**1.- POP3 (Post Office Protocol version 3)**

1.1.- Introducción

POP3 es un protocolo utilizado por clientes de correo electrónico para recuperar mensajes de un servidor de correo. Es uno de los protocolos más antiguos y comunes para la recepción de correos electrónicos.

1.2.- Detalles

• Nombre Protocolo: POP3

• Capa en que el protocolo funciona en el modelo OSI: Capa 7 (Aplicación)

• Puertos usados por defecto: 110

• Puertos Usados Seguros: 995 (POP3S)

• Descripción del Servicio que ofrece: Permite a los clientes de correo electrónico descargar mensajes desde un servidor de correo.

• ¿Cómo funciona?: El cliente se conecta al servidor POP3, autentica al usuario, descarga los mensajes y luego los elimina del servidor (aunque esto puede configurarse para que no se eliminen).

• Software típico que lo utiliza: Microsoft Outlook, Mozilla Thunderbird, Apple Mail.

**2.- SSL/TLS (Secure Sockets Layer / Transport Layer Security)**

2.1.- Introducción

SSL y su sucesor TLS son protocolos criptográficos diseñados para proporcionar comunicaciones seguras a través de una red informática.

2.2.- Detalles

• Nombre Protocolo: SSL/TLS

• Capa en que el protocolo funciona en el modelo OSI: Capa 6 ( (Presentación)

• Puertos usados por defecto: No tiene puertos específicos, se usa en combinación con otros protocolos (ej. HTTPS usa el puerto 443).

• Puertos Usados Seguros: Depende del protocolo con el que se combine (ej. HTTPS usa 443).

• Descripción del Servicio que ofrece: Proporciona cifrado y autenticación para asegurar la comunicación entre dos puntos.

• ¿Cómo funciona?: Utiliza un sistema de cifrado basado en certificados para establecer una conexión segura entre el cliente y el servidor.

• Software típico que lo utiliza: Navegadores web, servidores web, clientes de correo electrónico.

**3.- HTTPS (Hypertext Transfer Protocol Secure)**

3.1.- Introducción

HTTPS es una versión segura de HTTP, que utiliza SSL/TLS para cifrar la comunicación entre el navegador web y el servidor web.

3.2.- Detalles

• Nombre Protocolo: HTTPS

• Capa en que el protocolo funciona en el modelo OSI: Capa 7 (Aplicación)

• Puertos usados por defecto: 443

• Puertos Usados Seguros: 443

• Descripción del Servicio que ofrece: Proporciona una comunicación segura y cifrada para la transferencia de datos en la web.

• ¿Cómo funciona?: Combina HTTP con SSL/TLS para cifrar los datos transmitidos entre el cliente y el servidor.

• Software típico que lo utiliza: Navegadores web, servidores web.

**4.- WPA3 (Wi-Fi Protected Access 3)**

4.1.- introducción

WPA3 es el estándar de seguridad más reciente para redes Wi-Fi, diseñado para mejorar la seguridad en comparación con WPA2.

4.2.- Detalles

• Nombre Protocolo: WPA3

• Capa en que el protocolo funciona en el modelo OSI: Capa 2 (Enlace de Datos)

• Puertos usados por defecto: No aplica (es un protocolo de seguridad para redes inalámbricas).

• Puertos Usados Seguros: No aplica.

• Descripción del Servicio que ofrece: Proporciona autenticación y cifrado mejorados para redes Wi-Fi.

• ¿Cómo funciona?: Utiliza SAE (Simultaneous Authentication of Equals) para una autenticación más segura y cifrado de 192 bits.

• Software típico que lo utiliza: Routers Wi-Fi, dispositivos móviles, computadoras portátiles.

**5.- SNMPv3 (Simple Network Management Protocol version 3)**

5.1.- Introducción

SNMPv3 es una versión mejorada del protocolo SNMP que incluye características de seguridad como autenticación y cifrado.

5.2.- Detalles

• Nombre Protocolo: SNMPv3

• Capa en que el protocolo funciona en el modelo OSI: Capa 7 (Aplicación)

• Puertos usados por defecto: 161 (UDP)

• Puertos Usados Seguros: 161 (UDP) con seguridad mejorada.

• Descripción del Servicio que ofrece: Permite la gestión y monitoreo de dispositivos en una red.

• ¿Cómo funciona?: Utiliza mensajes GET, SET y TRAP para intercambiar información de gestión entre el administrador de red y los dispositivos gestionados.

• Software típico que lo utiliza: Nagios, Zabbix, SolarWinds.

**6.- SSH (Secure Shell)**

6.1.- Introducción

SSH es un protocolo de red que permite la administración remota segura de sistemas y la transferencia segura de archivos.

6.2.- Detalles

• Nombre Protocolo: SSH

• Capa en que el protocolo funciona en el modelo OSI: Capa 7 (Aplicación)

• Puertos usados por defecto: 22

• Puertos Usados Seguros: 22

• Descripción del Servicio que ofrece: Proporciona una conexión segura para la administración remota de sistemas y la transferencia de archivos.

• ¿Cómo funciona?: Establece una conexión cifrada entre el cliente y el servidor utilizando técnicas de criptografía asimétrica y simétrica.

• Software típico que lo utiliza: OpenSSH, PuTTY, SecureCRT.