Arp poisoning

L'ARP poisoning, o ARP spoofing, è una tecnica di attacco informatico in cui un attaccante invia pacchetti ARP (Address Resolution Protocol) falsificati in una rete locale al fine di dirottare il traffico di rete. L'ARP viene utilizzato per associare gli indirizzi IP ai corrispondenti indirizzi MAC sulla rete locale.

Un attacco di ARP poisoning avviene quando un attaccante invia pacchetti ARP falsi che asseriscono che l'indirizzo MAC del proprio dispositivo corrisponde all'indirizzo IP di un'altra macchina sulla rete. In questo modo, l'attaccante può intercettare, modificare o iniettare il traffico di rete destinato a quella macchina.

I sistemi che sono vulnerabili all'ARP poisoning sono quelli che utilizzano il protocollo ARP per la risoluzione degli indirizzi IP. Ciò include la maggior parte delle reti locali che utilizzano Ethernet o Wi-Fi. Sia i dispositivi connessi via cavo che quelli connessi in modalità wireless sono potenzialmente vulnerabili.

Per mitigare gli attacchi di ARP poisoning, è possibile adottare diverse azioni di sicurezza:

1. Utilizzare protocolli di sicurezza come Secure ARP (SARP) o Dynamic ARP Inspection (DAI) disponibili su alcuni dispositivi di rete. Questi protocolli possono rilevare e prevenire gli attacchi di ARP poisoning.
2. Configurare manualmente le tabelle ARP sui dispositivi di rete, in modo da associare gli indirizzi MAC agli indirizzi IP corretti. Questo può fornire una protezione aggiuntiva contro gli attacchi di ARP poisoning.
3. Utilizzare reti virtuali private (VPN) o reti virtuali locali (VLAN) per separare il traffico di rete e ridurre la portata degli attacchi di ARP poisoning.
4. Monitorare il traffico di rete in modo da individuare eventuali anomalie o attività sospette, come la presenza di molteplici indirizzi MAC associati a un singolo indirizzo IP.
5. Aggiornare regolarmente il firmware o il software dei dispositivi di rete per beneficiare delle patch di sicurezza più recenti e delle correzioni per le vulnerabilità note.
6. Utilizzare metodi di autenticazione aggiuntivi, come l'uso di certificati digitali o autenticazione a due fattori, per proteggere l'accesso ai dispositivi di rete critici.
7. Educare gli utenti sulla sicurezza informatica e sensibilizzarli sugli attacchi di ARP poisoning, ad esempio avvisandoli di non aprire allegati o fare clic su link sospetti nelle email o messaggi di testo.

Implementando queste azioni, si può ridurre significativamente il rischio di essere vittime di un attacco di ARP poisoning e proteggere la rete locale da questa forma di attacco informatico.