APR Poisoning: Funzionamento, Vulnerabilità e Mitigazione

W15-D3

Come funziona l’ARP poisoning?

L’ARP (Address Resolution Protocol) poisoning, anche noto come spoofing, è una tecnica di attacco utilizzata per intercettare il traffico, sfrutta la vulnerabilità del protocollo ARP che viene utilizzato per associare indirizzi IP a indirizzi MAC in una rete LAN.

L’attacco si suddivide in 3 fasi:

1. Connessione alla rete LAN, dove l’attaccante si connetterà alla rete del dispositivo target;
2. Inondazione di pacchetti ARP falsi, dove l’attaccante invia pacchetti ARP falsi a tutti i dispositivi nella rete, con l'obiettivo di associarsi falsamente agli indirizzi IP di altri dispositivi.
3. Intercettazione del traffico, in cui una volta avvelenata la cache ARP, il traffico destinato agli indirizzi IP avvelenati verrà inviato all'attaccante invece che ai legittimi destinatari. L'attaccante può quindi riesce ad Intercettare e registrare il traffico, modificare i dati in transito a suo piacimento e reindirizzare il traffico verso i legittimi destinatari per evitare di destare sospetti (attacco man-in-the-middle).

Quali sistemi sono vulnerabili all'ARP Poisoning?

Purtroppo i sistemi vulnerabili all'ARP poisoning sono molteplici:

- Qualsiasi dispositivo collegato alla rete LAN non dotato di protezioni ARP (computer, server, mobile, stampanti e dispositivi IoT);
- Dispositivi di rete come switch di rete non configurati correttamente e i router che posso essere target come mittenti e destinatari di pacchetti ARP falsi;
- Infrastrutture di rete ormai obsolete.

Mitigazione ARP Poisoning

Tuttavia possiamo mitigare, diminuire o addirittura eliminare il danno con delle tecniche che si possono implementare:

1. ***Voci ARP Statiche:***
   - Configurare manualmente le voci ARP statiche su dispositivi critici.
2. *Tools per la rilevazione di ARP Spoofing:*
   - Utilizzare strumenti come arpwatch o ARP anti-spoofing software.
3. ***Segmentazione della rete:***
   - Segmentare la rete in modo da limitare la portata dell'attacco, ed evitare di colpire tutti i dispositivi.
4. ***Crittografia*:**
   - Implementare protocolli sicuri, che implementano la crittografia nel passaggio dei dati (e.g., HTTPS, VPN).
5. ***Dynamic ARP Inspection (DAI)*:**
   - Utilizzare switch gestiti con Dynamic ARP Inspection (DAI) che garantisce il passaggio dei dati dal giusto mittente al giusto ricevente, per monitorare e bloccare ARP spoofing.

Efficacia delle azioni di mitigazione

1. ***Voci ARP statiche:***
- **Efficacia**: Alta per dispositivi critici.
- **Effort**: Elevato, richiede manutenzione manuale.

2. ***Tools per la rilevazione di ARP Spoofing:***
- **Efficacia**: Buona, rileva e avvisa in caso di allarme.
- **Effort**: Moderato, necessità di configurazione e monitoraggio continuo.

3. ***Segmentazione della rete:***
- **Efficacia**: Molto alta, limita l'area di impatto.
- **Effort**: Medio, implica la riorganizzazione della rete.

4. ***Crittografia:***
- **Efficacia**: Elevata, protegge i dati intercettati.
- **Effort**: Variabile, dipende dall'implementazione.

5. ***Dynamic ARP Inspection (DAI):***
- **Efficacia**: Molto alta in ambienti controllati.
- **Effort**: Medio-alto, necessita di hardware e configurazione avanzati.

Conclusioni

- ***Riepilogo***: L'APR Poisoning è un attacco pericoloso che non va mai sottovalutato e dato per scontato, nonostante ciò è facilmente mitigabile con le giuste misure come l’implementare una combinazione di tecniche per proteggere la rete.
- ***Raccomandazioni***: Si consiglia di monitorare continuamente la rete e aggiornare le protezioni in base alle nuove minacce.