

## Traccia:

1. Spiegare brevemente come funziona l'ARP Poisoning
2. Elencare i sistemi che sono vulnerabili a ARP Poisoning
3. Elencare le modalità per mitigare, rilevare o annullare questo attacco
4. Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda.

### 1. Come funziona l'ARP Poisoning:

- L'ARP Poisoning, o ARP Poisoning, è un tipo di attacco informatico che coinvolge la manipolazione della tabella ARP (Address Resolution Protocol) all'interno di una rete locale. Il protocollo ARP è utilizzato per mappare gli indirizzi IP agli indirizzi MAC dei dispositivi nella rete. In un attacco di ARP Poisoning, un aggressore invia pacchetti ARP falsificati alla rete, fornendo informazioni di mappatura IP-MAC inaccurata. Questo può causare il reindirizzamento del traffico di rete destinato a un determinato dispositivo verso il dispositivo controllato dall'attaccante, consentendo così all'attaccante di intercettare, modificare o bloccare il traffico.

### 2. Sistemi vulnerabili all'ARP Poisoning:

- Tutti i dispositivi collegati a una rete locale possono essere potenzialmente vulnerabili all'ARP Poisoning, inclusi computer, server, router, switch e dispositivi IoT.

### 3. Modalità per mitigare, rilevare o annullare questo attacco:

- Utilizzo di protocolli di sicurezza: Implementare protocolli di sicurezza come ARP Spoofing Detection o ARP Inspection sui dispositivi di rete per rilevare e prevenire gli attacchi ARP Poisoning.

- Configurazione sicura dei dispositivi di rete: Configurare correttamente i dispositivi di rete per evitare l'inoltro di pacchetti ARP sospetti o falsificati.

- Uso di strumenti di monitoraggio della rete: Utilizzare strumenti di monitoraggio della rete per rilevare anomalie nel traffico ARP e identificare potenziali attacchi ARP Poisoning.

- Implementazione di VPN: L'utilizzo di una VPN (Virtual Private Network) può contribuire a proteggere il traffico di rete da essere intercettato o manipolato da un attaccante sulla rete locale.

### 4. Commento sulle azioni di mitigazione:

- L'implementazione di protocolli di sicurezza e la configurazione sicura dei dispositivi di rete sono efficaci nel prevenire gli attacchi ARP Poisoning, ma richiedono una buona comprensione delle impostazioni di sicurezza di rete e potrebbero comportare un certo sforzo iniziale per essere configurati correttamente.

- L'uso di strumenti di monitoraggio della rete può essere utile nel rilevare attacchi ARP Poisoning in tempo reale, ma richiede l'installazione e la configurazione di tali strumenti e la competenza per interpretare correttamente i dati di monitoraggio.

- L'implementazione di una VPN può offrire un livello aggiuntivo di sicurezza per proteggere il traffico di rete da attacchi ARP Poisoning, ma può comportare costi aggiuntivi e complessità nella gestione della VPN stessa.

In sintesi, le azioni di mitigazione dell'ARP Poisoning sono efficaci nel proteggere una rete locale dai potenziali attacchi, ma richiedono una combinazione di configurazioni tecniche, strumenti di monitoraggio e misure di sicurezza aggiuntive, che possono richiedere tempo, sforzo e risorse per essere implementate e mantenute efficacemente.