

Traccia

- Spiegare brevemente come funziona l'ARP Poisoning
- Elencare i sistemi che sono vulnerabili a ARP Poisoning
- Elencare le modalità per mitigare, rilevare o annullare questo attacco
- Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda

APR Poisoning:

1. Come funziona l'ARP Poisoning:

L'ARP Poisoning (Address Resolution Protocol Poisoning) è un attacco informatico che sfrutta la vulnerabilità del protocollo ARP per manipolare la tabella ARP di un dispositivo di rete. Il protocollo ARP è responsabile di mappare gli indirizzi IP agli indirizzi MAC, e l'attacco avviene quando un attaccante invia pacchetti ARP falsificati per associare l'indirizzo IP di una vittima al proprio indirizzo MAC. Ciò può portare a una serie di problemi, come l'inoltro errato del traffico o l'esecuzione di attacchi di tipo "man-in-the-middle".

2. Sistemi vulnerabili a ARP Poisoning:

I sistemi vulnerabili all'ARP Poisoning includono reti locali e reti wireless. Questo attacco è particolarmente efficace in reti non protette o mal configurate, come quelle senza autenticazione e crittografia robusta.

3. Modalità per mitigare, rilevare o annullare l'attacco:

- Mitigazione:
 - Implementare VLAN (Virtual LAN) per isolare segmenti di rete critici.
 - Utilizzare reti wireless protette con WPA 3 e crittografia AES per ridurre l'accesso non autorizzato.
- Rilevamento:
 - Monitorare regolarmente la tabella ARP per rilevare discrepanze.
 - Utilizzare sistemi di rilevamento delle anomalie di rete per identificare comportamenti sospetti.
- Annullamento:
 - Aggiornare le tabelle ARP manualmente nei dispositivi coinvolti.
 - Utilizzare strumenti specifici, come ARPwatch, per rilevare e correggere automaticamente le alterazioni ARP.

4. Commento sulle azioni di mitigazione:

- Efficacia:
 - L'implementazione di VLAN riduce la superficie di attacco, limitando la portata dell'attacco ARP Poisoning.
 - L'uso di reti wireless sicure complica il compito degli attaccanti nel compromettere la sicurezza della rete.
- Effort per l'utente/azienda:
 - Implementare VLAN richiede una pianificazione approfondita e una configurazione accurata, ma può fornire una difesa efficace.
 - La gestione delle reti wireless sicure richiede la configurazione di protocolli di sicurezza avanzati, con la necessità di gestire le chiavi e gli aggiornamenti regolari delle credenziali.

In generale, la mitigazione e la prevenzione dell'ARP Poisoning richiedono un approccio multifattoriale che coinvolge sia configurazioni di rete avanzate che pratiche di sicurezza solide. L'adozione di queste misure può richiedere un certo sforzo iniziale, ma è cruciale per proteggere la rete da attacchi ARP Poisoning.