TRABAJO DE INVESTIGACION

PROTOCOLOS DE LAS CAPAS OSI

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 donde funciona en el modelo OSI: Capa 7 (Aplicación)
- Puertos usado por defecto: 110
- Puertos Usado Seguro: 995 (POP3S)
- Descripción del Servicio: Permite a los clientes de correo electrónico descargar mensajes desde un servidor de correo.
- Funcionamiento: El cliente se conecta al servidor POP3, autenticando al usuario, para descargar los mensajes y luego los elimina del servidor (aunque puede configurarse para que no se eliminen).
- Software: Microsoft Outlook, Mozilla Thunderbird, Apple Mail y otros.

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, proporcionando confidencialidad, integridad y autenticación en la transmisión de datos.

2.2.- Detalles

- Nombre Protocolo: SSL/TLS
- Capa donde funciona en el modelo OSI: Capa 6 ((Presentación)
- Puertos comunes usados:

Protocolo	Puerto	Descripción
HTTPS	443	HTTP sobre SSL/TLS
FTPS	990	FTP sobre SSL/TLS ([1]modo explícito)
FTPS	21	FTP sobre SSL/TLS ([2]modo implícito)
IMAPS	993	IMAP sobre SSL/TLS
POP3S	995	POP3 sobre SSL/TLS
SMTPS	465	SMTP sobre SSL/TLS
SMTP ([3]STARTTLS)	587	SMTP con STARTTLS
LDAPS	636	LDAP sobre SSL/TLS

- Descripción del Servicio: Proporciona cifrado y autenticación para asegurar la comunicación entre dos puntos, usándose en una variedad de servicios de la red.

[1] La conexión comienza sin cifrado y luego se actualiza a una conexión segura mediante comandos adicionales
[2] La conexión comienza directamente como una conexión segura
[3] Es una extensión de algunos protocolos de comunicación que permite la actualización de una conexión no segura a una segura usando SSL/TLS

- Funcionamiento: 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 que el protocolo usa 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.
- Funcionamiento: 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 el modelo OSI: Capa 2 (Enlace de Datos)
- Puertos usados por defecto: No aplica (es un protocolo de seguridad para redes inalámbricas).
- Descripción del Servicio que ofrece: Proporciona autenticación y cifrado mejorados para redes Wi-Fi.
- Funcionamiento: Utiliza el protocolo SAE[4] para una autenticación más segura y cifrado de 192 bits.
- Software que lo utiliza: Routers Wi-Fi, dispositivos móviles, computadoras portátiles, TV y otros.

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

5.1.- Introducción

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

5.2.- Detalles

- Nombre Protocolo: SNMPv3
- Capa 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.

[4] SAE (Simultaneous Authentication of Equals) es un método de autenticación basado en contraseñas que proporciona una mayor seguridad que el PSK en el WPA2, con mejoras ante ataques por fuerza bruta debido al uso del protocolo "Dragonfly" (protocolo que mejora la seguridad de redes wi-fi) para el intercambio de claves, proporcionando autenticación mutua en ambas partes.

- Funcionamiento: Utiliza mensajes GET[5], SET[6] y TRAP[7] para intercambiar información de gestión entre el administrador de red y los dispositivos gestionados, pero de manera mas segura en la autenticación, integridad y privacidad.
- Software típico que lo utiliza: Herramientas de monitorización de redes y sistemas como Nagios, Zabbix, SolarWinds, siendo las dos primeras de código abierto y la ultima con licencia comercial, siendo más fácil de usar y aprender Zabbix.

6.- SSH (Secure Shell)

6.1.- Introducción

SSH es un protocolo de red criptográfico que permite la administración remota segura de sistemas y la transferencia segura de archivos, operando de manera segura en redes inseguras.

6.2.- Detalles

- Nombre Protocolo: SSH
- Capa en el modelo OSI: Capa 7 (Aplicación)
- Puertos usados por defecto: 22
- Puertos Usados Seguros: 22
- Descripción del Servicio: Proporciona una conexión segura para la administración remota de sistemas y la transferencia de archivos, siendo una herramienta esencial para la administración remota segura de sistemas y redes, proporcionando autenticación segura, cifrado de datos, integridad de datos y capacidades de túneles seguros

5 Se usa para la recuperación de la información de un dispositivo gestionado con autenticación y cifrado, realizando una solicitud GET a un agente SNMP, incluyendo credenciales de autenticación verificando la identidad del gestor, cifrándose llegando a destino.
6 Se usa para modificar la configuración de un dispositivo gestionado, enviando el gestor SNMP solicitud SET a un agente SNMP, con autenticación y cifrado llegando a destino.
7 Se usa para enviar notificaciones asíncronas desde un agente SNMP al gestor SNMP generando un TRAP cuando ocurre un suceso significativo en la red, con las mismas medidas de seguridad que GET y SET.

- Funcionamiento: Establece una conexión cifrada entre el cliente y el servidor utilizando técnicas de criptografía asimétrica y simétrica.
- Software: OpenSSH, PuTTY, SecureCRT son tres herramientas populares para la administración remota segura utilizando el protocolo SSH, siendo las 2 primeras de código abierto y la ultima con licencia comercial, siendo la considerada más robusta y segura. En Linux la mas usada es OpenSSH, aunque existen versiones también para los demás programas.