Bastionado de Redes y Sistemas (BRS)

Conceptos Básicos

1. **Activo**

Un **activo** es cualquier recurso dentro de una organización que tiene valor y necesita ser protegido. Los activos pueden ser tangibles, como equipos de hardware, o intangibles, como información, aplicaciones o servicios. La protección de los activos críticos es una prioridad en el bastionado de sistemas y redes.

2. **Riesgo**

El **riesgo** en ciberseguridad es la probabilidad de que una amenaza aproveche una vulnerabilidad en el sistema, causando un impacto negativo en los activos. Los riesgos se gestionan mediante el bastionado y otras prácticas de seguridad que buscan reducir la probabilidad y el impacto de incidentes.

3. **Amenaza**

Una **amenaza** es cualquier evento potencial que puede explotar una vulnerabilidad y causar daño a un activo. Las amenazas pueden ser de distintos tipos, como amenazas internas (empleados malintencionados) o externas (hackers, malware), y pueden ser tanto intencionadas como accidentales.

1. **Vulnerabilidad**

Una **vulnerabilidad** es una debilidad o fallo en el sistema que puede ser explotado por una amenaza. Las vulnerabilidades pueden existir en software, hardware, configuraciones o procesos, y el proceso de bastionado se enfoca en identificarlas y mitigarlas.

5. **Impacto**

El **impacto** es el efecto que tendría la explotación de una vulnerabilidad sobre el activo afectado y, por extensión, sobre la organización. El impacto puede ser financiero, reputacional, legal o relacionado con la pérdida de datos sensibles.

6. **Hardening (Endurecimiento de Sistemas)**

El **hardening** implica asegurar un sistema eliminando vulnerabilidades y configurando de forma segura sus componentes. Incluye la eliminación de servicios innecesarios, la implementación de controles de acceso y el uso de cifrado para reducir la exposición a riesgos.

7. **Superficie de Ataque**

La **superficie de ataque** representa todos los puntos vulnerables del sistema susceptibles a ataques. Reducir esta superficie mediante bastionado y buenas prácticas de configuración es clave para disminuir los riesgos de seguridad.

8. **Gestión de Parches**

Gestionar parches consiste en mantener el software actualizado mediante la aplicación de correcciones que solucionen vulnerabilidades conocidas. Es una de las estrategias más efectivas para reducir la exposición a

amenazas.

9. **Principio de Menor Privilegio**

Este principio sugiere que los usuarios y servicios solo deben tener los permisos mínimos necesarios para cumplir sus funciones. De esta forma, se reduce el impacto de un posible compromiso.

10. **Control de Acceso**

Los **controles de acceso** garantizan que solo los usuarios autorizados puedan acceder a los recursos. Se implementan mediante autenticación y permisos, y forman parte fundamental del bastionado.

11. **Seguridad de la Red**

La seguridad de la red incluye la implementación de firewalls, segmentación de red y control de tráfico para proteger la infraestructura de red. Estas medidas permiten reducir el riesgo de accesos no autorizados y aislar recursos críticos.

12. **Desactivación de Servicios Innecesarios**

Algunos sistemas vienen con servicios activados por defecto que no son necesarios. **Desactivar servicios innecesarios** reduce la cantidad de puntos de entrada y, por tanto, la superficie de ataque.

13. **Registro y Monitoreo**

Registrar y monitorear actividades permite detectar posibles incidentes y responder a ellos rápidamente. Los sistemas bastionados incluyen herramientas de logging que registran eventos importantes y son monitoreadas continuamente.

14. **Cifrado de Datos**

El **cifrado de datos** asegura que, incluso si los datos son interceptados, no puedan ser leídos por personas no autorizadas. Es una práctica esencial para proteger información confidencial tanto en tránsito como en reposo.

15. **Análisis de Vulnerabilidades**

Realizar **análisis de vulnerabilidades** es un proceso preventivo que identifica y evalúa debilidades en sistemas y redes. Esto permite tomar medidas antes de que las vulnerabilidades sean explotadas.

16. **Evaluación de Riesgos**

La **evaluación de riesgos** consiste en identificar, analizar y priorizar riesgos potenciales para el sistema. Este proceso permite asignar recursos de manera eficiente, priorizando el tratamiento de los riesgos que podrían tener el mayor impacto.

17. **Plan de Continuidad del Negocio (BCP)**

El **plan de continuidad del negocio** establece las medidas y procedimientos necesarios para que una organización mantenga sus operaciones críticas durante y después de un incidente de seguridad. Aunque no es específico del bastionado, es parte del enfoque integral de la gestión de riesgos.

- IPS --> Intruder Prevention System