ARP POISONING

L’arp poisoning è una tecnica di attacco per intercettare il traffico su una rete LAN. Ipotizzando che un computer voglia inviare pacchetti ad un altro, è necessario conoscerne il MAC, e quindi invierà una richiesta ARP su tutti i nodi collegati allo switch, richiedendo un’associazione tra IP e MAC. Il secondo computer risponderò con il MAC e quindi avverrà l’associazione che verrà memorizzata in un ARP cache. L’attacco avviene su questa ARP cache che prende il posto dello switch, intercettando o modificando il traffico dei pacchetti nella comunicazione tra i due computer.

Tra i sistemi vulnerabili abbiamo lo switch, computer che utilizzano lo stesso gateway o lo stesso IP di rete.

Per risolvere possiamo:

- Crittografare la comunicazione: utilizzare protocolli come HTTPS oppure delle VPN;
- Segmentazione della rete: per ridurre il numero di potenziali vittime dell’attacco tramite utilizzo di WLAN;
- Monitoraggio traffico di rete: controllo del traffico per vedere se sono state fatte delle intrusioni oppure controllare traffico anomalo;
- Educare il personale: informare gli utenti sui rischi di questo attacco;