ARP POISONING - ESERCIZIO

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.

Esecuzione:

1. Spiegazione di ARP POISONING

Questo metodo di attacco alle reti sfrutta il protocollo **ARP** (**Address Resolution Protocol**). Quest'ultimo permette ad un sistema di associare l'indirizzo MAC di una scheda di rete all'indirizzo IP che un client intende raggiungere per avere una connessione. Esso manda delle richieste a tutti i dispositivi, presenti in una rete, e attende riscontro da quella macchina che tiene quel determinato indirizzo IP per poter poi associare il relativo indirizzo MAC. Tutte le associazioni vengono salvate all'interno della macchina che attua il protocollo al fine di poter effettuare una connessione diretta. Se una delle macchine cambia MAC ma non IP, questa riutilizzerà quel protocollo.

Questo protocollo si basa sulla "fiducia" e ciò è una potenziale vulnerabilità, soggetta ad un attacco del tipo **ARP Poisoning**. Un potenziale attaccante manda nella rete dei pacchetti ARP falsificati, dichiarandosi con l'indirizzo IP di una macchina presente nella rete (quale potrebbe essere uno switch, un server etc…). Con questo invio, i pc presenti in quella rete riassociano (nelle loro relative tabelle) il nuovo indirizzo MAC relativo a quel IP. In questo modo l'attaccante può ricevere i pacchetti che transitano nella rete e vederne il contenuto, che potrebbero essere anche dati sensibili.

2. Sistemi vulnerabili all'ARP Poisoning

I sistemi che possono essere vulnerabili potrebbero essere i seguenti:

- Una errata configurazione del protocollo ARP
- Un sistema/macchina non gestito lato sicurezza
- Wi-fi non correttamente configurate
- Reti locali in LAN non correttamente configurate e protette, quali anche Hub e switch stessi.

In tutte queste si può presentare un **Man in the Middle (MitM)** che sfruttando l'attacco citando l'attacco precedentemente citato, può fingersi una delle macchine configurate nella rete. Sistemi come questi che non gestiscono una tale avversità, potrebbero essere soggetti a **sniffing** e **spoofing**.

3. Modalità di mitigazione, rilevamento o annullamento

Di seguito riportiamo alcune indicazioni possibili per poter risolvere o trovare un attacco ARP Poisoning:

1. **Utilizzo di sistemi di sicurezza**: quali potrebbero essere firewall IDS che bloccano le attività identificate come sospette nella rete, analizzando i pacchetti in transito, la loro provenienza e relativa destinazione e tipologia di richiesta.
2. **Configurazione manuale (statica) delle tabelle ARP:** un utilizzo controllato, inserendo manualmente gli indirizzi MAC in una ARP Table, impedisce ad un sistema di cambiarlo qual ora questo venisse sostituito senza avviso o senza aver messo a conoscenza il proprietario della rete.
3. **Utilizzo di protocolli crittografati:** anche se ipoteticamente un attaccante riuscisse ad effettuare un ARP Poisoning, e quindi riuscisse ad intercettare il traffico all'interno di una rete, con dei protocolli di crittografia attivi (quale un HTTPS) non sarebbe in grado di leggere il traffico in transito nella rete.
4. **Aggiornamenti dei sistemi:** sistemi operativi di qualsiasi macchina (switch, firewall, pc etc...) deve tenere il passo con gli aggiornamenti del proprio sistema operativo. Periodicamente vengono rilasciate release o patch che correggono le vulnerabilità o ne potenziano la difesa delle stesse.
5. **Utilizzo di macchine gestite:** utilizzare macchine o sistemi operativi che possiedono livelli di sicurezza alti, come ad esempio il post security, che limita il numero di indirizzi MAC associati ad una porta specifica o proteggendo le stesse tramite password di accesso.
6. **Monitoraggio del traffico ARP**
7. **Rilevamento di ARP Spoofing:** Implementare sistemi di rilevamento che analizzano il traffico per identificare un comportamento tipico di ARP Poisoning. Questi potrebbero mandare avvisi di comportamento anomalo e/o implementare azioni di difesa.

4. Spiegazione sull'efficacia delle correzioni ed efforts

Tutte le azioni precedentemente indicate sono soluzioni implementabili che permettono di contrastare un potenziale attacco ARP Poisoning. Alcuni di questi sono anche implementabili fin da subito e senza eccessivi costi in quanto facenti parte della rete o del S.O. che presentano al suo interno, come ad esempio i punti **4**, **3** e **2**. Una riconfigurazione delle comunicazioni con protocolli crittografici o l'aggiornamento di tutti i sistemi presenti in una rete sono sicuramente utili e mitigano la possibilità dell'attacco, a patto che ciò che utilizza la rete per lavorare possa ospitare determinati cambiamenti di questo livello, che sono prontamente software.

Gli altri punti quali **1**, **5**, **6** e **7** richiedono una azione più invasiva, quali potrebbero essere il cambio delle macchine presenti nella rete o implementazione di nuove che eseguono uno dei punti richiesti. Potrebbe comportare dei costi al fine di poter essere applicate, con il beneficio di isolare le varie sotto reti presenti in una azienda e di tutelare le macchine contenenti file o dati sensibili che è bene non vengano raggiunte da un attaccante.