Nombre del Alumno: ***Vania Natali Santizo Morales***

Nombre del tema: ***Trabajo Plataforma 2***

Parcial: ***2° Parcial***

Nombre de la Materia: ***Seguridad En La Información***

Nombre del profesor: ***Andres Alejandro Reyes Molina***

Nombre de la Licenciatura: ***Ingeniería en Sistemas Computacionales***

Cuatrimestre: ***9°***

SEGURIDAD EN REDES Y COMUNICACIONES

3.1 ASPECTOS DE SEGURIDAD EN LAS COMUNICACIONES

Seguir una rutina a la hora de irse a dormir, es decir, acostarse y levantarse a la misma hora todos los días e intentar descansar al menos 8 horas diarias.
3.1 Aspectos de seguridad en las comunicaciones

3.2 DEBILIDADES DE LOS PROTOCOLOS TCP/IP

El modelo TCP/IP presenta vulnerabilidades como suplantación de identidad (spoofing), ataques de hombre en el medio (MITM) y inyección de paquetes maliciosos debido a la falta de cifrado nativo.

3.3 TRANSMISIÓN DE PAQUETES Y PROMISCUIDAD

Algunas redes permiten que dispositivos operen en modo promiscuo, interceptando tráfico de otros equipos, lo que facilita el espionaje y la captura de paquetes sin restricciones.

3.4 REDES LOCALES (VLAN) Y AMPLIAS (VPN)

Las VLAN segmentan redes para mejorar la seguridad y reducir el tráfico innecesario. Las VPN ofrecen comunicación segura a través de redes públicas mediante tunelado y cifrado.

3.5 DOMICILIOS IP

Las direcciones IP identifican dispositivos en la red. Se clasifican en IP pública y privada, y pueden ser dinámicas o estáticas, afectando la conectividad y seguridad.

3.6 VIGILANCIA DE PAQUETES

Técnicas como sniffing y packet inspection permiten analizar el tráfico de red para detectar amenazas o intrusiones

3.7 ESTÁNDARES PARA LA SEGURIDAD EN REDES

Existen normas como ISO/IEC 27001, NIST Cybersecurity Framework y PCI DSS, que guían la protección de datos y la infraestructura de TI.

3.8 VULNERABILIDAD DE LOS PROTOCOLOS INALÁMBRICOS WEP, WPA, WPA2

- WEP: Algoritmo débil, fácilmente vulnerable a ataques.
- WPA: Mejora el cifrado, pero susceptible a ataques de diccionario.
- WPA2: Uso de AES robusto, aunque vulnerable al ataque KRACK.

FIREWALL DE CAPAS INFERIORES

Protege la red desde el nivel de transmisión, filtrando tráfico según direcciones IP y puertos.

3.10 FIREWALL DE CAPA DE APLICACIÓN

Analiza y bloquea tráfico según contenido específico de aplicaciones, evitando ataques dirigidos.

3.11 FIREWALL PERSONAL

Software en dispositivos individuales que protege contra accesos externos no deseados.

3.12 VENTAJAS DE UN FIREWAL

- Bloquea accesos no autorizados.
- Filtra tráfico peligroso.
- Protege contra ataques maliciosos.

3.13 LIMITACIONES DE UN FIREWAL

- No impide ataques internos.
- No protege contra malware avanzado.
- Puede afectar el rendimiento de la red.

3.14 POLÍTICAS DEL FIREWALL

Las reglas deben definirse según el tipo de tráfico permitido y estrategias de seguridad, como listas blancas y negras, inspección de tráfico y control de acceso