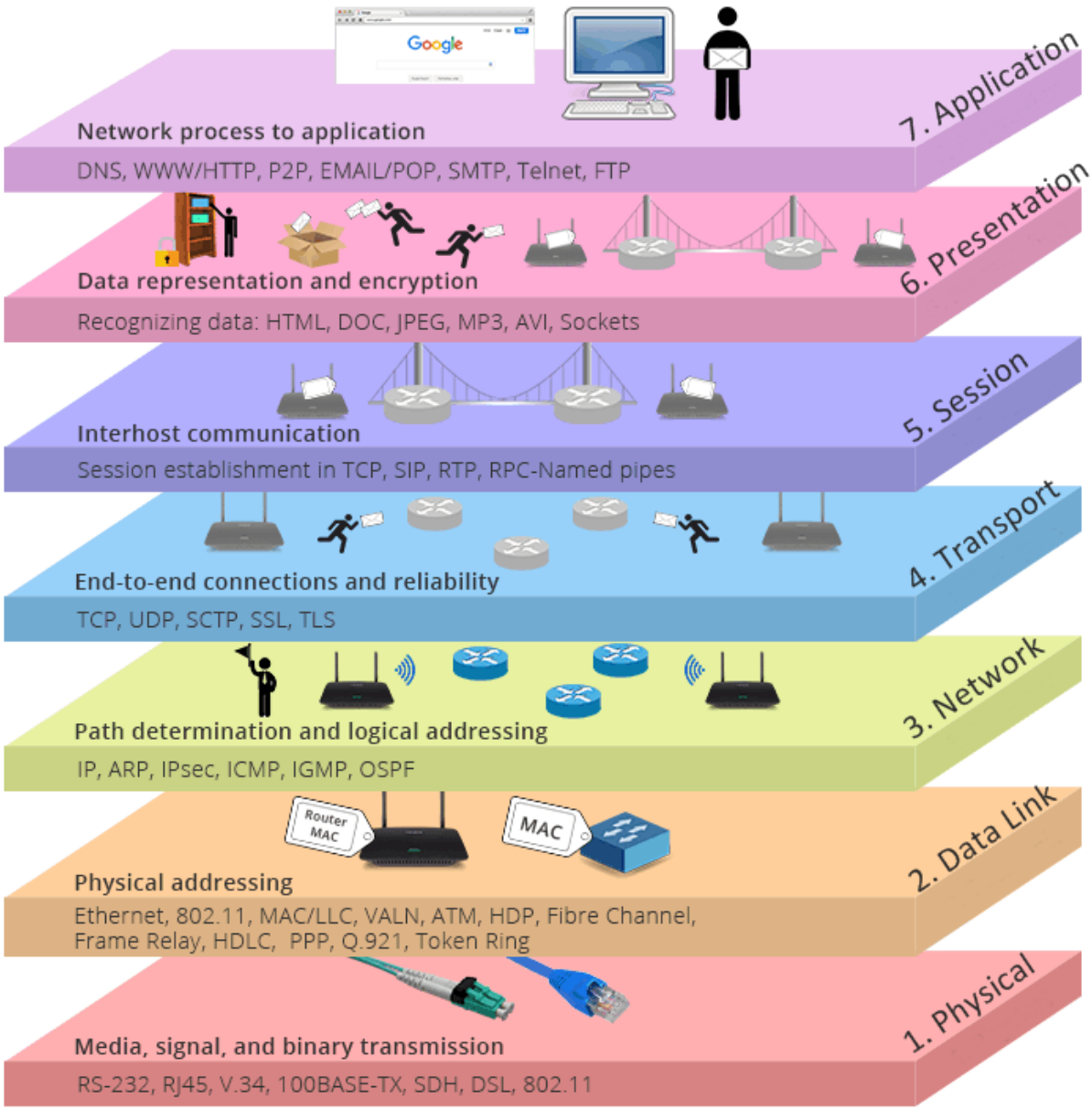
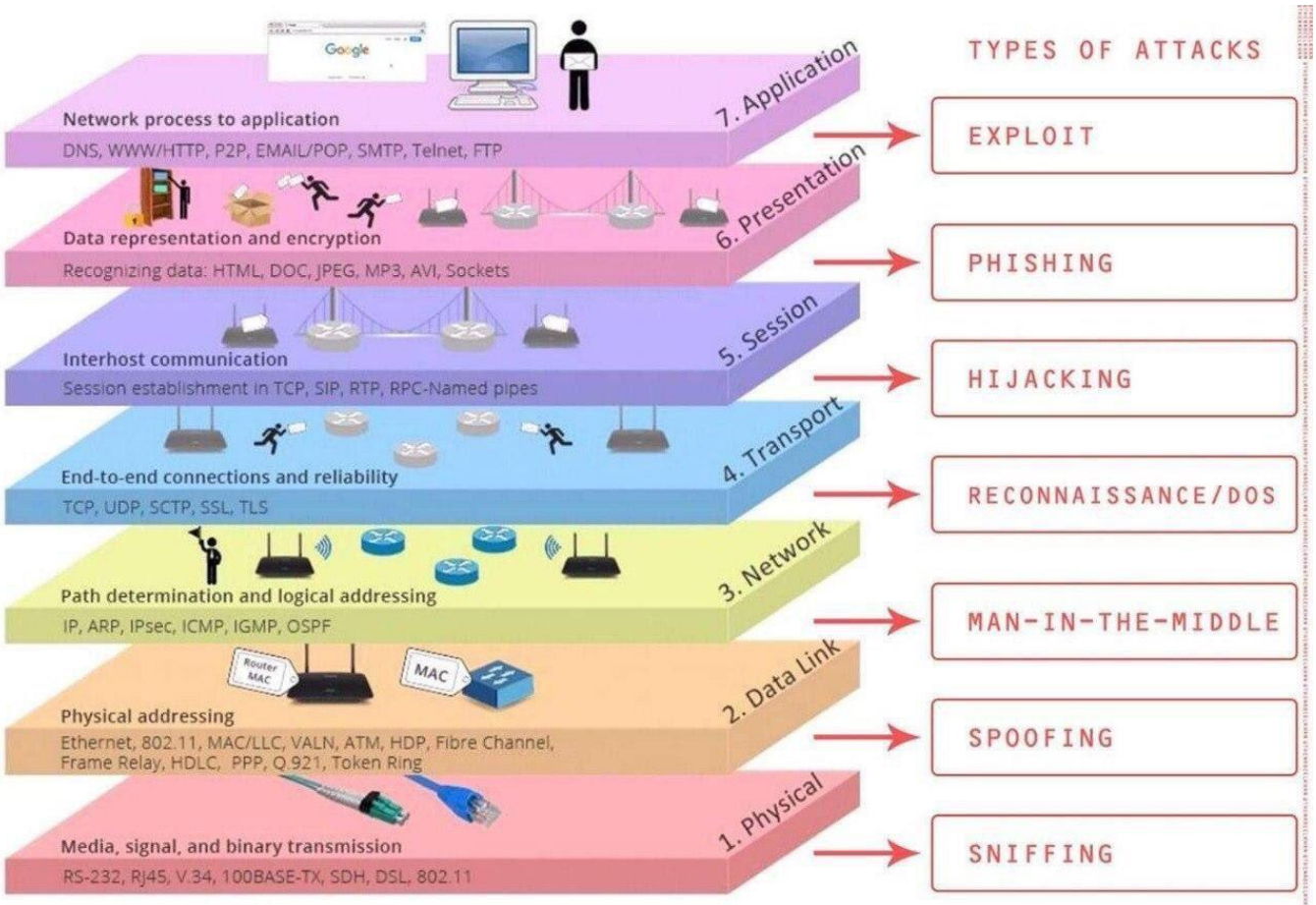
Modelo OSI

