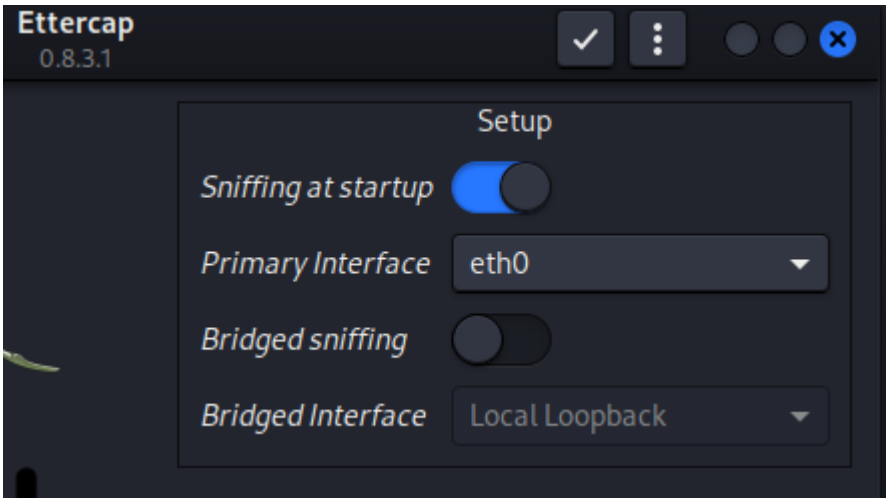
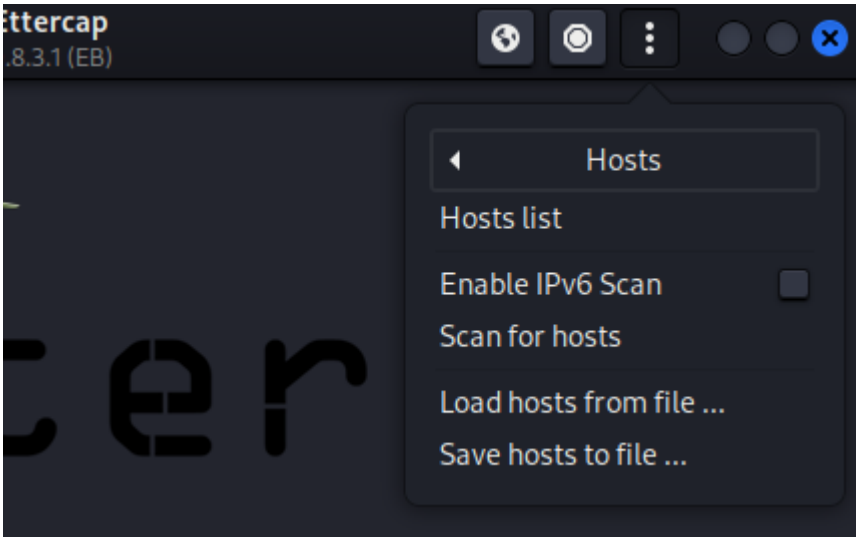
- Cos'è il protocollo ARP?
  ARP (Address Resolution Protocol) è un protocollo che collega un indirizzo ip ad un indirizzo fisso di una macchina fisica, quindi l'indirizzo MAC.
- Cos'è un attacco MITM (Man In The Middle)?
  Un attacco MITM è quando l'attaccante si inserisce "in mezzo" ad una comunicazione tra due parti legittime intercettando la comunicazione e permettendo di inviare o ricevere dati ad una parte legittima senza che ne siano consapevoli.
- Cos'è un attacco ARP-Poisoning?
  Un attacco ARP-Poisoning riguarda la manipolazione della tabella di traduzione degli indirizzi IP nei pacchetti di rete, inviando messaggi ARP falsificati all'interno di una rete locale al fine di corrompere le associazioni tra indirizzi Mac e IP degli host presenti su quella rete. L'obiettivo è di intercettare la comunicazione tra i dispositivi di rete consentendo di ottenere le informazioni sensibili oppure permettendo di modificare o inviare pacchetti di dati nella rete.

- Simulo un attacco ARP-Poisoning dalla macchina kali al mio computer.

