Instituto Tecnológico de Costa Rica

Base de Datos II - IC4302

Clase Presencial - Martes 17 de octubre 2023

Conceptos vistos en clase

- **Snifer:** Tecnología que captura todos los paquetes que llegan a la tarjeta de red, se pueden ver como robots que buscan vulnerabilidades mediante exploits.

Seguridad en Bases de Datos

Physical Security

- **Seguridad Perimetral(Network):** Incluye la red y también el edificio donde se encuentra la base de datos.
- **Collocations(Ubicación Física):**

  Se conoce como la ubicación física que se contrata para tener las bases de datos. Un collocation se organiza en lo que se conoce como un **cage**, lugar donde se encuentran los servidores y también se encuentra custodiado por oficiales de seguridad. Dentro de los cage se encuentran los **racks**, se manejan en medida que se conocen como **US**, y estas definen el tamaño del servidor. Dentro de los racks se encuentran los **Blade Servers** que tienen asociado una controladora de red.

  En el rack se encuentran los servidores y en el mismo rack se encuentra redundancia a nivel de rack, para obtener alta disponibilidad y seguridad de las aplicaciones, se debe tener un espejo del rack original. Además se posee redundancia a nivel de proveedores de internet como lo es **"Internet Service Provider(ISP)"**, por buenas practicas se deben de tener dos proveedores de internet distintos. Los servidores dentro de cada rack poseen tarjetas de red redundantes, permite conectar los ISP necesarios.

- **Hardware:**
- **Servers:**

En una base de datos hay tres tipos de redes:

- **Red privada:** En este tipo de red no se tiene ni entrada ni salida al internet, debido a esto las bases de datos no pueden realizar actualizaciones desde el internet, normalmente se tiene un repo dentro de la red, y gracias a un operador o un proceso, lee los paquetes desde el internet, verifica que sean seguros y luego de esto los paquetes son guardados en el repo, para que seguidamente la base de datos los obtenga.
- **Red pública:** En una red pública nunca se coloca una base de datos, ya que es prohibido, ya que desde el internet, alguien podria llegar a la red pública y es posible salir al internet desde la red pública.
- **Red privada con tráfico de salida: ** En este caso es posible desde la red ir al internet, pero desde el internet no puede llegar a la red, esto implica, que si se tiene una base de datos y se debe realizar una

actualización puedo traerla del internet y realizar la actualización.

Normalmente no se tiene una única red, se deben de tener múltiples redes, al menos deben de ser tres, donde las tres son independientes físicamente y eso garantiza que, si se pierde una de las redes, las otras redes que se tengan van a quedar funcionando.

Una red física se le conoce como **Switch**, este dispositivo de red realiza una red física independiente, es posible tener varias redes en el mismo switch, pero no es muy bueno usarlo debido a que si se pierde un switch, se pierden las tres redes y se pierde la base de datos, de igual forma los switches posee, fuentes de poder redundantes y conexiones a internet redundantes.

Seguridad a nivel de sistema operativo

- **Service Pack:** Es un conjunto de bug fixed que se deben de aplicar en un servidor, a nivel de bases de datos, siempre que haya un service pack nuevo se debe de aplicar, esto sirve para evitar posibles **exploits**, los exploits funcionan de forma que cuando se identifica una vulnerabilidad lo ataca inmediatamente.
- **Upgrades Patches:** Es parte de Linux y además son un conjunto de bug fixed o también mejoras al software como lo son, aumento del mejora de inscripción que va a tener la base de datos, mejora en los protocolos de comunicación entre servidores.

Sistemas de detección de intrusos

- **Access Logs:** Mediante un análisis, dan patrones de uso de los usuarios y según las acciones del usuario levantaría un red flag.
- **Audit(Security Logs):** Guardan todo lo que hacen los usuarios y esto produce un track de las acciones que realizan los usuarios, los service acount y la base de datos.
- **LDAP(Base de datos de seguridad):** Centraliza la autenticación y la autorización de usuarios, cuando se debe autorizar, se autoriza desde LDAP y toda la información se replica a los otros servidores, de igual forma con la autenticación.
- **Service Account:** Mediante la base de datos que se utilice en ese momento, se restringe según el usuario que se desee, el acceso a diferentes acciones que se puedan utilizar en la base de datos, esto a nivel de file system, también limitan permisos a nivel de red.

Conceptos:

- **Principals:** Individuos que tienen acceso a la base de datos.
- **Grupos:** Los permisos se heredan a los usuarios.
- **Proccess** No poseen una sesión interactiva, eso quiere decir que son indicadores de un posible hackeo al intentar crear una.

Funcionamiento a nivel de Cloud

Amazon posee un servicio llamado Identity and access managment(IAM), dicho servicio maneja todo lo que son usuarios. Este servicio posee los conceptos de **usuarios**, concepto de **gupos** y el concepto de **roles**, a nivel de usuarios y grupos solo se utiliza para personas, a nivel de roles es para servicios, además posee

políticas y dan permisos para acceder a los recursos como las bases de datos. Cada rol tiene asociado un servicio.

- **Secure Token Service(STS):** Cada vez que se accede a un servicio, además de que se obtiene el rol, se obtienen permisos antes de acceder al servicio.
- **Políticas de Bloqueo:** Si mediante inteligencia artificial se detecta un patrón de uso no habitual, la política bloquea al usuario, esto a ayuda a ser más activo que reactivo.