L'ARP (Address Resolution Protocol) Poisoning è un attacco che sfrutta la vulnerabilità del protocollo ARP, utilizzato per mappare gli indirizzi IP agli indirizzi MAC all'interno di una rete locale che operano al livello 2 OSI L'obiettivo dell'attacco è manipolare le tabelle ARP in modo che un host vittima invii il suo traffico a un indirizzo MAC controllato dall'attaccante, anziché al corretto destinatario.

Come funziona l'ARP Poisoning:

1. L'attaccante invia pacchetti ARP falsificati alla rete locale, annunciando che l'indirizzo MAC di un determinato indirizzo IP è cambiato e ora corrisponde al suo indirizzo MAC.
2. Gli altri dispositivi di rete ricevono questo annuncio e aggiornano le proprie tabelle ARP in base alle informazioni fornite dall'attaccante.
3. Quando la vittima tenta di comunicare con l'indirizzo IP target, invierà il traffico alla MAC address manipolata dall'attaccante, consentendo a quest'ultimo di intercettare, modificare o bloccare il traffico.

Sistemi vulnerabili all'ARP Poisoning:

Tutti i sistemi operativi che utilizzano il protocollo ARP, tra cui:

1. Windows
2. macOS
3. Linux
4. Android
5. iOS

Inoltre, i sistemi vulnerabili ad ARP Poisoning sono in genere presenti nelle reti locali e includono computer, server e dispositivi di rete.

Mitigazione, rilevamento e annullamento dell'ARP Poisoning:

Mitigazione:

- Disattivare l'inoltro IP: impedisce all'attaccante di reindirizzare il traffico.
- Utilizzare un firewall con filtro MAC: consente solo ai dispositivi con indirizzi MAC specifici di accedere alla rete.
- Configurare ARP statico: associare manualmente gli indirizzi IP agli indirizzi MAC dei dispositivi di fiducia.
- Utilizzare protocolli di sicurezza come SSL/TLS: proteggono il traffico di rete da intercettazioni.

Rilevamento:

- Monitorare il traffico ARP: identificare pacchetti ARP sospetti.
- Utilizzare software di sniffing: analizzare il traffico di rete per identificare l'attacco.
- Controllare i log di sistema: cercare errori o attività insolite.

Annullamento:

- Rimuovere l'attaccante dalla rete: disconnettere il dispositivo dell'attaccante dalla rete.
- Cambiare le password: modificare le password dei dispositivi e dei servizi di rete.
- Aggiornare il firmware dei dispositivi: correggere eventuali vulnerabilità del firmware.

Azioni di mitigazione:

- Disattivare l'inoltro IP:

Efficacia: Alta. Impedisce all'attaccante di reindirizzare il traffico.

Effort: Basso. Richiede la modifica delle impostazioni del router.

- Utilizzare un firewall con filtro MAC:

Efficacia: Media. Può essere aggirato da un attaccante esperto.

Effort: Medio. Richiede la configurazione del firewall.

- Configurare ARP statico:

Efficacia: Alta. Protegge da attacchi ARP Poisoning semplici.

Effort: Alto. Richiede la configurazione manuale di ogni dispositivo.

- Utilizzare protocolli di sicurezza come SSL/TLS:

Efficacia: Molto alta. Protegge il traffico di rete da intercettazioni.

Effort: Medio. Richiede la configurazione dei server e dei client.

- Rilevamento:

Efficacia: Media. Può essere difficile identificare l'attacco se non si è esperti.

Effort: Medio. Richiede l'utilizzo di strumenti specifici e la conoscenza del protocollo ARP.

- Annullamento:

Efficacia: Alta. Elimina l'attacco dalla rete.

Effort: Medio. Richiede l'identificazione del dispositivo dell'attaccante e la modifica delle password.

In generale, si consiglia di combinare diverse di queste misure per ottenere una protezione completa contro l'ARP Poisoning può avere gravi conseguenze per la sicurezza della rete, per questo motivo, è importante adottare le opportune misure di mitigazione e rilevamento per proteggere la propria rete da questo tipo di attacco.