Ettercap

Descrizione dell’esercizio

L’esercizio ci chiede di simulare un attacco ARP-Poisoning utilizzando Ettercap e scrivere 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 di rete utilizzato per associare un indirizzo IP a un indirizzo MAC all’interno di una rete locale.

Tutto ciò avviene tramite la tabella ARP dove viene prima fatto un tentativo per associare un IP a un MAC. In caso di riscontro avviene l’associazione di IP/MAC, in caso di esito negativo invece viene inviata una richiesta ARP broadcast chiedendo a tutti i dispositivi nella rete di rispondere col proprio indirizzo MAC. Viene quindi aggiornata la tabella ARP con le nuove associazioni IP/MAC per uso futuro.

Cosa sono gli attacchi MITM.

Un attacco MITM (Man in the Middle) avviene quando un attaccante si posiziona fra due parti che cercano di comunicare, intercettando e/o modificando le informazioni scambiate fra di essi.

Un esempio di attacco può essere un attaccante che intercetta il traffico fra la vittima e un Router/Gateway avendo così la possibilità di vedere tutti i dati scambiati in chiaro fra i due, come le credenziali per effettuare un login.

Cos’è l'attacco ARP-Poisoning.

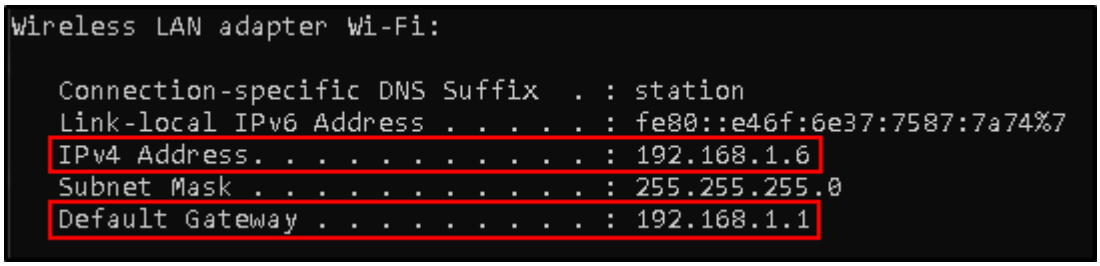
L’ARP Poisoning è un tipo di attacco MITM che manipola le tabelle ARP associando l’indirizzo IP dell’attaccante a un indirizzo MAC utilizzato dalla vittima presente sulla stessa rete.

Il software utilizzato per l’attacco (nel nostro caso Ettercap) intercetta quindi tutti i dati permettendo all’attaccante di leggerli o modificarli prima di inviarli al destinatario reale.

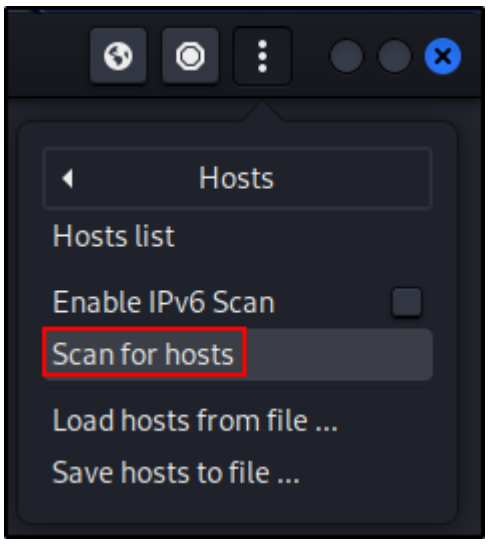
Nell’attacco che andremo a vedere con Ettercap ci limiteremo ad intercettare e leggere le credenziali inviate in chiaro sulla rete.

Le fasi dell'attacco.

