Triada de la ciberseguridad.

Ataques a la seguridad

Los ataques a la seguridad pueden clasificarse principalmente en dos tipos:

1. Ataques activos: Tiene como objetivo la alteración de los recursos de un sistema, pudiendo afectar su funcionamiento.
2. Ataques pasivos: Un ataque pasivo es aquel en el cual un atacante monitorea deforma no autorizada el trafico de la red, para capturar contraseñas u otra información para su uso posterior.

Principalmente hay dos tipos de ataque activos, la obtención de contenido de mensajes y el análisis de trafico.

Análisis de trafico: Es un ataque que permite observar no solo el contenido de los mensajes enviados por la red, si no también el patrón de dichos mensajes, un atacante podría extraer información de la comunicación que le permitiese determinar el tipo de comunicación que esta teniendo el lugar.

El ataque de repetición se entiende como la captura de uno o mas mensajes de trafico de la red para su posterior retransmisión, con el fin de realizar una acción no deseado. Por ejemplo transacciones repetidas.

Ataque de modificación de mensajes: Un mensaje original es modificado parcialmente con el fin de modificar un objeto no deseado.

Man-in-the-Middle (MITM):

1. Intercepción de red (Sniffing o Eavesdropping)
   1. El atacante se conecta a la misma red (por ejemplo, Wi-Fi público) y usa herramientas como Wireshark o Ettercap para capturar el tráfico.
   2. Ejemplo: En un café con Wi-Fi libre, alguien monitorea el tráfico y roba credenciales no cifradas.
2. Suplantación de ARP (ARP Spoofing / ARP Poisoning)
   1. El atacante envía respuestas ARP falsas para asociar su dirección MAC con la IP del servidor o del router.
   2. Resultado: todo el tráfico pasa por su equipo.
   3. Ejemplo: En una red local de oficina, el atacante redirige el tráfico de los usuarios a través de su máquina para espiar correos o contraseñas.
3. DNS Spoofing
   1. Se modifica la caché DNS para redirigir a los usuarios a sitios falsos aunque escriban la URL correcta.
   2. Ejemplo: El usuario entra “banco.com”, pero el DNS manipulado lo manda a una copia idéntica del sitio que roba sus credenciales.
4. HTTPS Spoofing / SSL Stripping
   1. El atacante fuerza la conexión a pasar de HTTPS a HTTP, quitando el cifrado.
   2. Ejemplo: Durante una compra en línea, el usuario cree estar en conexión segura, pero el atacante intercepta los datos de la tarjeta.
5. Ataques en correos electrónicos (Email Hijacking)
   1. El atacante se infiltra en la comunicación entre cliente y proveedor (por ejemplo, entre comprador y vendedor).
   2. Ejemplo: Intercepta un correo de una empresa e inserta sus propios datos bancarios para desviar un pago.
6. Session Hijacking (Secuestro de sesión)
   1. El atacante roba cookies o tokens de autenticación para tomar el control de una sesión activa.
   2. Ejemplo: Tras un login en redes sociales, alguien roba la cookie de sesión y accede a la cuenta sin necesidad de contraseña.
7. Ataques por Rogue Access Point (Punto de acceso falso)
   1. El atacante crea una red Wi-Fi con nombre similar a una real (“Café\_Free\_WiFi”), engañando a los usuarios.
   2. Ejemplo: Un viajero se conecta en un aeropuerto a un Wi-Fi falso y el atacante captura su tráfico.

### Ejemplos famosos de ataques MITM

* Superfish(Lenovo,2015):  
  Algunos portátiles Lenovo incluían un hadware que instalaba un certificado raíz propio, permitiendo interceptar tráfico HTTPS sin que los usuarios lo supieran.
* DigiNotar(2011):  
  Un ataque comprometió esta autoridad certificadora y se emitieron certificados falsos para dominios de Google, Yahoo y otros. Sirvieron para espiar comunicaciones cifradas en Irán.
* Equifax y ataques en hoteles Marriott:  
  En varios casos se detectaron accesos indebidos donde MITM fue parte del método de infiltración inicial antes del robo de datos masivo.
* Wi-Fi públicos en aeropuertos y cafés (casos reales documentados por Kaspersky y Symantec):  
  Miles de usuarios fueron espiados mediante redes falsas y capturas de tráfico sin cifrar.

Un 0day exploit (o “zero-day”) es una vulnerabilidad de software que todavía no ha sido descubierta o corregida por el fabricante.

El nombre viene de que los desarrolladores tienen cero días para arreglarla: el fallo ya está siendo explotado antes de que exista un parche.

Hay tres piezas clave en esto:

* Vulnerabilidad 0-day: el fallo técnico en el sistema (por ejemplo, un error en el manejo de memoria de Windows o en un navegador).
* Exploit 0-day: el código o técnica que aprovecha esa vulnerabilidad para ejecutar acciones no autorizadas (robar datos, ejecutar código remoto).
* Ataque 0-day: el uso real del exploit contra un blanco.

Suelen ser muy valiosos, sobre todo en espionaje o ciberataques dirigidos, porque no hay defensa conocida aún.