W15D1

ARP Poisoning

[L’ **Address Resolution Protocol**(ARP) è un **protocollo di risoluzione degli indirizzi.** Lo scopo dell’ARP è quello di creare una **mappatura tra gli indirizzi MAC** e degli indirizzi IP,consentendo ai dispositivi di “chiedere” a quale dispositivo è attualmente assegnato un determinato indirizzo IP.]

L’**ARP Spoofing** è utilizzato per entrare in rete in modo che l'utente malintenzionato possa esaminare ogni pacchetto di dati che viaggia nella rete locale e quindi manipolarlo fino a quando il traffico non cambia o cessa.

Pertanto, questo è un attacco in cui vengono consegnati pacchetti ARP falsi a una LAN.

Sistemi vulnerabili a ARP Poisoning:

ARP Poisoning può colpire qualsiasi sistema o dispositivo che utilizza ARP per risolvere gli indirizzi IP in indirizzi MAC, inclusi:

- **Reti Ethernet:** Tutti i dispositivi su una rete Ethernet sono potenzialmente vulnerabili, compresi computer, switch, router, stampanti, e dispositivi IoT.
- **Dispositivi senza meccanismi di sicurezza avanzati:** Sistemi operativi e dispositivi che non implementano contromisure specifiche contro l'ARP Poisoning sono particolarmente a rischio.

Modalità per mitigare, rilevare o annullare l’attacco:

Ci sono diverse misure che dobbiamo prendere per evitare di diventare vittime dell’ARP Spoofing.
Di seguito alcune raccomandazioni:

- **Strumenti di monitoraggio:**
  l’utilizzo di tecnologie di monitoraggio per individuare potenziali vulnerabilità del sistema. Esistono alternative gratuite e open source come arpwatch che ti forniscono il controllo sulle attività della rete.
- **Dividere la rete in più segmenti:**
  la rete può anche essere suddivisa in sezioni. Ciò garantisce che se un estraneo tenta

un attacco, questo ha un impatto solo su una parte della rete e non sull’intera rete. Ciò, tuttavia, richiede un’implementazione di rete più sofisticata.

- **Protocollo per Secure Neighbor Discovery:**
  consiste nell’utilizzare Safe Neighbor Discovery (SEND), che è compatibile solo con i sistemi operativi più recenti.È un'estensione del protocollo **Neighbor Discovery Protocol (NDP)** utilizzato in IPv6 per migliorare la sicurezza delle operazioni di scoperta dei vicini su una rete locale.

[Il **Neighbor Discovery Protocol (NDP)** è utilizzato dai dispositivi IPv6 per scoprire altri dispositivi nella stessa rete, ottenere indirizzi IP, determinare l'indirizzo del gateway predefinito e trovare i router sulla rete locale.]