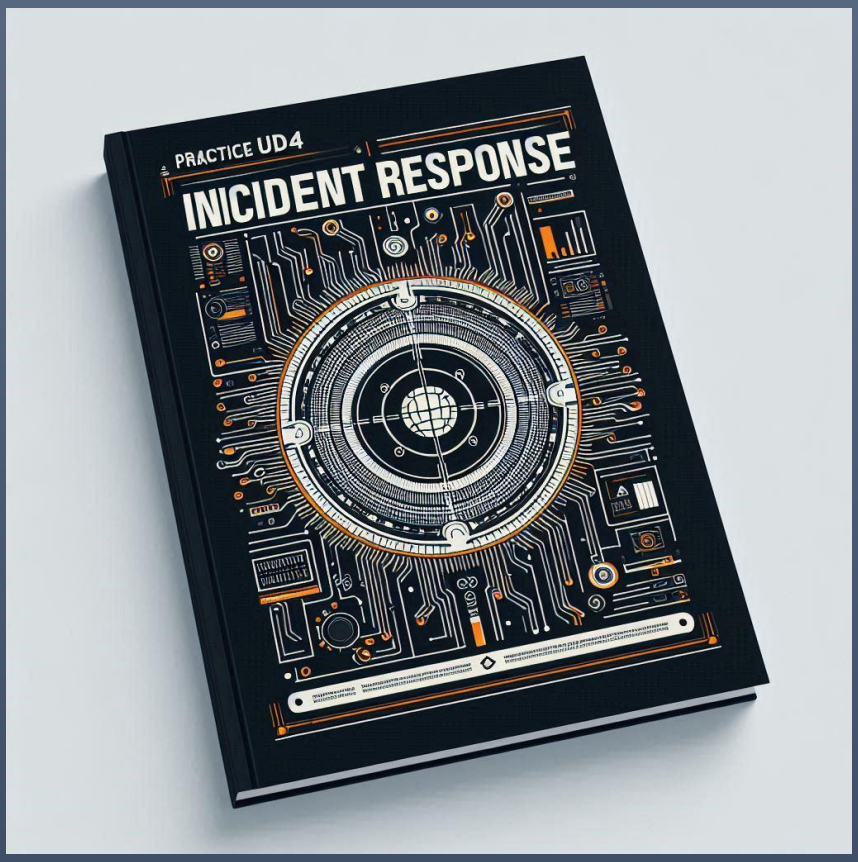
2024




# Incidentes de Ciberseguridad

## PRÁCTICA UD4- RESPUESTA DE INCIDENTES

PEDRO MANUEL GARCÍA ÁLVAREZ

13/05/2024 | int.marisma@gmail.com

# Índice

# Actividad 1 (4p): Aplicación de un Playbook existente

**Descripción del Reto:** El desafío es responder adecuadamente al incidente de formar parte de una botnet y atacar a otra empresa sin saberlo. Esto implica que la red de la empresa ha sido comprometida y está siendo utilizada para lanzar ataques distribuidos de denegación de servicio (DDoS) u otros tipos de ataques cibernéticos contra un tercero.

**Aplicación del Playbook Existente:** Para abordar este incidente, aplicaremos el Playbook "Respuesta a Incidentes de Botnet" proporcionado por el Centro Nacional de Ciberseguridad (NCSC). Este playbook sigue las mejores prácticas y procedimientos para identificar, contener y eliminar la participación involuntaria en una botnet.

Especificación de Actividades por Etapa:

- **Etapa de Identificación del Incidente**:

  1.- Recopilación de Información:
  - Obtener detalles sobre el comportamiento anómalo de la red, como tráfico inusual o patrones de comunicación sospechosos.
  - Revisar registros de eventos y de seguridad para identificar conexiones salientes a direcciones IP conocidas por ser parte de botnets.

