INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 35

04 DE ABRIL DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplos: DNS open-resolvers o Servidores NTP con monitorización monlist.

Realiza la Gestión del Incidente solicitado siguiendo las siguientes fases :

1º.- Preparación.-

Afecta a todos los activos.-

2º.- Identificación.-

Afecta solamente al equipo con el IDS/IPS.-

3º.- Contención.-

Afecta solamente al equipo con el IDS/IPS.-

4º.- Mitigación.-

Afecta a todos los activos.-

5º.- Recuperación.-

Afecta a todos los activos.-

6º.- Actuaciones post-incidente.-

Activos Informáticos :

1º.- CPD1 : Expedientes académicos + laborales .-

2º.- CPD2 : Moodle Centros (Aula Virtual) + Página Web .-

3º.- Equipos Equipo Directivo +Admon + Sala de Profesoras/es + Ordenadores Departamentos +Ordenador Profesor Aula.-

4º.- Ordenadores de Laboratorio.-

5º.- Elementos de red .-

GESTIÓN DE INCIDENTE—Ddos (Denegación de Servicio)

Preparación

- Identificación y documentación de activos: Enumerar y describir todos los activos informáticos relevantes, incluyendo servidores, redes, sistemas de almacenamiento y equipos terminales. Para cada uno, se debe tener un registro que indique su función, ubicación física y virtual, así como su criticidad para las operaciones del negocio.

- Evaluación de riesgos: Realizar un análisis de riesgos para determinar la importancia y vulnerabilidad de cada activo frente a ataques DDoS. Esto implica evaluar la probabilidad de ocurrencia de un ataque, el impacto potencial en las operaciones del negocio y la efectividad de las medidas de seguridad existentes.

- Implementación de medidas de seguridad: Basándose en los resultados del análisis de riesgos, implementar medidas de seguridad adecuadas para proteger los activos contra ataques DDoS. Esto puede incluir la configuración de firewalls, la implementación de sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), así como la actualización regular de software y parches de seguridad.

Identificación

- Monitoreo con IDS/IPS: Configurar el IDS/IPS para monitorear el tráfico de red en busca de patrones asociados con ataques DDoS, como un aumento repentino en el tráfico de paquetes o solicitudes anómalas a servicios específicos.

- Análisis de registros: Examinar los registros generados por el IDS/IPS y otros sistemas de registro para identificar posibles actividades maliciosas. Esto puede incluir la revisión de registros de servidores DNS y NTP en busca de solicitudes de amplificación.

Contención:

- Bloqueo de tráfico malicioso: Configurar el IDS/IPS para bloquear o filtrar el tráfico malicioso identificado, evitando que llegue a los activos objetivo y minimizando el impacto del ataque.

- Restricción de acceso a servicios susceptibles: Implementar medidas para desactivar o restringir el acceso a los servicios que podrían ser utilizados en ataques DDoS, como asegurar los servidores DNS y NTP mediante la configuración adecuada de acceso y la aplicación de parches de seguridad.

Mitigación

- Implementación de medidas adicionales de seguridad: Reforzar la seguridad de la infraestructura de red mediante la implementación de filtros de paquetes en los routers y firewalls, así como la configuración de sistemas de mitigación de ataques DDoS, como servicios de protección de mitigación de DDoS basados en la nube.

- Actualización y parcheo de sistemas vulnerables: Identificar y corregir las vulnerabilidades de seguridad en los sistemas y aplicaciones afectadas para prevenir futuros ataques DDoS.

Recuperación

- Restauración de servicios afectados: Una vez que se ha mitigado el ataque, restaurar los servicios afectados a su estado normal y realizar pruebas exhaustivas para garantizar su funcionamiento adecuado.

- Revisión post-incidente: Realizar una revisión exhaustiva del incidente para identificar las lecciones aprendidas y las áreas de mejora en los protocolos de seguridad y respuesta a incidentes.

Actuaciones post-incidentes

- Análisis del impacto del incidente: Evaluar el impacto del incidente en los activos informáticos y en la organización en general, teniendo en cuenta aspectos como la interrupción de las operaciones comerciales, el costo financiero y la reputación de la empresa.

- Actualización de medidas de seguridad: Basándose en las lecciones aprendidas del incidente, actualizar y mejorar las medidas de seguridad existentes para mitigar el riesgo de futuros ataques DDoS.

- Capacitación y concienciación del personal: Proporcionar capacitación y concienciación sobre las mejores prácticas de seguridad cibernética al personal de la organización, incluyendo la importancia de mantener los sistemas actualizados y seguros y la necesidad de estar alerta ante posibles amenazas de seguridad.