ESERCIZIO W15D1 (1)

L’arp poisoning è una vulnerabilità che può essere sfruttata solamente su rete locale.
Un utente invia pacchetti ARP modificati all’interno della rete , questi pacchetti contengono informazioni specifiche sulle associazioni ip-mac facendo così credere agli altri dispositivi sulla rete che un indirizzo ip corrisponda ad un diverso indirizzo mac.
Questo fa si che che un utente con il suo dispositivo manda pacchetti ad un’altro, questi pacchetti arriveranno probabilmente a destinazione ma nel mentre vengono intercettati dall’attaccante che può analizzarli, bloccarli o manipolarli a suo piacimento.
I dispositivi vulnerabili possono essere server, pc o dispositivi IoT presenti sulla rete locale.
Per prevenire questo tipo di attacco si puo utilizzare un firewall che sia in grado di rilevare questo tipo di attacco.
Aggiornare prontamente i dispositivi di rete come i router o switch.
Monitorare il traffico di rete per rilevare anomalie del traffico e studiare i pacchetti in transito.
Dividere la rete con un VLAN per far si che l’attaccante abbia accesso ad un numero minore di dispositivi sulla rete.