SUPLANTACIÓN DE IDENTIDAD ARP

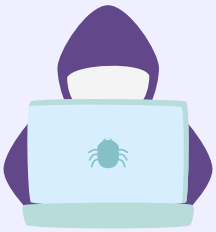
Por:Roberto Rodriguez, Freddy Leon, Ana Churo, Valeria Yunga

El ataque Man-in-the-Middle (MITM) es un tipo de ataque informático donde un atacante intercepta y manipula la comunicación entre dos partes sin que estas se den cuenta.

DEBILIDADES QUE APROVECHA EL ATAQUE

- Falta de autenticación en el protocolo ARP
- Inseguridad en las redes locales
- Comunicaciones sin cifrado

IMPLEMENTACIÓN



1. Configurar la red LAN e identificar las direcciones IP de las máquinas
2. Iniciar Ettercap
3. Analizar los hosts en la red
4. Seleccionar las víctimas
5. Iniciar el envenenamiento ARP
6. Capturar el tráfico con Wireshark
7. Evidenciar el ataque

EFECTOS EN LA RED

- Intercepción de datos sensibles
- Alteración de la comunicación

- Denegación de servicio (DoS)
- Falsificación de información

ESTRATEGIAS DE PREVENCIÓN

- Uso de protocolos seguros (HTTPS, SSH, etc.)
- Verificación de las tablas ARP
- Habilitar características de seguridad en los dispositivos(IDS)
- Implementación de herramientas de detección de intrusos(Dynamic ARP Inspection (DAI))
- Uso de VPNs

CONCLUSIÓN

El ataque Man-in-the-Middle mediante envenenamiento ARP explota la falta de autenticación del protocolo ARP para interceptar y manipular el tráfico en redes locales. No obstante, su impacto puede reducirse con estrategias de prevención bien implementadas.