L'ARP poisoning (o ARP spoofing) è un attacco informatico in cui un aggressore manipola le tabelle di associazione ARP per inviare informazioni di indirizzo IP errate agli altri dispositivi di rete. L'ARP (Address Resolution Protocol) è il protocollo utilizzato per associare gli indirizzi IP ai loro indirizzi MAC corrispondenti. Normalmente, quando un dispositivo desidera comunicare con un altro dispositivo nella rete locale, invia una richiesta ARP per ottenere l'indirizzo MAC corrispondente all'indirizzo IP di destinazione. L'ARP poisoning sfrutta questa comunicazione, inviando risposte ARP fraudolente che associano indirizzi IP validi a indirizzi MAC controllati dall'attaccante. Di conseguenza, il traffico di rete destinato a un dispositivo viene dirottato verso l'attaccante, che può quindi monitorare o manipolare la comunicazione.

Gli attacchi di ARP poisoning possono essere eseguiti in reti locali, quindi i sistemi vulnerabili includono qualsiasi dispositivo che partecipa alla comunicazione di rete nella stessa sottorete. Ciò include computer, server, dispositivi mobili e altri dispositivi di rete come router o switch.

Per mitigare, rilevare o annullare l'attacco di ARP poisoning, ecco alcune modalità:

Implementare la sicurezza a livello di rete, come l'uso di VLAN (Virtual Local Area Network) o segmentazione di rete, per limitare la visibilità e l'accesso degli attaccanti.

Utilizzare protocolli di autenticazione sicura, come 802.1X, per garantire che solo i dispositivi autorizzati possano connettersi alla rete.

Monitorare costantemente la rete per rilevare anomalie o comportamenti sospetti, ad esempio attraverso l'utilizzo di sistemi di rilevamento delle intrusioni (IDS) o di analisi del traffico di rete.

Impiegare tecniche di crittografia per proteggere la comunicazione di rete, come l'utilizzo di protocolli sicuri come HTTPS o VPN.

Le azioni di mitigazione sopra menzionate sono fondamentali per proteggere l'utente e l'azienda dagli attacchi di ARP poisoning. L'implementazione di sicurezza a livello di rete e l'utilizzo di protocolli di autenticazione sicura riducono la possibilità che un attaccante possa manipolare le tabelle ARP e dirottare il traffico. Il monitoraggio costante della rete aiuta a individuare tempestivamente eventuali anomalie o attività sospette, consentendo di prendere provvedimenti immediati. L'utilizzo di tecniche di crittografia protegge la comunicazione di rete da possibili intercettazioni o manipolazioni da parte di un attaccante. Insieme, queste azioni migliorano la sicurezza generale della rete e mitigano il rischio di successo di un attacco di ARP poisoning.