Esercizio ARP Poisoning Daniele Atzori
M4-W15-D2

Funzionamento dell'ARP Poisoning

L'ARP (Address Resolution Protocol) Poisoning, noto anche come ARP Spoofing, è un attacco in cui un malintenzionato invia falsi messaggi ARP sulla rete locale. L'obiettivo è associare l'indirizzo MAC dell'attaccante all'indirizzo IP di un altro dispositivo sulla rete, come il gateway predefinito. Quando questo avviene, il traffico destinato a quell'indirizzo IP viene inviato all'attaccante, permettendogli di intercettare, modificare o interrompere le comunicazioni.

Sistemi Vulnerabili a ARP Poisoning

I sistemi vulnerabili all'ARP Poisoning sono principalmente:
- Reti locali Ethernet: L'ARP è un protocollo di rete di basso livello utilizzato all'interno delle LAN.
- Dispositivi connessi alla stessa subnet: Qualsiasi dispositivo che utilizza ARP per risolvere gli indirizzi IP in indirizzi MAC è potenzialmente vulnerabile.
- Switch e router: Anche se generalmente più difficili da compromettere rispetto agli host finali, possono essere vulnerabili se non adeguatamente configurati.

Modalità per Mitigare, Rilevare o Annullare questo Attacco

Per mitigare, rilevare o annullare gli attacchi ARP Poisoning, si possono adottare le seguenti misure:

1. Static ARP Entries: Configurare le voci ARP statiche su router, switch e host critici, specificando manualmente gli indirizzi MAC per determinati indirizzi IP.

2. ARP Spoofing Detection Software: Utilizzare strumenti che monitorano la rete alla ricerca di attività sospette, come cambiamenti non autorizzati nelle voci ARP. Alcuni esempi includono ARPwatch, XArp e altri sistemi di intrusion detection.

3. Port Security: Configurare la sicurezza delle porte sugli switch per limitare il numero di indirizzi MAC che possono essere associati a una singola porta, prevenendo attacchi di spoofing.

4. Dynamic ARP Inspection (DAI): Implementare DAI sugli switch per monitorare e filtrare i pacchetti ARP in base a una tabella di binding IP-MAC affidabile, spesso basata su DHCP snooping.

5. Network Segmentation: Segmentare la rete in VLAN separate per limitare la portata di un potenziale attacco ARP Poisoning.

Commento sulle Azioni di Mitigazione

Static ARP Entries: Questa soluzione è molto efficace, ma non è scalabile per reti di grandi dimensioni poiché richiede configurazioni manuali e aggiornamenti costanti.

ARP Spoofing Detection Software: Strumenti di rilevamento sono utili per identificare e rispondere rapidamente agli attacchi, ma possono generare falsi positivi e richiedono risorse per il monitoraggio continuo.

Port Security: Questa misura è efficace per prevenire attacchi su porte specifiche, ma può essere complessa da configurare correttamente e mantenere, soprattutto in ambienti con molti dispositivi mobili o dinamici.

Dynamic ARP Inspection (DAI): DAI è altamente efficace ma richiede switch di livello aziendale che supportino questa funzionalità e una corretta configurazione della rete, inclusa la gestione di una tabella di binding IP-MAC.

Network Segmentation: Segmentare la rete in VLAN è una strategia efficace per limitare l'impatto di un attacco ARP Poisoning. Tuttavia, richiede un'adeguata pianificazione e gestione della rete, e può aumentare la complessità della configurazione.

In sintesi, mentre alcune soluzioni come l'utilizzo di ARP statici sono semplici ma poco scalabili, altre come DAI e la segmentazione della rete offrono protezione più robusta ma richiedono maggiori risorse e competenze per l'implementazione e la gestione. Le aziende devono bilanciare l'efficacia delle misure di mitigazione con il loro impatto operativo per scegliere le soluzioni più adatte alle loro esigenze di sicurezza.