14.-Introduuccion

Se compone de 7 capas, nos permite entender cómo se realizan las comunicaciones y todas las fases, y las virtudes de cada una, gracias a esto podemos identificar los posibles errores dentro de la red





15.-Capa1/Nivel físico

Comunicaciones se realizan a través de señales eléctricas en un circuito de memoria

Funciones:

- codificación de datos
- detección de colisiones
- modulación de la señal
- conversión analógica digital

En esta capa encontraos protocolos como: PPP, Frame Realy, ethernet.

Desde la seguridad informática, aquí se debe impedir el acceso a terceros, es decir a accesos no autorizados.

Si se habla de un data center donde físicamente se encuentran los servidores, por la norma ISO27001 se recomienda colocar cámaras y control de acceso biométrico

Se encarga de la gestión física de la red, de realizar la conversión física modulación y codificación, y la conversión entre los datos físicos diferenciando el ordenador y la red.

16.-Capa2/Enlace de datos

Direccionamiento físico (MAC y LLC)

Encargado de transferir datos de forma confiable dentro del circuito de transferencia de datos

Funciones:

- establecimiento, control y finalización de los enlaces

- controla el volumen de información

- control de errores gestión

- evita el flujo que sature el equipo siguiente

Comunica la capa de red con la capa física. Los switches son ejemplos de un dispositivo importante en esta capa

La inutilización de los puertos sin utilizar es clave en esta capa, evita las conexiones fraudulentas o Ataques de envenenamiento ARP, hombre de en medio.

También aquí podemos encontrar los protocolos seguros de comunicación como ser pueden ser el WPA2 o WPA para medios inalámbricos.

17.-Capa3/Red

Determinación de ruta direccionamiento lógico(ip)

Permite la comunicación entre dispositivos que se encuentran en redes distintas. De esta forma estos dispositivos se pueden comunicar por más que no haya una comunicación directa.

