Esercitazione 8 Modulo 4 – Alessio Russo

Nella lezione teorica abbiamo visto l'attacco 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.

L'attacco ARP Poisoning è una tecnica malevola utilizzata per intercettare, analizzare o manipolare il traffico di rete all'interno di una LAN (rete locale). Questo attacco sfrutta il protocollo ARP (Address Resolution Protocol) per inviare informazioni ARP false sulla rete, promuovendo il proprio indirizzo MAC come il legittimo indirizzo MAC del router o di un altra macchina. Ciò consente all'attaccante di intercettare il traffico di rete tra le macchine e il router o di dirottare questo traffico ogni volta che una macchina invia un pacchetto al gateway o al router. L'attacco ARP Poisoning colpisce esclusivamente i sistemi all'interno di una LAN, in particolare tutte le macchine che utilizzano lo stesso gateway e lo stesso indirizzo IP di rete. In altre parole, gli utenti all'interno della stessa rete locale saranno vulnerabili all'attacco ARP Poisoning.

Esistono diverse tecniche per mitigare questo tipo di attacco:

- Utilizzo di protocolli di sicurezza: i protocolli come HTTPS, SSL, TLS o VPN crittografano i dati in transito e impediscono agli attaccanti di leggerli o manipolarli.
- Utilizzare Switch livello 3: in questo modo si divide la rete in sottoreti, ma gli switch layer 3 hanno un costo maggiore e richiedono configurazione.
- Monitoraggio costante: controllare regolarmente la rete per individuare eventuali intrusioni, come accessi non autorizzati o attacchi di ARP poisoning.
- Utilizzo di software per la sicurezza: alcuni software antivirus e anti-malware possono individuare e prevenire attacchi ARP poisoning.
- Educazione del personale aziendale: informare gli utenti sulla sicurezza informatica e sui rischi di attacchi come l'ARP poisoning può aiutare a prevenire incidenti. Informare gli utenti che non tutto il traffico può essere lecito.

Monitoraggio di rete: Diversi produttori di software offrono anche dei programmi di monitoring con i quali si possono controllare le reti e rilevare i procedimenti ARP insoliti. Ad esempio: Arpwatch, XArp. Altrimenti possiamo usare l'IDS Snort per effettuare il monitoraggio