Práctica Logs

Parte 1

Ud. está trabajando en una plataforma web que recibe ataques SQLi, IDOR y XSS frecuentemente. Además, durante las noches son atacados mediante payloads que logran que la memoria RAM del servidor se ocupe en su totalidad, haciendo que la plataforma web se caiga.

1. ¿Qué logs definiría a nivel de aplicación? ¿Qué datos registraría por cada log?.
   Rta: definiría logs críticos, de errores, de advertencia y de información. Registraría fecha y hora del ataque, IP de donde provino, user agent, recurso al que se quiso acceder, entre otros aspectos.
2. ¿En qué aspecto de hardware realizaría monitoreo para poder reaccionar ante caídas de la plataforma web?
   Rta: realizaría un monitoreo sobre el uso de la memoria RAM del servidor ya que los ataques a la disponibilidad de nuestro sitio web se realizan sobre este recurso.
3. ¿Qué alertas definiría para enterarse lo antes posible ante un ataque?
   Rta: definiría alertas ante múltiples intentos fallidos de sesión desde una misma dirección IP, comportamientos que parezcan automatizados, exceso en el uso de disco, RAM y red, entre otras alertas.
4. Si el tamaño de los archivos de logs crecen mucho, ¿qué haría?
   Rta: cuando el tamaño de los logs se extienda demasiado, buscaría de separar en unos archivos los logs viejos y en otros los más recientes, para poder eliminar los más antiguos o en su defecto hacer un backup de estos en otro medio de almacenamiento,
5. ¿Considera que una herramienta como Grafana serviría en este caso o prefiere ir por una alternativa más simple? Justifique.
   Rta: considero que si serviría en este caso, ya que simplifica mucho el trabajo del monitoreo del sistema, el establecimiento de alertas, visualización de métricas, etc.

Parte 2

1. Dado el archivo de logs subido a la UV, determinar si hubo intentos de ataques SQLi.
   Rta: Si hubo ataques de SQLi. Para encontrarlos, busqué dentro del archivo de texto diferentes payloads que suelen utilizarse para este tipo de ataques de manera frecuente. Como por ejemplo buscar dos guiones seguidos “--” en alguna de las peticiones.
2. ¿Cómo haría para detectar en tiempo real un ataque SQLi?
   Rta: para detectar ataques SQLi en tiempo real podríamos automatizar la detección de estos en los archivos de logs, de esta manera apenas se genera el registro del log que nos da la información necesaria para saber que estamos siendo atacados la herramienta nos dará una alerta acerca de esto.

Parte 3

Considerando el sistema de Ciudadano Digital de Córdoba (CiDi) y las siguientes 2 APIs.
API 1: Solicitar trámite.
API 2: Eliminar trámite.

1. Definir los riesgos de seguridad asociados a cada API (a nivel técnico). Por ejemplo, “Un ciberdelincuente elimina un trámite de otro ciudadano”.
   Rta:
   a. Ciberdelincuente elimina uno o más trámites de otro ciudadano

   b. Ciberdelincuente averigua el estado de uno o más trámites de otro ciudadano
   c. Ciberdelincuente solicita uno o más trámites en nombre de otro ciudadano
2. Por cada riesgo, definir un nivel de probabilidad de ocurrencia y de impacto.
   Rta:
   a. Probabilidad de ocurrencia: Baja. Impacto: Alto
   b. Probabilidad de ocurrencia: Alta. Impacto: Bajo
   c. Probabilidad de ocurrencia: Media. Impacto: Medio

3. ¿Considera que una gestión de logs correcta podría resolver o minimizar el impacto o la probabilidad de ocurrencia de algún riesgo?
   Rta: Si, porque podríamos detectar si usuarios no autorizados pueden acceder a determinados recursos y tomar medidas correctivas, preventivas y reactivas.