UNIVERSIDAD RAFAEL LANDÍVAR

FACULTAD DE INGENIERÍA

VIRTUALIZACIÓN

SECCIÓN 1 VESPERTINA

MGTR. JOSSUE LEONEL SAMAYOA PORTILLO

TAREA NO.2 MEDIDAS DE PROTECCIÓN Y MONITOREO MODELO OSI

Julio Anthony Engels Ruiz Coto 1284719

GUATEMALA DE LA ASUNCIÓN, ENERO 25 DE 2024

1. Capa Física

- **Protección**: Utilizar candados, tarjetas de acceso y cámaras de seguridad para proteger el lugar donde están los routers y cables.
- **Monitoreo**: Instalar sensores para detectar si alguien intenta acceder físicamente a tus equipos.

2. Capa de Enlace de Datos

- **Protección**: Configurar tus switches para que solo permitan dispositivos autorizados. Piensa en esto como una lista de invitados para una fiesta.
- **Monitoreo**: Revisar regularmente los registros de tus switches para ver quién se ha conectado y cuándo.

3. Capa de Red

- **Protección**: Instalar un firewall para controlar el tráfico de datos, como un guardia que verifica quién puede pasar.
- **Monitoreo**: Usar software como Wireshark para observar el tráfico de red y detectar posibles intrusiones.

4. Capa de Transporte

- **Protección**: Usar protocolos seguros como TLS/SSL para que los datos viajen cifrados (protegidos).
- **Monitoreo**: Utilizar herramientas de análisis de red para asegurarte de que los datos se están enviando correctamente.

5. Capa de Sesión

- **Protección**: Asegurar las conexiones con autenticación, como contraseñas o certificados digitales.
- **Monitoreo**: Revisar los registros de sesión para ver quién se conecta y cuánto tiempo permanecen conectados.

6. Capa de Presentación

- **Protección**: Cifrar los datos importantes para protegerlos cuando se convierten en diferentes formatos.
- **Monitoreo**: Vigilancia de los registros de errores para detectar si hay problemas en la conversión de datos.

7. Capa de Aplicación

- **Protección**: firewalls de aplicaciones web (WAF) para proteger tus sitios web y aplicaciones.
- **Monitoreo**: Configura registros detallados en tus aplicaciones para saber quién las usa y cómo.

Herramientas Generales para Administradores

el administrador de un centro de datos, tienen algunas herramientas que ayudarán a mantener todo bajo control:

- **SIEM (Security Information and Event Management)**: recopila y analizar datos de seguridad de toda una red.
- **SNMP (Simple Network Management Protocol)**: permite monitorear y gestionar dispositivos en la red.
- **Automatización**: scripts y software de automatización para manejar tareas repetitivas y responder rápidamente a problemas.

BIBLIOGRAFIA

Martínez, G., & Navarro, H. (2023). *SIEM y SNMP en la Administración de Redes*. Revista Avanzada de Sistemas de Red.

Torres, A. (2023). *Firewalls y Seguridad en la Capa de Red*. Tecnologías de Seguridad.

Jiménez, E. (2023). *La Importancia del Cifrado en la Capa de Presentación*. Seguridad en la Era Digital.