ESTUDIO DE CASO Nº4

Evaluación del módulo

Profesor: Lautaro Castillo

UNIDAD 4: Implementación del proceso de gestión de incidentes de seguridad de la información

Contexto:

La empresa **SerFinNet S.A.**, dedicada a servicios financieros en línea, experimenta un **ataque DDoS** un lunes a las 9:30 AM. Sus clientes reportan que la plataforma web está **extremadamente lenta o inaccesible**. El equipo de TI detecta un tráfico anómalo que supera los **15 Gbps de solicitudes simultáneas**, principalmente desde direcciones IP distribuidas en múltiples países.

En paralelo, la **central de atención al cliente** recibe cientos de llamadas por reclamos. El ataque provoca la **interrupción parcial de servicios críticos** como transferencias bancarias y consulta de saldos.

La organización cuenta con una **Política de Gestión de Incidentes** basada en la **Norma ISO 27035**, y un **Playbook de Respuesta a DDoS** diseñado previamente. Sin embargo, el equipo de respuesta debe decidir cómo **activar los procedimientos, coordinar con el ISP y proteger la continuidad de los servicios.**

Preguntas de análisis:

1. **Diseño del Proceso**: ¿Qué fases del proceso de gestión de incidentes de la ISO 27035 se deben activar primero en este caso?

2. **Política:** Según la política de gestión de incidentes, ¿qué criterios permiten clasificar este ataque DDoS como un incidente mayor?

3. **Procedimiento:** ¿Qué acciones técnicas inmediatas deberían tomar los analistas para mitigar el ataque?

4. **Playbook**: ¿Qué pasos del playbook de DDoS aplicarías en este escenario?

5. **Comunicación:** ¿Qué medidas de comunicación interna y externa se deben
aplicar durante el incidente?

6. **Lecciones Aprendidas**: Una vez controlado el ataque, ¿qué elementos deberían documentarse para la mejora continua?

Estructura del trabajo

Portada: La portada incluye el título del trabajo, los nombres del autor o de los autores, la afiliación del autor (nombre de la institución), el nombre del curso y profesor/orientador para el cual se presenta el trabajo. También se debe agregar la fecha y el número de página.

Introducción: Presenta el tema, su relevancia e importancia, y proporciona una visión general de lo que se discutirá en el trabajo. También establece el propósito y el alcance del mismo, y presenta la idea principal.

Desarrollo del tema: Expande los puntos clave del trabajo, proporciona evidencia, ejemplos y argumentos que respalden tu tesis. Organiza esta sección de manera lógica y coherente, utilizando párrafos bien estructurados.

Conclusión: Resume los puntos principales discutidos en el trabajo. Puedes ofrecer también reflexiones finales o implicaciones prácticas del tema tratado.

Formato: Documento Word, fuente legible y profesional, Arial 11. Márgenes Superior 2.5 inferior 2.5; Izquierdo 3, derecho 3.

Numeración de páginas: Numerar todas las páginas del documento, generalmente en la esquina superior derecha, excepto en la página de título.

Extensión: máximo 4 páginas, incluida la portada.

Grupos: Los grupos deben estar conformados por 3 integrantes.

Fecha de Entrega: A más tardar el día **jueves 21 de agosto, 23:59 horas**.