  2.- Verificación de la Autenticidad:
  - Confirmar la participación de la empresa en una botnet mediante análisis de tráfico de red y detección de malware.
  - Evaluar el impacto del incidente en los sistemas y la infraestructura de la empresa, así como en terceros afectados por los ataques.

- **Etapa de Contención del Incidente**:

  1.- Aislamiento de Sistemas Afectados:
  - Identificar y aislar los sistemas comprometidos que están participando en la botnet para evitar que continúen siendo utilizados en ataques.
  - Bloquear las comunicaciones salientes con las direcciones IP asociadas a la botnet mediante reglas de firewall y filtrado de tráfico.

- **Etapa de Erradicación del Incidente**:

  1.- Identificación y Eliminación del Malware:

  - Realizar un análisis exhaustivo de los sistemas comprometidos para identificar y eliminar el malware responsable de la participación en la botnet.
  - Actualizar y escanear todos los sistemas afectados con herramientas antivirus y antimalware actualizados.

- **Etapa de Recuperación:**

  1.- Restauración de la Red:

  - Restablecer la configuración de red y los servicios afectados a un estado seguro y funcional.
  - Implementar medidas adicionales de seguridad, como monitoreo continuo de tráfico y actualizaciones de seguridad, para prevenir futuras infecciones.

Al seguir este playbook, el equipo de respuesta estará preparado para identificar, contener y eliminar la participación involuntaria en una botnet, minimizando así el impacto en la empresa y en terceros afectados por los ataques.

## Actividad 2 (1p): Explicación de la ciberresiliencia ante incidentes

La ciberresiliencia ante incidentes es la capacidad de una organización para resistir, adaptarse y recuperarse de eventos cibernéticos adversos. Ante la creciente sofisticación y frecuencia de los ataques cibernéticos, la ciberresiliencia se ha convertido en un aspecto crítico de la seguridad de la información y la continuidad del negocio.

- **Resistencia:** La resiliencia cibernética implica la implementación de medidas preventivas sólidas para evitar o mitigar el impacto de posibles incidentes de seguridad. Esto incluye la adopción de controles de seguridad robustos, como firewalls, sistemas de detección de intrusiones, antivirus actualizados y políticas de seguridad bien definidas. Además, implica la realización de evaluaciones de riesgos regulares y la identificación proactiva de vulnerabilidades para abordarlas antes de que sean explotadas por los adversarios.

- **Adaptabilidad:** La adaptabilidad es otra faceta clave de la ciberresiliencia. Dado el panorama en constante cambio de las amenazas cibernéticas, las organizaciones deben ser capaces de ajustar rápidamente sus estrategias y medidas de seguridad para hacer frente a nuevas y emergentes amenazas. Esto implica tener procesos ágiles de detección y respuesta, así como la capacidad de aprender de incidentes pasados para mejorar continuamente las prácticas de seguridad.

- **Recuperación:** La recuperación es el tercer pilar de la ciberresiliencia. Aunque las medidas preventivas y adaptativas son importantes, ninguna organización puede garantizar una seguridad cibernética absoluta. Por lo tanto, es crucial contar con planes de respuesta a incidentes bien definidos que permitan a la organización recuperarse rápidamente de un incidente y restaurar sus operaciones normales. Esto implica tener copias de seguridad adecuadas y probadas, así como procedimientos claros para restaurar sistemas y datos comprometidos.

En resumen, la ciberresiliencia ante incidentes es fundamental para proteger los activos de una organización y garantizar su continuidad operativa en un entorno cibernético cada vez más hostil. Al combinar resistencia, adaptabilidad y capacidad de recuperación, las organizaciones pueden reducir el impacto de los incidentes de seguridad y mitigar el riesgo de interrupciones graves en sus operaciones.

## Actividad 3 (1p): Especifica cuál es la utilidad de establecer un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.

