Seguridad Multicapa: Del Cable de Cobre al Factor Humano

En el mundo de la ciberseguridad, existe una máxima: **"La seguridad es tan fuerte como el eslabón más débil"**. Para entender dónde están esos eslabones, los profesionales utilizamos el Modelo OSI (Open System Interconnection), pero con una adición crítica: la Capa 8, el usuario.

El Cimiento: Capas Físicas y de Red (Capas 1 a 3)

La seguridad comienza en lo tangible. En la **Capa 1 (Física)**, el riesgo no es un virus, sino el acceso físico: un *keylogger* conectado al teclado o un cable "pinchado" (*tapping*). Subiendo a la **Capa 2 (Enlace)** y **Capa 3 (Red)**, el peligro se vuelve lógico. Aquí, ataques como el *ARP Spoofing* o el *Man-in-the-Middle* permiten a un atacante situarse como un "intermediario invisible", escuchando conversaciones privadas entre equipos que creen estar conectados de forma segura.

El Motor de Comunicación: Transporte y Sesión (Capas 4 y 5)

A medida que los datos fluyen, los atacantes buscan colapsar el camino o robar la identidad del viaje. En la **Capa 4 (Transporte)**, el objetivo suele ser la disponibilidad mediante ataques de denegación de servicio (DoS/DDoS), saturando los puertos con tráfico basura. En la **Capa 5 (Sesión)**, el ataque es más personal: el *Session Hijacking* busca robar la "llave" (cookie o token) que ya ha abierto la puerta, permitiendo al atacante entrar sin conocer la contraseña.

La Interfaz y el Código: Presentación y Aplicación (Capas 6 y 7)

Aquí es donde reside la lógica del software. La **Capa 6 (Presentación)** sufre cuando el cifrado es débil o inexistente, dejando los datos expuestos. Por su parte, la **Capa 7 (Aplicación)** es el escenario de los ataques más famosos, como la *Inyección SQL (SQLi)*, donde un formulario web mal programado se convierte en la puerta trasera hacia la base de datos de toda la empresa.

El Factor Determinante: La Capa 8 (Usuario)

Podemos tener el mejor firewall y el cifrado más robusto, pero si un usuario cae en un engaño de **Ingeniería Social**, la tecnología no podrá detener el ataque. La **Capa 8** representa el factor humano. El *vishing* (llamadas falsas) o el *baiting* (dejar

un USB malicioso en el parking) demuestran que, a menudo, es más fácil engañar a una persona que romper un algoritmo de cifrado.

Conclusión: La seguridad efectiva no es un producto, es un proceso que cubre todas las capas. Una defensa sólida requiere tecnología en las capas bajas y concienciación en la capa más alta.

Ejercicio: "El Mapa de la Intrusión"

Objetivo: Identificar en qué capa del modelo OSI actúa cada amenaza y proponer una medida defensiva.

Escenario de Incidente:

La empresa "TechSecure" ha sufrido un ataque encadenado. Los alumnos deben clasificar cada evento en la capa correspondiente:

1. **Evento A:** Un atacante deja caer varios pendrives en la cafetería con la etiqueta "Salarios 2025". Un empleado conecta uno en su puesto de trabajo.
2. **Evento B:** El malware del pendrive analiza la red local y realiza un *ARP Spoofing* para interceptar el tráfico de los servidores.
3. **Evento C:** Al interceptar el tráfico, el atacante detecta que el servidor de correo utiliza un protocolo de cifrado de hace 15 años, lo que le permite ver las contraseñas.
4. **Evento D:** Con las contraseñas, accede al portal web de administración y aprovecha un fallo de *SQL Injection* para borrar la base de datos de clientes.
5. **Evento E:** Para evitar que IT recupere el sistema, lanza un ataque *SYN Flood* que satura los puertos del router principal.

Tareas para el alumno:

1. **Mapeo de Capas:** Crea una tabla indicando qué **Capa** (1 a 8) corresponde a cada **Evento** (A al E).
2. **Propuesta de Contención:** Para cada evento, propón una medida técnica o organizativa para evitarlo (ej. cortafuegos, formación, cifrado moderno, etc.).
3. **Debate:** Si tuvieras presupuesto limitado, ¿en qué capa invertirías primero y por qué?

VECTORES DE ATAQUE: MODELO OSI + CAPA 8 (HUMANA)

Usuario (Factor Humano) - El eslabón más débil.
Ingeniería Social, Errores, Negligencia, Vishing, Baiting.

CAPA 7 Aplicación | Explotación de vulnerabilidades, SQLi, RCE

CAPA 6 Presentación | Phishing, Cifrado débil

CAPA 5 Sesión | Session hijacking, ataques XSS

CAPA 4 Transporte | Detección, DoS/DDoS, Flooding

CAPA 3 Red | Man-in-the-Middle, Smurf Attack

CAPA 2 Enlace de datos | Spoofing (MAC/ARP)

CAPA 1 Física | Tapping, manipulación de hardware