Nella lezione teorica abbiamo visto l'attacco **ARP Poisoning**

Traccia

- Spiegare brevemente come funziona l'APR Poisoning
- Elencare i sistemi che sono vulnerabili a APR 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.

ARP Poisoning

ARP (Address Resolution Protocol) Poisoning, noto anche come **ARP Spoofing**, è un attacco in cui un malintenzionato invia messaggi ARP falsificati sulla rete locale. L'obiettivo è associare l'indirizzo MAC del malintenzionato a un indirizzo IP legittimo, così da intercettare, modificare o interrompere il traffico di rete destinato a quel IP. Questo attacco permette all'attaccante di effettuare operazioni come il **Man-in-the-Middle** , sniffing dei dati o il dirottamento del traffico.

Sistemi Vulnerabili a ARP Poisoning

Tutti i dispositivi che utilizzano il protocollo ARP per la risoluzione degli indirizzi IP a indirizzi MAC sono potenzialmente vulnerabili a ARP Poisoning, inclusi:

- **Windows**
- **Linux**
- **macOS**
- **Dispositivi di rete (router, switch)**
- **Sistemi IoT (Internet of Things) che utilizzano ARP**
-

Modalità per Mitigare, Rilevare o Annullare ARP Poisoning

1. **Static ARP Entries**: Configurare manualmente le voci ARP statiche nei dispositivi di rete.
2. **Dynamic ARP Inspection (DAI)**: Utilizzare funzionalità di sicurezza nei switch gestiti che convalidano le risposte ARP.
3. **Port Security**: Configurare la sicurezza delle porte sui switch per limitare il numero di indirizzi MAC per porta.

4. **Encryption (IPsec, HTTPS)**: Utilizzare protocolli di cifratura per proteggere il traffico di rete, rendendo inefficaci gli attacchi MITM.
5. **ARP Spoofing Detection Tools**: Implementare strumenti per rilevare anomalie nel traffico ARP, come ARPwatch o Snort.
6. **Network Segmentation**: Segmentare la rete per limitare la superficie di attacco e isolare i dispositivi vulnerabili.

Commento sulle Azioni di Mitigazione

1. **Static ARP Entries**
   - **Efficacia**: Alta, elimina la possibilità di spoofing per gli indirizzi configurati.
   - **Effort**: Alto, richiede configurazioni manuali e gestione continua, non pratico per reti grandi o dinamiche.
2. **Dynamic ARP Inspection (DAI)**
   - **Efficacia**: Alta, previene attivamente gli attacchi ARP spoofing.
   - **Effort**: Moderato, richiede hardware di rete compatibile e configurazione da parte di personale tecnico qualificato.
3. **Port Security**
   - **Efficacia**: Moderata, limita l'impatto dell'attacco riducendo il numero di indirizzi MAC per porta.
   - **Effort**: Moderato, necessita di configurazioni precise e monitoraggio continuo.
4. **Encryption (IPsec, HTTPS)**
   - **Efficacia**: Alta, protegge il contenuto del traffico anche se intercettato.
   - **Effort**: Variabile, può richiedere modifiche significative alle applicazioni e ai servizi di rete.
5. **ARP Spoofing Detection Tools**
   - **Efficacia**: Moderata, permette di rilevare e rispondere rapidamente agli attacchi.
   - **Effort**: Moderato, necessita di implementazione e monitoraggio continuo.
6. **Network Segmentation**
   - **Efficacia**: Alta, limita la propagazione degli attacchi e isola i dispositivi compromessi.
   - **Effort**: Moderato, richiede una pianificazione attenta e una gestione attiva delle reti.

Conclusioni

Le misure di mitigazione per ARP Poisoning variano in termini di efficacia e sforzo richiesto. Configurazioni manuali come voci ARP statiche sono altamente efficaci ma difficili da gestire su larga scala. Soluzioni come DAI e port security offrono un buon equilibrio tra protezione e sforzo, ma richiedono hardware compatibile e competenze tecniche. L'uso di cifratura e strumenti di rilevamento aggiunge un ulteriore livello di sicurezza, ma comporta costi e complessità aggiuntive. Infine, la segmentazione della rete è una strategia potente per limitare gli effetti di un attacco, ma richiede una buona conoscenza della topologia di rete e delle pratiche di gestione.