El establecimiento de un flujo de toma de decisiones y escalado de incidentes, tanto interno como externo, es fundamental para garantizar una respuesta eficaz ante situaciones de seguridad cibernética, como el caso de una botnet. A continuación, se detallan las utilidades de este proceso específicamente en el contexto de una botnet:

### 1.- Coordinación y Organización Interna

- Establecer un flujo de toma de decisiones y escalado interno permite una mejor coordinación y organización de los recursos de la organización involucrados en la respuesta al incidente de la botnet. Define roles y responsabilidades específicos para cada miembro del equipo de respuesta, asegurando que cada uno sepa qué acciones tomar en cada etapa del proceso.

- Esto es crucial para asegurar una respuesta coordinada y efectiva, minimizando el tiempo de respuesta y maximizando la eficiencia de los recursos disponibles.

## 2.- Rapidez de Respuesta

- Un flujo de toma de decisiones bien definido agiliza la respuesta ante el incidente de la botnet al proporcionar un marco estructurado para evaluar, clasificar y escalonar las amenazas.
- Al establecer protocolos claros para la detección temprana, la notificación, la evaluación y la respuesta, se reduce el tiempo necesario para tomar medidas, lo que puede ser crítico en la mitigación del impacto de una botnet.

## 3.- Coordinación Externa y Colaboración

- Además del flujo interno, establecer canales de comunicación y protocolos de escalado externo adecuados es esencial para garantizar una respuesta integral y efectiva.
- Esto implica establecer relaciones con organizaciones y agencias externas relevantes, como proveedores de servicios de seguridad gestionada (MSSP), fuerzas del orden público, CERTs (Equipos de Respuesta a Incidentes de Seguridad Informática), y otros socios de confianza.
- Estos canales permiten compartir información relevante, coordinar acciones conjuntas y acceder a recursos adicionales y experiencia externa, fortaleciendo así la capacidad de respuesta de la organización frente a una botnet.

## 4.- Priorización y Gestión de Recursos

- Un flujo de toma de decisiones bien definido permite priorizar los recursos de acuerdo con la gravedad y el impacto potencial del incidente de la botnet.

- Esto asegura que los esfuerzos se centren en abordar primero las amenazas más críticas, maximizando la eficacia de la respuesta y minimizando las pérdidas.

### 5.- Comunicación Efectiva

- Establecer protocolos claros de comunicación interna y externa garantiza que la información relevante se comparta de manera oportuna y se tomen las medidas adecuadas para gestionar el incidente de la botnet de manera eficiente.
- La comunicación efectiva también ayuda a mantener a todas las partes interesadas informadas sobre el estado del incidente, las acciones tomadas y las medidas de mitigación implementadas, lo que contribuye a la transparencia y la confianza en la gestión del incidente.

## Actividad 4 (1p): Partiendo de un Playbook indica cuales serían las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.

Partiendo de un Playbook diseñado para abordar un incidente de botnet, las tareas de restablecimiento de servicios afectados podrían incluir:

### 1.- Evaluación del Alcance del Incidente

- Evaluar la magnitud del incidente de botnet para determinar qué servicios y sistemas se vieron afectados y en qué medida.

### 2.- Identificación y Aislamiento de Hosts Infectados

- Utilizar herramientas de detección y análisis para identificar todos los hosts infectados por el malware de la botnet.
- Aislar estos hosts de la red principal para evitar la propagación del malware y proteger otros sistemas.

### 3.- Eliminación del Malware

- Utilizar herramientas de eliminación de malware para limpiar los sistemas infectados y eliminar cualquier rastro del malware de la botnet.

- Verificar la integridad de los sistemas afectados después de la eliminación para asegurarse de que estén libres de malware.

## 4.- Restauración de Servicios

- Restaurar los servicios afectados a su estado operativo normal utilizando copias de seguridad limpias y verificadas.
- Asegurar que los servicios restaurados estén configurados correctamente y funcionen según lo esperado.

