ESERCIZIO 15D1

Vista la teoria degli ultimi giorni, andiamo ora far luce su alcune caratteristiche dell'arp poisoning.

Traccia:

• Spiegare brevemente come funziona l'APR Poisoning

• Elencare i sistemi che sono vulnerabili a APR Poisoning

• Elencare le modalità per mitigare, rilevare o annullare questo attacco

• Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda.

Spiegazione ARP poisoning

Questa tipologia di attacco intercetta e manipola il traffico di pacchetti tra un client e un server presenti in una rete locale. L'ARP poisoning sfrutta il protocollo ARP per inviare informazioni false, spacciandosi per lo switch che indirizza il i datagrammi all'interno della rete dei bersagli. L'attaccante riceve i pacchetti destinati per l'una e l'altra parte.

Sistemi vulnerabili all'ARP poisoning

Questo attacco colpisce solamente i sistemi all'interno di una rete LAN, ovvero tutte le macchine che utilizzano lo stesso IP e lo stesso gateway.

Modi per prevenire e mitigare l’attacco

Qui sotto elencheremo le tecniche migliori per proteggerci da un ARP poisoning.

- Utilizzare i protocolli di sicurezza, parliamo di HTTPS, SSL, TLS o VPN, che crittografano i dati inviati durante la comunicazione.
- Utilizzare uno switch di livello 3, in modo da diviere la rete in più sottoreti. Tuttavia, gli swith di livello 3 sono piuttosto costosi e richiedono una configurazione a monte.
- Monitorare la rete, o più semplicemente restare vigili in caso di eventuali intrusioni, ad esempio accessi non autorizzati o attacchi ARP poisoning.
- Utilizzare software antivirus e anti-malware per prevenire attacchi ARP poisoning
- Educare il personale alla sicurezza informatica. Se informiamo i dipendenti sulla pericolosità dell’ ARP poisoning sicuramente quest’ultimi faranno più attenzione ai traffici poco sicuri.