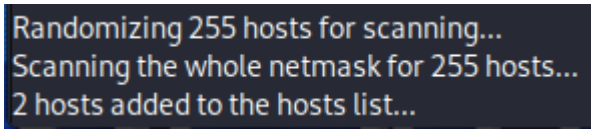
Per prima cosa abbiamo bisogno dei due IP da specificare come target dell’attacco, in questo caso sto usando l’IP privato del mio dispositivo Windows e l’IP del mio gateway, che posso recuperare tramite il comando ipconfig



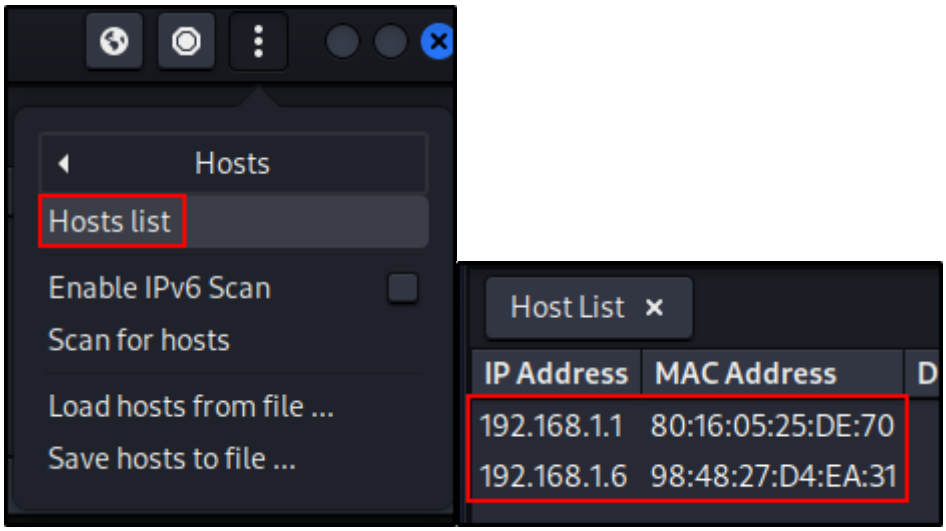
Apro quindi Ettercap su Kali e clicco in alto a destra su Hosts > Scan for hosts per permettere al programma di trovare gli host presenti sulla rete



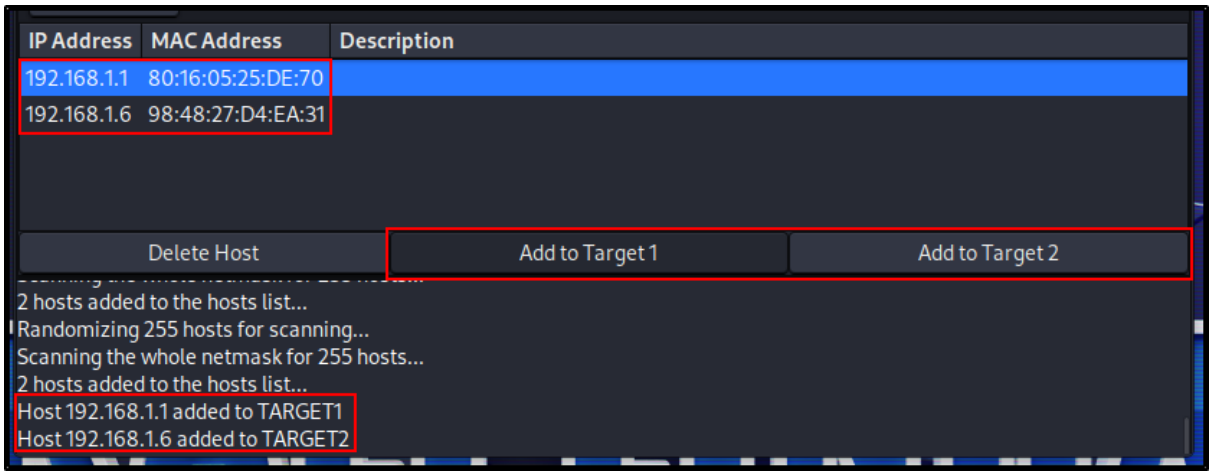
Dopo qualche secondo Ettercap mi trova i due host presenti sulla rete