Funciones:

- identificar equipos de red

- enrutamiento del trafico

- control de gestión de red

Se encarga del encaminamiento de paquetes entre redes. Su esquema es el direccionamiento a través de niveles que son direcciones IP, centralizado por un router o servidor

Como hablamos de router o servidor las medidas de seguridad son el control no autorizado de ingreso a través de contraseñas fuertes y la configuración de protocolos de administración a través de conexiones cifradas

Existen vulnerabilidades de protocolos como ser el RIP u OSPF ya que a través de estos se pueden inyectar routers falsos

Se debe considerar la implementación de Ipsec, que es una suite de protocolos encargado de brindar seguridad

Solo abrir puertos de servicios cuando se estén utilizando

Lista de accesos de control para permitir conexiones entre la red

18.-Capa4/Transporte

transporte conexión de extremo a extremo y control de flujo de datos

Su objetivo es ofrecer un sistema para enviar información sin errores a las capas superiores.

Funciones:

- Entrega la información de forma fidedigna.

- Brinda la información en el orden correcto.

- Gestiona de forma eficiente el flujo de comunicación.

Esta capa toma los datos que vienen de la aplicación, los divide en segmentos y luego lo envía a la capa de red. Los protocolos que usa por excelencia son TCP y UDP, los cuales establecen el vínculo real desde el origen al destino.

La seguridad en esta capa se aplica desde: El cifrado de los datos. Autenticación de todas las partes, prevenir la manipulación que atente contra la integridad de datos. Evasión de ataques de reinyección, (forma de ataque que es

llevada a cabo por el autor o por el envenenamiento ARP, y este enmascarado)

En esta capa se pueden apreciar protocolos para una comunicación segura como puede ser SSL, TLS o SSH.

19.-Capa5/Sesión

Comunicación entre dispositivos de la red

Facilita los mecanismos de gestión de sesión entre la comunicación de capas superiores.

Servicios:

- Control de diálogo

- Agrupamiento

- Recuperación

Protocolos de esta capa

- RPC procedimiento remoto, permite a un programa de computadora, enrutar código en otra computadora remota, sin preocuparse de la conexión.

- SCP es básicamente lo mismo al rcp, pero cambia, cuando los datos se transfieren son encriptados para que los Sniffer (Podemos decir que un **Sniffer de red** es un software que está diseñado específicamente para redes informáticas, para lograr capturar y analizar los paquetes que se envían y reciben. Pongamos como ejemplo que estamos conectados a un Wi-Fi y visitamos una página web o usamos cualquier plataforma. Constantemente enviamos y recibimos paquetes, que es básicamente la información necesaria.

Un Sniffer de red podría **capturar esos paquetes**. Podría detectar qué estamos visitando, qué información enviamos, etc. De esta forma nuestra privacidad podría verse comprometida. Esto puede ocurrir especialmente cuando nos conectamos a una red desprotegida o un Wi-Fi público donde no sabemos realmente quién puede estar detrás.

Por tanto, podemos indicar que se trata de un **rastreador de redes**. Este tipo de programas puede ser muy útil si queremos analizar nuestra red, ver si tenemos algún problema de seguridad y tener un mayor control. Sin embargo podría volverse en nuestra contra en caso de que un atacante utilice

este tipo de herramientas para comprometer nuestra seguridad y privacidad.) no puedan extraer paquetes de datos.

- ASP protocolo desarrollado por apple, ofrece el establecimiento de la sesión y desmontaje

- H.245 protocolo de telefonía ip

- L2TP

La seguridad es lo que caracteriza a la capa de sesión, ya que dentro de sus capacidades es la de gestionar la autenticación y autorización del envió o recepción de información a través de métodos criptográficos.

En la gestión de comunicaciones simultaneas, en ambos sentidos se llama full dúplex, cuando se alterna los sentidos es half duplex

20.-Capa6/presentación

representación de los datos, sintáctica y semántica

Dado que cuando se establece una comunicación, cada autor responsable, puede tener sin ir más lejos, sistemas operativos distintos, es cuando entra en juego el protagonismo de esta capa, la de presentación la cual efectivamente se encarga de hacer una correcta interpretación de la información enviada.

Servicios:

-La conversación de datos a formatos normalizados, sin importar el SO

-Comprime los datos para que ocupen el menor número de bits.

-Cifra los datos.

Protocolos de esta capa:

NCP control de niveles de redes, con pp

XDR protocolo de representación de datos

AFP ofrece servicio para servicio a Windows

21.-Capa7/Aplicación

servicios de red a aplicaciones

Responsable de gestionar la información de las aplicaciones del cliente.

Protocolos de esta capa:

-Correo: SMTP, POP, IMAP

-Navegación web: HTTP, HTTPS

-Transferencias de archivos: FTP, TFTP, SFTP

-Conexión remota: SSH, RDP, Telnet

DNS, DHCP

Es importante no confundir el nombre de esta capa con aplicaciones que podamos tener instaladas en nuestras PC.

Esta capa se centra netamente en las comunicaciones.

Para esta capa en cuanto a la seguridad, podemos encontrar ids, que es una detección de intrusos, también tenemos, ips, que es sistema de prevención de intrusos, aquí también se tiene que educar a los usuarios de IT.

22.- Cierre de la sección Modelo OSI