## 5.- Revisión de Configuraciones y Políticas de Seguridad

- Revisar y actualizar las configuraciones y políticas de seguridad en todos los sistemas afectados para prevenir futuros incidentes similares.
- Implementar controles de seguridad adicionales según sea necesario para mejorar la protección contra botnets y otras amenazas.

## 6.- Capacitación y Concientización del Personal

- Proporcionar capacitación adicional al personal sobre las mejores prácticas de seguridad cibernética, incluida la detección y prevención de infecciones de botnet.
- Reforzar la importancia de la seguridad en línea y la vigilancia constante para evitar caer en trampas de malware.

## 7.- Monitorización Continua

- Implementar una monitorización continua de la red y los sistemas para detectar cualquier actividad sospechosa que pueda indicar una reinfección por botnet u otros ataques.
- Configurar alertas para notificar al equipo de respuesta a incidentes sobre posibles amenazas emergentes.

## 8.- Lecciones Aprendidas

- Realizar una revisión post-incidente para identificar lecciones aprendidas y áreas de mejora en los procedimientos de seguridad y respuesta a incidentes.
- Incorporar estas lecciones aprendidas en futuros planes de respuesta a incidentes y estrategias de seguridad.

Estas tareas, basadas en el Playbook diseñado específicamente para abordar un incidente de botnet, son fundamentales para restablecer los servicios afectados y garantizar la continuidad operativa de la

organización mientras se minimiza el riesgo de futuros ataques de botnet.

# Actividad 5 (1p): Especifica las acciones realizadas y las conclusiones que permitan mantener un registro de lecciones aprendidas ante el incidente.

## 1.- Acciones Realizadas

- **Identificación rápida del incidente**: Se realizó una detección temprana del incidente de botnet, lo que permitió una respuesta inmediata y la contención del malware.
- **Aislamiento de sistemas afectados**: Se identificaron y aislaron rápidamente los sistemas infectados por la botnet para evitar la propagación del malware a otros dispositivos en la red.
- **Eliminación del malware**: Se utilizaron herramientas especializadas para limpiar los sistemas infectados y eliminar completamente el malware de la botnet de los sistemas comprometidos.
- **Restauración de servicios**: Se restauraron los servicios afectados a su estado operativo normal utilizando copias de seguridad verificadas y limpias.
- **Revisión de políticas de seguridad**: Se revisaron y actualizaron las políticas de seguridad para fortalecer la protección contra futuros ataques de botnet y otras amenazas cibernéticas.
- **Capacitación del personal**: Se proporcionó capacitación adicional al personal sobre las mejores prácticas de seguridad cibernética y la detección de amenazas de botnet.
- Monitorización continua: Se implementó una monitorización continua de la red y los sistemas para detectar cualquier actividad sospechosa que pudiera indicar una reinfección por botnet u otros ataques.

## 2.- Conclusiones y Lecciones Aprendidas

- **Importancia de la detección temprana**: Se reconoció la importancia de una detección temprana para minimizar el impacto de los ataques de botnet y otros incidentes de seguridad.
- **Fortalecimiento de las políticas de seguridad**: Se identificaron áreas de mejora en las políticas de seguridad,

especialmente en lo que respecta a la protección contra botnets y malware.

- **Necesidad de capacitación continua**: Se destacó la importancia de proporcionar capacitación continua al personal para aumentar la conciencia sobre las amenazas cibernéticas y promover prácticas seguras en línea.
- **Monitorización proactiva**: Se resaltó la necesidad de una monitorización continua y proactiva de la red y los sistemas para detectar y responder rápidamente a posibles amenazas.

Al mantener un registro detallado de las acciones realizadas y las conclusiones extraídas, la organización puede aprender de la experiencia y mejorar sus prácticas de seguridad cibernética para mitigar el riesgo de futuros incidentes de botnet y otros ataques.

## Actividad 6 (2p): Indica las acciones a realizar para garantizar un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.

