**Esercizio ARP-Poisoning**

Utilizzando Ettercap andiamo a simulare un attacco ARP-Poisoning. La macchina web vittima è a piacere, in alternativa si può usare: vulnweb. http://testphp.vulnweb.com/login.php

Fare un report su:

* Cos’è il protocollo ARP.
* Cosa sono gli attacchi MITM.
* Cos’è l'attacco ARP-Poisoning.
* Le fasi dell'attacco.

**Cos’è il protocollo ARP**

Il protocollo ARP (Address Resolution Protocol) è un protocollo utilizzato in reti IP per mappare un indirizzo di rete (come un indirizzo IP) a un indirizzo fisico di rete (come un indirizzo MAC). Quando un dispositivo vuole comunicare con un altro nella stessa rete locale e conosce solo il suo indirizzo IP, usa ARP per scoprire l'indirizzo MAC corrispondente. In questo modo, il dispositivo può indirizzare correttamente i pacchetti di dati al destinatario giusto nella rete locale.

**Cosa sono gli attacchi MITM**

Gli attacchi MITM (Man-In-The-Middle) sono una categoria di attacchi informatici in cui un aggressore si interpone segretamente nella comunicazione tra due parti, intercettando e potenzialmente alterando i dati scambiati. In questo tipo di attacco, l'aggressore può ascoltare segretamente la comunicazione, rubare dati sensibili, manipolare i messaggi scambiati o impersonare una delle parti per ingannare l'altra.

**Cos’è l'attacco ARP-Poisoning**

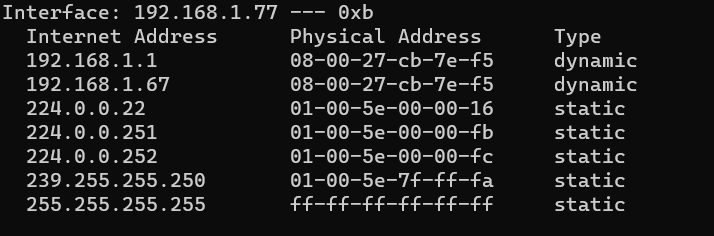
L'attacco ARP-Poisoning, una forma di attacco MITM specifica per le reti locali, sfrutta il protocollo ARP. L'aggressore invia messaggi ARP falsificati nella rete per associare il proprio indirizzo MAC con l'indirizzo IP di un'altra macchina nella rete (spesso il gateway). Questo fa sì che il traffico destinato a quella macchina venga inviato all'aggressore, permettendogli di intercettare, leggere o modificare i dati prima di inoltrarli alla destinazione corretta.

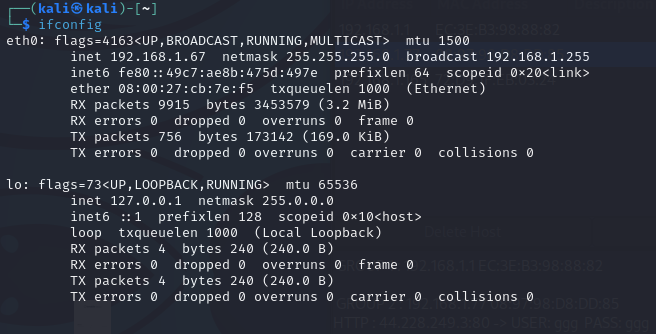
**Le fasi dell'attacco**

Scansione della rete: L'aggressore esegue una scansione della rete per identificare gli indirizzi IP e MAC dei dispositivi connessi.

Creazione di pacchetti ARP falsificati: L'aggressore crea pacchetti ARP con informazioni false, indicando che l'indirizzo IP di un determinato dispositivo (ad esempio, il gateway della rete) è associato al suo indirizzo MAC.

Diffusione dei pacchetti falsificati: Questi pacchetti vengono inviati nella rete. I dispositivi che ricevono questi pacchetti ARP falsificati aggiornano le loro tabelle ARP, riassegnando l'indirizzo IP del dispositivo bersaglio all'indirizzo MAC dell'aggressore.





Intercezione del traffico: Con le tabelle ARP modificate, il traffico destinato al dispositivo bersaglio (come il gateway) viene inviato all'aggressore.

Analisi e/o manipolazione del traffico: L'aggressore può quindi esaminare o modificare i dati intercettati prima di inoltrarli al destinatario originale, mantenendo l'illusione di una comunicazione normale.

Inoltro del traffico: Infine, l'aggressore inoltra il traffico al destinatario previsto, evitando di suscitare sospetti.

Questo tipo di attacco è particolarmente pericoloso in quanto può avvenire in modo trasparente, senza che le vittime si rendano conto.

A screenshot of a computer

Description automatically generated