensas**:

- **Análisis**: Realizar un análisis de brechas comparando las capacidades defensivas actuales con las técnicas documentadas en ATT&CK. Esto ayuda a identificar áreas vulnerables que necesitan mejoras.

- **Implementación de Controles**: Basado en el análisis, implementar controles técnicos, como sistemas de detección y prevención de intrusiones (IDS/IPS), firewalls de aplicaciones web (WAF), y capacidades de monitoreo de red para detectar y mitigar ataques DoS.

3. **Simulación y Ejercicios de Ataque**:

   - **Red Team**: Organizar ejercicios de red team donde se simulen ataques de DoS usando las técnicas descritas en ATT&CK. Esto ayuda a probar la efectividad de las defensas y a identificar puntos débiles.

   - **Purple Team**: Colaboración entre equipos de red y equipos de defensa (blue team) para mejorar las capacidades de detección y respuesta, ajustando las defensas en tiempo real basándose en las simulaciones.

4. **Respuesta a Incidentes y Mejora Continua**:

   - **Playbooks de Respuesta**: Desarrollar y actualizar playbooks de respuesta a incidentes basados en las técnicas de MITRE ATT&CK. Estos playbooks deben incluir procedimientos específicos para identificar, contener y mitigar ataques de DoS.

   - **Lecciones Aprendidas**: Después de cada incidente, realizar análisis post-incidente y ajustar los playbooks y defensas basados en las lecciones aprendidas y en las técnicas de ATT&CK.

5. **Entrenamiento y Capacitación**:

   - **Capacitación del Personal**: Entrenar al personal de seguridad en las técnicas y tácticas de ATT&CK para que puedan identificar y responder eficazmente a los ataques de DoS.

   - **Simulacros Regulares**: Realizar simulacros regulares para garantizar que todo el personal esté familiarizado con los procedimientos y pueda actuar rápidamente durante un incidente real.

6. **Monitoreo y Detección**:

   - **Alertas y Correlación de Eventos**: Configurar sistemas de monitoreo para generar alertas basadas en indicadores de compromiso (IoCs) y técnicas de ATT&CK relacionadas con DoS. Utilizar soluciones SIEM (Security

Information and Event Management) para correlacionar eventos y detectar patrones de ataque.

- **Inteligencia de Amenazas**: Integrar fuentes de inteligencia de amenazas que utilicen el marco ATT&CK para identificar nuevas tácticas y técnicas de ataque y ajustar las defensas en consecuencia.

- ¿Qué tácticas del MITRE ATT&CK se ven reflejadas en las acciones tomadas por el equipo de seguridad durante el incidente?

Las acciones tomadas por el equipo de seguridad durante el incidente pueden reflejar varias tácticas del marco MITRE ATT&CK.

- **Initial Access TA0001**: Identificación y bloqueo de las fuentes de tráfico malicioso que inicialmente comprometen la red.
- **Execution TA0002**: Ejecución de scripts o comandos para mitigar el ataque.
- **Credential Access TA0006:** Verificación de intentos de acceder a credenciales durante el ataque, especialmente si el DoS es una táctica para facilitar otras formas de acceso.
- **Discovery TA0007**: Realización de análisis de red para descubrir y mapear la extensión del ataque, incluyendo la identificación de las direcciones IP y los puertos afectados.
- **Lateral Movement TA008:** Comprobar si los atacantes están utilizando la denegación de servicio como una distracción para realizar movimientos laterales dentro de la red.
- **Collection TA0009**: Recolección de logs y datos de tráfico para analizar y entender el comportamiento del ataque y los métodos utilizados.
- **Exfiltration TA0010**: Asegurarse de que el ataque DoS no está siendo utilizado para cubrir actividades de exfiltración de datos.
- **Command and Control TA0011**: Identificación y bloqueo de canales de comando y control utilizados por los atacantes para coordinar el ataque de DoS.
- **Impact TA0040**: Técnicas como el filtrado de datos para evitar el acceso de los atacantes a datos sensibles. Evaluación del impacto del ataque DoS en la disponibilidad del servicio, la integridad y la confidencialidad de los datos.
- **Reconnaissance TA0043**: Investigar las IPs y patrones de tráfico para identificar la fuente del ataque.