ESERCITAZIONE W15D1(2)

EPICODE

Esercizio
Traccia

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.

L'ARP Poisoning è un attacco che manipola la tabella ARP di un dispositivo di rete, sostituendo gli indirizzi MAC legittimi con quelli dell'attaccante. Questo porta a indirizzare il traffico destinato a un certo dispositivo verso l'attaccante anziché al legittimo destinatario. Praticamente tutti i dispositivi connessi a una rete locale, come computer, server, dispositivi IoT e router, sono vulnerabili all'ARP Poisoning. Questo attacco può essere eseguito all'interno di reti locali dove non sono implementate misure di autenticazione ARP.

Per mitigare, rilevare o annullare l'ARP Poisoning, è possibile adottare diverse misure:

1. Utilizzare tecniche di autenticazione ARP, come il rilevamento dello spoofing ARP o l'ispezione ARP, per identificare e rispondere agli attacchi ARP falsificati.

2. Segmentare la rete utilizzando VLAN per limitare la diffusione degli attacchi ARP solo all'interno di segmenti di rete specifici.

3. Implementare strumenti di sicurezza di rete come firewall o sistemi di rilevamento delle intrusioni (IDS) per monitorare e segnalare anomalie nel traffico ARP.

Queste azioni possono aiutare a prevenire o rilevare gli attacchi ARP Poisoning, ma potrebbero richiedere un impegno aggiuntivo da parte dell'utente o dell'azienda. Ad esempio, configurare e gestire le tecniche di autenticazione ARP richiede tempo e competenze specifiche, mentre l'utilizzo di strumenti di sicurezza aggiuntivi potrebbe comportare costi aggiuntivi e la necessità di personale dedicato per la configurazione e la manutenzione.