ARP POISONING

L'**ARP Poisoning** è una vulnerabilità che riguarda principalmente le reti locali (LAN) che utilizzano il protocollo ARP (Address Resolution Protocol) per la risoluzione degli indirizzi IP in indirizzi MAC. Poiché l'ARP è un protocollo fondamentale per il funzionamento delle reti Ethernet, quasi tutti i sistemi operativi e dispositivi che si connettono a una LAN tradizionale sono potenzialmente vulnerabili a questo tipo di attacco.

I sistemi operativi potenzialmente vulnerabili sono:
- **Windows (tutte le versioni):** Windows XP, Vista, 7, 8, 10, 11 e Windows Server.
- **macOS:** Tutte le versioni.
- **Linux:** Tutte le distribuzioni (Ubuntu, Debian, Fedora, CentOS, ecc.).
- **Unix/BSD:** Sistemi come FreeBSD, OpenBSD e varianti Unix.

I dispositivi di rete potenzialmente vulnerabili sono:
- **Router e Switch non Gestiti:** I router domestici e molti switch non gestiti, in quanto non includono funzionalità avanzate di protezione ARP come il Dynamic ARP Inspection (DAI).
- **Access Point Wi-Fi:** Access point wireless standard che operano in una LAN e utilizzano ARP per il traffico IP.
- **Stampanti di Rete e altri Dispositivi Embedded:** Dispositivi come stampanti, NAS (Network Attached Storage), videocamere di sorveglianza.
- **Dispositivi IoT:** Molti dispositivi Internet of Things (IoT) utilizzano ARP per la comunicazione in LAN e possono essere vulnerabili.

Per prevenire l'ARP Poisoning, si possono usare tecniche come l'uso di ARP statici, il filtro dei pacchetti ARP con software IDS/IPS, o l'implementazione di protocolli di sicurezza come **Dynamic ARP Inspection (DAI)** su switch di rete.

- **Dynamic ARP Inspection (DAI):** Implementato su switch di rete gestiti per prevenire ARP Spoofing.
- **Static ARP Entries:** Configurare manualmente le associazioni IP-MAC per dispositivi critici.
- **Utilizzo di VPN:** Le VPN cifrano il traffico, rendendo inefficace l'intercettazione del traffico.
- **Monitoraggio della Rete con IDS/IPS**
  - **Intrusion Detection Systems (IDS)** o **Intrusion Prevention Systems (IPS)** possono rilevare pacchetti ARP anomali, segnalando indirizzi MAC duplicati o pacchetti ARP inaspettati.

In sintesi, qualsiasi dispositivo o sistema che utilizza ARP su una LAN tradizionale può essere vulnerabile all'ARP Poisoning, a meno che non siano implementate specifiche misure di sicurezza.