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

Nombre del tema: ***Trabajo Plataforma I***

Parcial: ***I° 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°***

Mapa Conceptual sobre PKI y Protocolos de Seguridad

SSH
- Funcionalidad de SSH
  - Secure Shell (SSH) es un protocolo para acceder de manera segura a dispositivos remotos.
  - Proporciona autenticación y cifrado para proteger las conexiones.
- Usos Comunes
  - Se utiliza principalmente para la administración de sistemas y transferencias de archivos seguras.
  - Permite la ejecución remota de comandos en servidores de manera segura.

TSL
- Propósito y Características
  - Transport Layer Security (TLS) es el sucesor de SSL, ofreciendo mejor seguridad.
  - Proporciona cifrado, autenticación y garantía de integridad de datos.
- Aplicaciones de TSL
  - Se utiliza en diversas aplicaciones, incluyendo navegadores web y correo electrónico.
  - Permite establecer conexiones seguras en una variedad de protocolos de red.

SSL
- Definición y Función
  - Secure Sockets Layer (SSL) es un protocolo de seguridad que cifra la comunicación entre aplicaciones.
  - Asegura la transmisión de datos confidenciales en redes.
- Evolución y Relevancia
  - Ha sido reemplazado en gran medida por TLS, aunque todavía se utiliza en algunas aplicaciones.
  - La seguridad depende de la correcta implementación y configuración.

Ejemplo de un protocolo de seguridad: HTTPS
- Caracteristicas de HTTPS
  - Protocolo que utiliza SSL/TLS para asegurar la comunicación en la web.
  - Garantiza la confidencialidad, integridad y autenticación en las conexiones.
- Implementación de HTTPS
  - Se utiliza comúnmente en sitios web para proteger datos sensibles.
  - Requiere la obtención de un certificado SSL de una CA.

Estándares y protocolos de certificación
- Normas Relevantes
  - Incluyen X.509 para certificados y PKCS para la gestión de claves.
  - Establecen las especificaciones para asegurar la interoperabilidad.
- Protocolos de Seguridad
  - Protocolos como OCSP para la validación en tiempo real de certificados.
  - Protocolos para la distribución segura de claves y certificados.

Distribución de claves
- Propósito y Función
  - Facilitar el intercambio seguro de información entre partes mediante el uso de claves criptográficas.
  - Asegurar que las claves sean accesibles para los usuarios autorizados.
- Características Clave
  - Utiliza diferentes métodos para distribuir las claves, como la infraestructura de clave pública (PKI).
  - Puede incluir la generación de claves en un entorno seguro.

Certificación
- Componentes de la Certificación
  - Utiliza entidades de certificación (CA) que emiten certificados digitales.
  - Los certificados garantizan la identidad de los usuarios y dispositivos en una red.
- Proceso de Certificación
  - Implica la verificación de la identidad del solicitante antes de emitir un certificado.
  - Incluye pasos como la solicitud, validación y emisión del certificado.

Componentes de una PKI
- Elementos Esenciales
  - Incluye entidades de certificación, registros de certificados, y autoridades de registro.
  - Proporciona la infraestructura necesaria para la gestión de claves y certificados.
- Funciones de los Componentes
  - Las entidades de certificación emiten y gestionan certificados.
  - Los registros de certificados mantienen un historial de los certificados emitidos.

Arquitecturas PKI
- Tipos de Arquitecturas
  - Puede ser jerárquica, con múltiples niveles de CA, o de malla, donde todas las CA son iguales.
  - Cada arquitectura tiene sus propias ventajas y desventajas en términos de escalabilidad y seguridad.
- Ejemplos de Implementación
  - Arquitectura jerárquica: una CA raíz con varias CA subordinadas.
  - Arquitectura de malla: CA interconectadas sin jerarquía estricta.

Políticas y prácticas de certificación
- Importancia de las Políticas
  - Establecen las normas y procedimientos para la emisión y gestión de certificados.
  - Aseguran la conformidad y la confianza en la infraestructura de certificación.
- Prácticas Comunes
  - Inclusión de criterios de validación y requisitos de seguridad.
  - Documentación de procedimientos para el manejo de certificados revocados.

Gestión de una PKI
- Tareas Clave en la Gestión
  - Implica la creación, emisión, renovación y revocación de certificados.
  - Requiere monitorear el estado y la seguridad de la PKI continuamente.
- Herramientas de Gestión
  - Software especializado para gestionar la infraestructura de certificados.
  - Monitoreo de registros y auditorías para garantizar el cumplimiento.