- Resume la utilidad de la plataforma https://app.letsdefend.io/ en el contexto del seguimiento de incidentes.
- Cita al menos dos herramientas que conozcas para el seguimiento o ticketing de incidentes. Indica el motivo por el que en ellas existe la posibilidad de integrar Playbooks.

Para garantizar un seguimiento adecuado del incidente de botnet y evitar que una situación similar se vuelva a repetir, se deben tomar las siguientes acciones:

**1.- Análisis Post-Incidente:** Realizar un análisis exhaustivo del incidente de botnet una vez que se haya resuelto por completo. Esto incluye revisar qué causó el incidente, cómo se detectó, cómo se respondió y qué medidas se tomaron para prevenir su recurrencia.

**2.- Actualización de Políticas y Procedimientos:** Basado en el análisis post-incidente, actualizar las políticas y procedimientos de seguridad cibernética para abordar las vulnerabilidades o deficiencias identificadas durante el incidente de botnet. Esto podría incluir mejoras en la detección de amenazas, la respuesta a incidentes y las medidas de protección.

**3.- Capacitación Continua:** Proporcionar capacitación continua al personal en relación con las últimas amenazas cibernéticas, incluidas las botnets. Esto ayudará a mejorar la conciencia de

seguridad y la capacidad de detección temprana dentro de la organización.

**4.- Mejoras en la Monitorización:** Reforzar y ampliar los sistemas de monitorización de seguridad para detectar proactivamente actividades sospechosas que podrían indicar un ataque de botnet u otras amenazas cibernéticas.

**5.- Simulacros de Incidentes:** Realizar simulacros regulares de incidentes de seguridad cibernética, incluidos escenarios de botnet, para poner a prueba la efectividad de los procedimientos de respuesta y identificar áreas de mejora.

**6.- Revisión de Configuraciones de Seguridad:** Revisar y fortalecer las configuraciones de seguridad de la red y los sistemas para mitigar las vulnerabilidades que podrían ser explotadas por botnets u otras amenazas similares.

## Utilidad de la plataforma letsdefend.io en el seguimiento de incidentes:

La plataforma letsdefend.io ofrece una serie de ventajas en el contexto del seguimiento de incidentes:

**1.- Centralización de Datos:** Letsdefend.io permite centralizar todos los datos relacionados con los incidentes en un solo lugar, lo que facilita su seguimiento y análisis.

**2.- Automatización de Respuestas:** La plataforma ofrece capacidades de automatización que permiten definir y ejecutar respuestas automatizadas a incidentes comunes, incluidos los ataques de botnet.

**3.- Análisis Avanzado:** Letsdefend.io proporciona herramientas de análisis avanzado que pueden ayudar a identificar patrones de actividad maliciosa y a mejorar la detección y respuesta a incidentes.

## Herramientas para el seguimiento o ticketing de incidentes:

**1.- Jira Service Management:** Jira es una herramienta ampliamente utilizada para la gestión de proyectos y tickets. Permite el seguimiento detallado de incidentes, asignación de tareas y colaboración entre equipos. La posibilidad de integrar Playbooks en Jira permite automatizar ciertas acciones en

respuesta a incidentes, mejorando así la eficiencia y la consistencia de la respuesta.

https://www.atlassian.com/es/software/jira/service-management/customer-service-software

**2.- ServiceNow:** ServiceNow ofrece una plataforma completa para la gestión de servicios de TI, que incluye funciones de seguimiento de incidentes y gestión de tickets. Al igual que Jira, la integración de Playbooks en ServiceNow permite definir y ejecutar procesos estandarizados para la gestión de incidentes, garantizando una respuesta rápida y eficiente.

https://www.servicenow.com/es/what-is-servicenow.html

# Índice Alfabético

## *I*



## *L*



## *M*



## *N*



## *O*



## *P*



## *R*



## *S*



## *T*

## *U*



## *V*