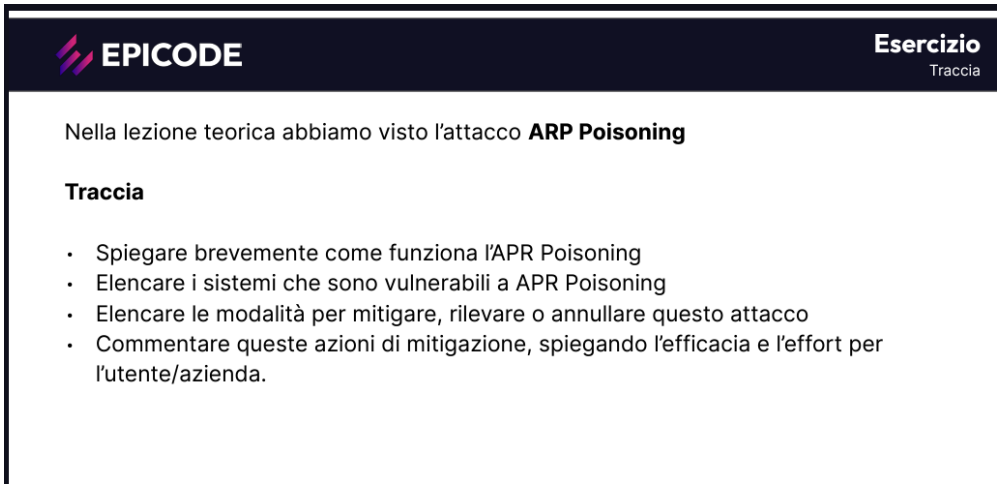
ESERCITAZIONE WEEK 15 DAY 3



L'ARP Poisoning e il conseguente ARP Spoofing, sono attacchi che sfruttano la debolezza del protocollo ARP (Address Resolution Protocol) utilizzato nelle reti locali per associare gli indirizzi IP agli indirizzi MAC. Viene coinvolta la manipolazione della tabella ARP di un dispositivo di rete, spesso con l'obiettivo di indirizzare il traffico di rete attraverso un dispositivo controllato dall'attaccante.

Funzionamento dell'ARP Poisoning:

1. **Intercettazione ARP:** L'attaccante invia pacchetti ARP falsificati alla rete, annunciando un indirizzo IP fittizio associato al proprio indirizzo MAC.
2. **Aggiornamento delle tabelle ARP:** I dispositivi nella rete aggiornano le loro tabelle ARP con l'informazione falsificata, associando l'indirizzo IP al MAC dell'attaccante.
3. **Reindirizzamento del traffico:** L'attaccante può ora intercettare o inoltrare il traffico destinato all'indirizzo IP fittizio.

Sistemi vulnerabili a ARP Poisoning:

- **Dispositivi di rete non protetti:** Switch, router, e host che non implementano misure di sicurezza contro ARP Spoofing.

Modalità per mitigare, rilevare o annullare l'attacco:

1. **Mitigazione:**
    - **Implementazione di DHCP statico:** Assegnare manualmente gli indirizzi IP ai dispositivi anziché utilizzare DHCP dinamico riduce la vulnerabilità agli attacchi ARP.
    - **Configurazione di ARP Inspection sui dispositivi di rete:** Impedire il cambio non autorizzato nella tabella ARP.
2. **Rilevamento:**
    - **Monitoraggio delle anomalie ARP:** Rilevare variazioni anomale nelle tabelle ARP e nell'attività di rete.
    - **Utilizzo di strumenti di rilevamento ARP Spoofing:** Software che rileva e segnala l'attività ARP sospetta.
3. **Annullamento:**

- **Utilizzo di tecnologie di crittografia:** Proteggere il traffico di rete attraverso l'uso di VPN o protocolli sicuri riduce l'impatto di ARP Poisoning.
- **Implementazione di soluzioni di sicurezza avanzate:** Firewall, sistemi di rilevamento delle intrusioni (IDS) e sistemi di prevenzione delle intrusioni (IPS) possono contribuire ad annullare o limitare gli effetti dell'attacco.

Commento sulle azioni di mitigazione:

- **Efficacia:** Le azioni di mitigazione possono ridurre significativamente il rischio di ARP Poisoning, ma nessuna soluzione è completamente immune. La combinazione di diverse misure aumenta l'efficacia complessiva.
- **Effort per l'utente/azienda:** L'implementazione di queste misure richiede un certo sforzo iniziale per la configurazione e la gestione continua. Tuttavia, considerando i rischi associati agli attacchi ARP Poisoning, gli sforzi sono giustificati per mantenere un ambiente di rete sicuro.