ESERCIZIO M4 D5 - 2

ARP POISONING

MARCO TANI

ARP POISONING: Cos’è?

ARP Poisoning: ARP Poisoning (o ARP spoofing) è un attacco in cui un aggressore invia pacchetti ARP falsificati (Address Resolution Protocol) nella rete al fine di associare indirizzi IP legittimi a indirizzi MAC falsi. Questo crea un ambiente in cui l'attaccante può intercettare, modificare o iniettare il traffico di rete tra due host legittimi.

SISTEMI VULNERABILI AD ARP POISONING:

In generale, qualsiasi dispositivo connesso a una rete locale (LAN) che utilizza il protocollo ARP per risolvere gli indirizzi IP può essere vulnerabile all'ARP Poisoning. Ciò include computer, server, router, switch e altri dispositivi di rete che utilizzano ARP per comunicare sulla rete.

Modalità per mitigare, rilevare o annullare l'attacco:

- Uso di ARP Inspection: I dispositivi di rete avanzati supportano spesso la funzionalità di "ARP inspection" che monitora e verifica la coerenza delle informazioni ARP sulla rete, individuando e bloccando gli attacchi di ARP Poisoning.
- Uso di VLAN: La segmentazione della rete in VLAN (Virtual Local Area Network) può limitare l'impatto dell'ARP Poisoning. Le VLAN separate rendono più difficile agli attaccanti influenzare il traffico tra le reti.
- Uso di IPsec o VPN: L'utilizzo di protocolli di sicurezza come IPsec o l'uso di una VPN (Virtual Private Network) può crittografare il traffico di rete, rendendo più difficile agli attaccanti intercettare e manipolare i pacchetti.
- Monitoraggio del traffico di rete: Utilizzare strumenti di monitoraggio del traffico di rete per rilevare anomalie o modelli di traffico sospetti che potrebbero indicare un attacco di ARP Poisoning in corso.

Commento sulle azioni di mitigazione:

- Efficacia: L'uso di ARP Inspection, VLAN, IPsec o VPN e il monitoraggio del traffico di rete sono misure efficaci per mitigare e rilevare l'ARP Poisoning. Queste azioni aiutano a proteggere il traffico di rete e a prevenire gli attacchi di ARP spoofing.

- Impegno per l'utente/azienda: Implementare queste azioni di mitigazione richiede un impegno significativo in termini di configurazione di dispositivi di rete avanzati, segmentazione della rete, implementazione di protocolli di sicurezza e utilizzo di strumenti di monitoraggio. Tuttavia, considerando i rischi associati all'ARP Poisoning, l'impegno necessario per attuare queste misure è fondamentale per proteggere la rete e i dati aziendali sensibili.