W15D3

ARP POISONING

La 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.

Come funziona l'arp poisoning

ARP poisoning, o ARP spoofing, è una tecnica utilizzata per intercettare o manipolare il traffico di rete all'interno di una LAN (Local Area Network). L'ARP (Address Resolution Protocol) è un protocollo utilizzato per mappare gli indirizzi IP sui MAC address all'interno di una rete locale.
Nell'ARP poisoning:

L'attaccante invia pacchetti ARP falsificati (spoofati) alla rete locale, facendo credere agli altri dispositivi di essere il legittimo proprietario di un particolare indirizzo IP.
Gli altri dispositivi nella rete aggiornano le proprie tabelle ARP con l'indirizzo MAC fornito dall'attaccante, pensando che sia il destinatario corretto per un determinato indirizzo IP.
Tutto il traffico destinato a quell'indirizzo IP viene quindi inoltrato all'attaccante, che può intercettare o manipolare il traffico come desiderato.
Questo tipo di attacco è spesso utilizzato per intercettare comunicazioni sensibili come username, password o altri dati sensibili, o per eseguire altri tipi di attacchi di rete. È un attacco locale e richiede che l'attaccante sia sulla stessa rete locale delle vittime.

Come funziona l'arp poisoning

Tutti i sistemi che utilizzano ARP sono potenzialmente vulnerabili all'ARP poisoning. Tuttavia, alcuni sistemi operativi sono noti per essere più suscettibili a questo tipo di attacco rispetto ad altri. Questo è dovuto principalmente alla loro implementazione del protocollo ARP e alla mancanza di protezioni o contromisure per mitigare gli attacchi ARP spoofing.
Ecco alcuni sistemi operativi che possono essere più vulnerabili all'ARP poisoning:
1.Sistemi operativi Windows: Le versioni più vecchie di Windows, come Windows XP, Windows 7 e Windows Server 2003, sono state notoriamente vulnerabili all'ARP poisoning a causa della loro gestione meno sicura delle tabelle ARP e della mancanza di meccanismi di difesa integrati.
2.Sistemi operativi Linux: Anche alcuni sistemi Linux possono essere vulnerabili all'ARP poisoning, soprattutto se non sono configurati correttamente per mitigare gli attacchi ARP spoofing. Tuttavia, molte distribuzioni Linux moderne includono strumenti e contromisure per proteggere contro tali attacchi.
3.Sistemi operativi macOS: Anche i sistemi macOS possono essere vulnerabili all'ARP poisoning, specialmente se non sono configurati correttamente per proteggersi da tali attacchi.

Azioni di mitigazione

Una delle azioni potrebbe essere quella di impiegare un IPS o un IDS per rilevare l'inoltro «anomalo» come quelle delle ARP reply verso le macchine target.

Un'altra soluzione potrebbe essere quella di separare i dispositivi ponendoli in sottoreti diversi, soprattutto quelli più sensibili.