L'ARP (Address Resolution Protocol) poisoning, è un tipo di attacco informatico in cui un attaccante modifica o manipola la tabella ARP di una rete locale per indirizzare il traffico di rete destinato a un dispositivo, a un altro indirizzo MAC, a scopo malevolo. Questo tipo di attacco può avere diverse finalità, tra cui la cattura del traffico di rete, il furto di dati sensibili o la manipolazione delle comunicazioni di rete.

Ecco come funziona l'ARP poisoning:

1. **Tabella ARP**: Ogni dispositivo in una rete locale mantiene una tabella ARP che associa gli indirizzi IP agli indirizzi MAC dei dispositivi presenti nella stessa rete. Questa tabella è utilizzata per instradare i pacchetti di rete al dispositivo di destinazione corretto.
2. **ARP Request e ARP Reply**: Quando un dispositivo deve comunicare con un altro dispositivo nella stessa rete, invia una richiesta ARP (ARP Request) per ottenere l'indirizzo MAC associato all'indirizzo IP del dispositivo di destinazione. Il dispositivo di destinazione risponde con un ARP Reply contenente il suo indirizzo MAC.
3. **Manipolazione ARP**: Un attaccante che esegue ARP poisoning invia falsi messaggi ARP alla rete, annunciando che l'indirizzo IP di un dispositivo di destinazione specifico è associato al proprio indirizzo MAC. Questo fa sì che tutti i pacchetti destinati al dispositivo di destinazione vengano reindirizzati all'attaccante invece che al dispositivo corretto.
4. **Cattura o Manipolazione del Traffico**: Una volta che l'attaccante riceve il traffico destinato al dispositivo di destinazione, può catturarlo per esaminare i dati sensibili o manipolarlo prima di inviarlo al dispositivo corretto.
5. **Persistenza**: In alcuni casi, l'attaccante può continuare a inviare messaggi ARP falsi per mantenere la sua posizione nell'attacco e continuare a intercettare o manipolare il traffico.

Le modalità per mitigare o risolvere l'ARP poisoning:

1. **Utilizzare ARP Inspection**: Molti switch di rete supportano la funzionalità di ARP inspection, che può rilevare e prevenire gli attacchi ARP spoofing monitorando e validando i messaggi ARP nella rete. Questa modalità è piuttosto semplice ed immediata qualora si è già in possesso di uno switch con tale funzione altrimenti richiede l’acquisto dello stesso e una successiva installazione da parte di un tecnico.
2. **Utilizzare VPN**: L'utilizzo di una VPN (Virtual Private Network) può crittografare il traffico di rete tra i dispositivi nella rete locale, rendendo più difficile per un attaccante eseguire ARP poisoning. Questa soluzione è di facile applicazione ma richiede un investimento economico poiché è necessario un abbonamento a un fornitore di VPN.
3. **Utilizzare MAC Statici**: Assegnare manualmente gli indirizzi MAC ai dispositivi nella rete può impedire agli attaccanti di manipolare la tabella ARP. Questa soluzione è di facile applicabilità per l’utente/azienda che può in maniera autonoma o tramite tecnico eseguire questo tipo di modifica.
4. **Monitoraggio del Traffico**: Implementare sistemi di monitoraggio del traffico di rete per rilevare comportamenti anomali, inclusi i tentativi di ARP poisoning. Questa modalità di intervento oltre che richiedere delle capacità più approfondite a livello informatico e quindi un tecnico che controlli periodicamente il traffico di rete richiede l’utilizzo di strumenti di monitoraggio che per essere utilizzati nella loro versione completa necessitano dell’acquisto di una licenza, quindi tale soluzione è applicabile per un’azienda in cui un eventuale attacco di APR poisoning creerebbe un danno economico maggiore.
5. **Autenticazione e Sicurezza**: Utilizzare autenticazione forte per l'accesso alla rete e implementare misure di sicurezza avanzate, come la segmentazione di rete e le politiche di sicurezza rigorose. Questa soluzione non è facilmente applicabile, ciò è dovuto al fatto che richiede un investimento economico per adeguare la rete fisica dell’azienda e per un tecnico che configuri correttamente la rete, che crei delle politiche di sicurezza chiare e ben definite che stabiliscano le regole e le procedure per proteggere la rete e i dati, che implementi un sistema di controllo degli accessi basato su ruoli, che implementi quindi la rete con varie misure di sicurezza avanzate.

6. **Aggiornare il Software**: Assicurarsi che tutti i dispositivi nella rete eseguano software aggiornato e applichino patch di sicurezza per ridurre le opportunità per gli attaccanti. Questo metodo è di facile applicabilità e non richiede particolari conoscenze in materia.
7. Sensibilizzare gli utenti sulla sicurezza informatica e sui pericoli degli attacchi ARP poisoning può aiutare a prevenire comportamenti rischiosi. Questa modalità di prevenzione potrebbe rivelarsi meno onerosa rispetto al danno causato da un eventuale attacco di questo tipo.