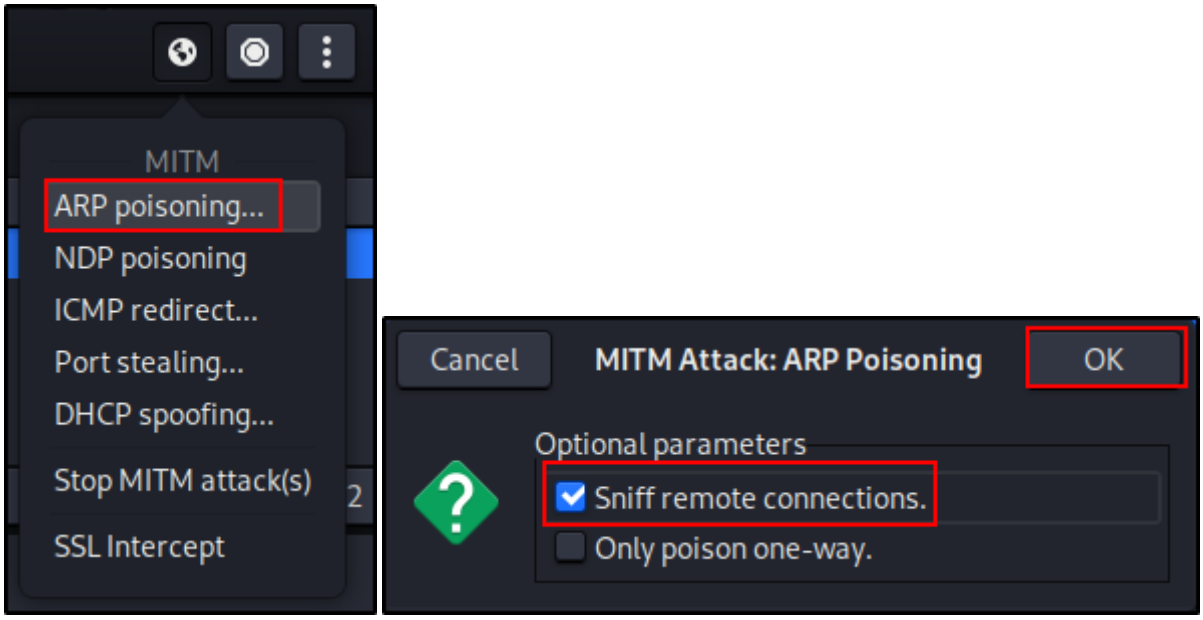
Cliccando su Hosts > Hosts list posso vedere l'elenco degli host trovati



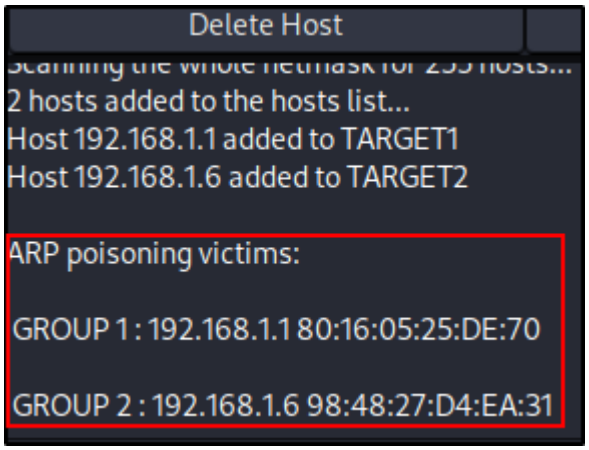
Seleziono quindi un host da usare come primo bersaglio cliccando su Add to Target 1 e ripeto lo stesso processo per il secondo host



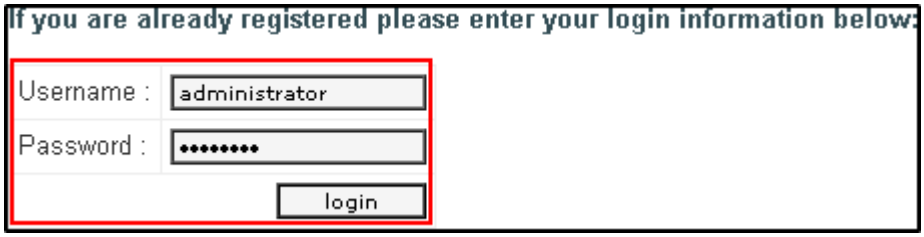
Per far partire l'attacco clicco sul pulsante MITM in alto a destra e seleziono ARP poisoning, assicurandomi che il parametro Sniff remote connections sia attivo



Dal terminale di Ettercap è possibile vedere che l'attacco è partito con successo



Per testare l'attacco vado sull'URL http://testphp.vulnweb.com/login.php usando la mia macchina Windows che farà da vittima e provo ad inserire delle credenziali nel form di login e clicco su login per inviare la richiesta



Le credenziali utilizzate in questo caso sono username: administrator e password:password

Tornando su Ettercap posso confermare dal terminale che ha catturato le credenziali in chiaro