Esercitazione W15D1 - Pratica 2

Arp Poisoning

Fabio Benevento - 14/02/2024

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.

Implementazione

L'ARP spoofing, noto anche come ARP poisoning, è un attacco Man in the Middle (MitM) che consente agli aggressori di intercettare le comunicazioni tra i dispositivi di rete. L'attacco funziona come segue:

- L'attaccante deve avere accesso alla rete. Esegue una scansione della rete per determinare gli indirizzi IP di almeno due dispositivi, ad esempio una workstation e un router.
- L'aggressore utilizza uno strumento di spoofing per inviare risposte ARP contraffatte.
- Le risposte falsificate comunicano che l'indirizzo MAC corretto per entrambi gli indirizzi IP, appartenenti al router e alla workstation, è l'indirizzo MAC dell'attaccante. In questo modo il router e la workstation si collegano al computer dell'aggressore, anziché l'uno all'altro.
- I due dispositivi aggiornano le loro voci della cache ARP e da quel momento in poi comunicano con l'aggressore invece che direttamente tra loro.

La vulnerabilità riguarda tutti i dispositivi connessi su rete locale, in particolare tramite reti wireless in quanto è più semplice per l'attacante avere accesso alla rete.

Modalità per Mitigare o Risolvere la Vulnerabilità

1. **Utilizzo di VPN**

Efficacia: Alta - *Effort*: Medio

Tramite l'utilizzo di una VPN il traffico viene cifrato per cui in caso di attacco di tipo Arp Poisoning, l'attaccante non sarebbe in grado di analizzare il contenuto del traffico tra i dispositivi, mitigando quindi un eventuale attacco

2. **Implementazione di Port Security sullo Switch**

Efficacia: Media - *Effort*: Medio

Imponendo restrizioni sul numero di dispositivi che possono essere collegati a una specifica porta dello switch è possibile liimitare la possibilità di attacchi ARP Poisoning da parte di dispositivi non autorizzati.

3. **Utilizzo di ARP Spoofing Detection Tools**

Efficacia: Alta - *Effort*: Basso

Questa modalità coinvolge l'utilizzo di strumenti specifici progettati per monitorare e rilevare attività ARP sospette. Tali strumenti controllano costantemente la rete, identificando discrepanze tra gli indirizzi IP e MAC registrati nelle tabelle ARP.

4. **Configurazione Statica delle Tabelle ARP**

Efficacia: Alta - *Effort*: Alta

Impostanto manualmente in maniera fissa l'associazione tra Indirizzi MAC e Indirizzi IP nella tabella ARP impedisce agli aggressori di effettuare l'attacco