ARP POISONING

Cos'è il protocollo ARP

ARP (Address Resolution Protocol) è utilizzato per mappare un indirizzo IP a un indirizzo MAC in una rete locale. Un host deve conoscere il MAC address del next hop quando invia un pacchetto IP. Il next hop potrebbe essere qualsiasi device, anche un router, uno switch oppure l'host di destinazione.

Per identificare il MAC address, gli host su una rete utilizzano il protocollo ARP – Address Resolution Protocol. utilizzando il **MAC Address di broadcast** (FF:FF:FF:FF:FF:FF) , richiedendo associazione IP / MAC:

ARP: chi ha l'indirizzo IP 192.168.1.11? A quale MAC è associato?
L'IP richiesto risponderà con il suo MAC address.

L'host salva quindi la coppia IP – MAC nella propria **ARP cache**, una tabella con le coppia IP – MAC salvata localmente per futuri utilizzi.

Come funziona l'ARP Poisoning

L'ARP poisoning, anche conosciuto come ARP Spoofing, è un attacco che si può utilizzare per intercettare del traffico su una rete basata su switch manipolando le tabelle ARP delle due entità coinvolte in una comunicazione bidirezionale. Questo tipo di attacchi è anche chiamato MITM – Man in the middle.

E' una tecnica di attacco nella quale un attaccante invia pacchetti ARP falsificati nella rete locale per associare il proprio indirizzo MAC all'indirizzo IP di un altro host, solitamente lo switch o il gateway.

Senza aspettare che un host invii una richiesta, l'atttaccante invia agli altri host della rete delle risposte ARP non richieste (Gratuitous ARP) per associare il proprio indirizzo MAC as esempio all'indirizzo MAC dello switch.

Attaccante:

ARP: Lo switch è su questo MAC address: aa:bb:cc:dd:ee:ff

In questo modo l'attacante modifica volutamente le tabelle ARP degli host sulla rete.Fino a che l'indirizzo MAC dell'attaccante resta all'interno della tabella ARP cache degli hosts, l'attaccante può continuare ad intercettare liberamente il traffico.

Sistemi vulnerabili a ARP Poisoning:

Praticamente ogni dispositivo connesso a una rete locale (LAN) che utilizza il protocollo ARP può essere vulnerabile a questo tipo di attacco. Ciò include:

- PC e laptop
- Server
- Switch e router (sebbene alcuni switch moderni abbiano misure per prevenire l'ARP spoofing)
- Smartphone e tablet
- Dispositivi IoT (Internet delle Cose)

Modalità per mitigare, rilevare o annullare questo attacco:

Utilizzo di reti private virtuali (VPN): Le VPN cifrano il traffico tra un dispositivo e la rete, rendendo difficile per un attaccante leggere o modificare i dati intercettati.

- *Efficacia:* Alta, in quanto cifra il traffico.
- *Effort:* Medio-alto. La configurazione di una VPN può richiedere competenze tecniche e potrebbe comportare costi aggiuntivi.

Utilizzo di switch che supportano la sicurezza ARP: Alcuni switch moderni hanno funzioni che possono rilevare e bloccare il traffico ARP sospetto.

- *Efficacia: Media-alta, possono prevenire attivamente l'ARP spoofing.*
- *Effort: Medio. La configurazione può richiedere competenze tecniche.*

Implementazione di software di rilevamento ARP spoofing: Ci sono strumenti e software disponibili che possono rilevare tentativi di ARP spoofing nella rete e allertare gli amministratori.

- *Efficacia: Media, in quanto possono rilevare l'attacco ma non necessariamente prevenirlo.*
- *Effort: Medio. La configurazione e la monitorazione possono richiedere attenzione e competenze tecniche.*

Impostazioni statiche ARP: Gli indirizzi MAC possono essere mappati staticamente agli indirizzi IP corrispondenti, ma questa soluzione può essere difficile da gestire in reti di grandi dimensioni.

- *Efficacia: Alta, ma solo fattibile per reti piccole.*
- *Effort: Alto. La gestione degli indirizzi statici può essere laboriosa.*

Isolamento di segmenti di rete: Dividere una rete in segmenti separati può ridurre l'area di attacco per l'ARP spoofing.

- *Efficacia: Media. Riduce l'area di attacco ma non previene l'attacco in sé.*
- *Effort: Medio-alto, in quanto può richiedere una riprogettazione della rete.*