ARP Poisoning

L'ARP (Address Resolution Protocol) Poisoning, noto anche come ARP Spoofing, è un tipo di attacco informatico in cui un aggressore manipola le tabelle ARP di una rete locale per inviare pacchetti di rete a indirizzi MAC (Media Access Control) non validi o non autorizzati. L'obiettivo principale di questo attacco è intercettare o manipolare il traffico di rete destinato a un particolare indirizzo IP.

Durante un attacco di ARP Poisoning, l'attaccante invia pacchetti ARP falsificati nella rete locale, affermando di essere il proprietario legittimo di un indirizzo IP specifico. Questo inganna gli altri dispositivi nella rete facendo loro credere che l'indirizzo MAC corrispondente a quell'indirizzo IP appartenga all'attaccante. Di conseguenza, il traffico destinato a quell'indirizzo IP viene inviato all'attaccante invece del destinatario legittimo.

Alcuni sistemi vulnerabili agli attacchi di ARP Poisoning includono:

1. Reti locali cablate: Le reti locali cablate sono particolarmente vulnerabili agli attacchi di ARP Poisoning a causa della loro natura broadcast. Quando un dispositivo invia un pacchetto ARP, viene trasmesso a tutti gli altri dispositivi nella stessa rete locale.
2. Reti wireless: Anche le reti wireless possono essere vulnerabili agli attacchi di ARP Poisoning. Tuttavia, gli attacchi di ARP Poisoning nelle reti wireless possono

richiedere ulteriori tecniche, come il rogue access point, per intercettare il traffico.

Per mitigare, annullare e rilevare gli attacchi di ARP Poisoning, è possibile adottare diverse misure:

3. Utilizzo di ARP Inspection: La funzione ARP Inspection viene spesso fornita da switch di rete o router e consente di monitorare e verificare i pacchetti ARP che attraversano la rete. In questo modo, si possono individuare pacchetti ARP falsificati e impedire che le tabelle ARP vengano alterate.
4. Configurazione di static ARP: Configurare manualmente le tabelle ARP dei dispositivi con indirizzi IP e indirizzi MAC legittimi può ridurre la vulnerabilità agli attacchi di ARP Poisoning. Questo può essere particolarmente utile in ambienti in cui la rete è relativamente statica e non ci sono frequenti cambiamenti nella configurazione dei dispositivi.
5. Utilizzo di VLAN: Le VLAN (Virtual Local Area Network) consentono di suddividere una rete locale in segmenti logici separati. Isolare i dispositivi in VLAN diverse può limitare la portata di un attacco di ARP Poisoning, impedendo all'attaccante di influenzare l'intera rete.
6. Utilizzo di crittografia e autenticazione: L'utilizzo di protocolli di crittografia e autenticazione, come WPA2 per reti wireless, può rendere più difficile agli attaccanti intercettare il traffico e manipolare i pacchetti ARP.
7. Monitoraggio e rilevamento degli attacchi: È possibile utilizzare strumenti di monitoraggio della rete e intrusion detection systems (IDS) per individuare attività