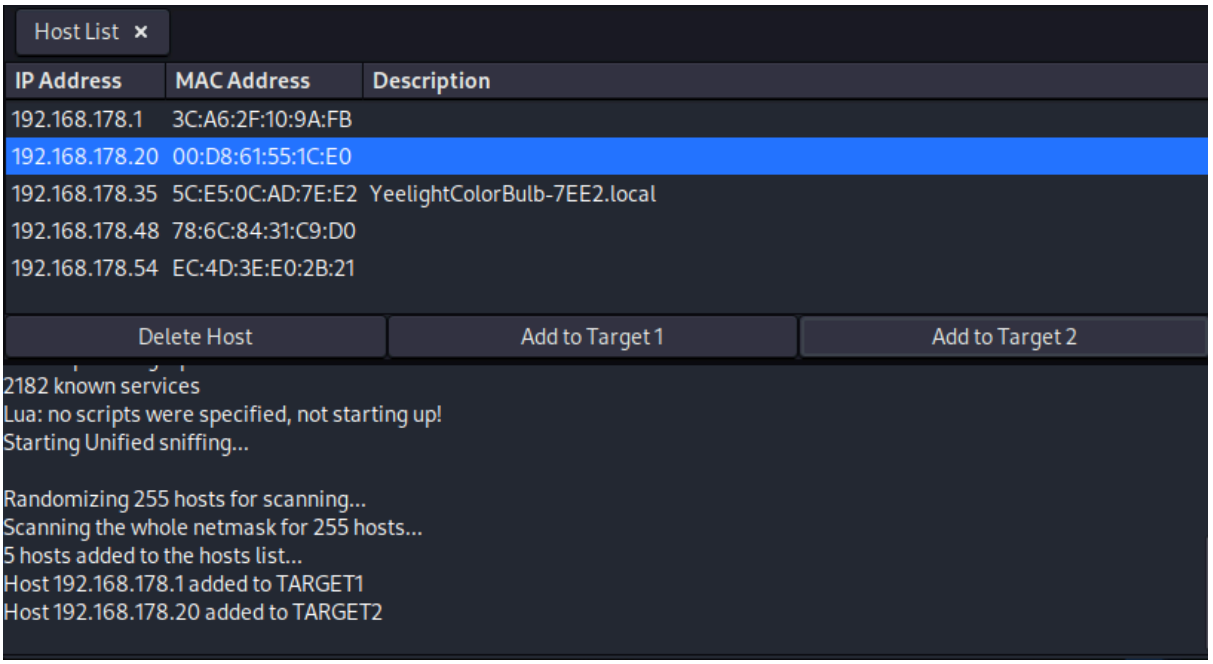
Le fasi di un attacco sono, di avviare ettercap sulla macchina dell'attaccante e cliccare sulla spunta che sta in alto a destra.



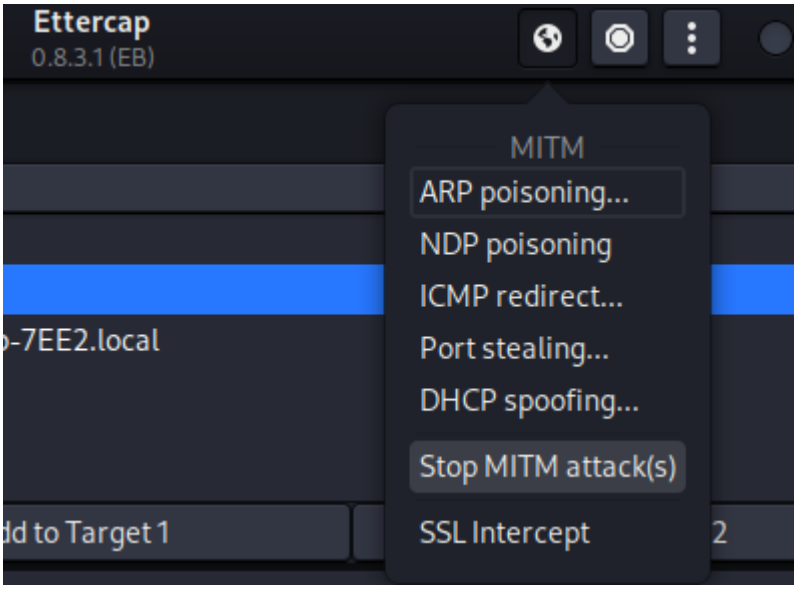
Dopo aver fatto questo cliccando sui tre punti in alto vado a fare uno scan for hosts e apro la hosts list.



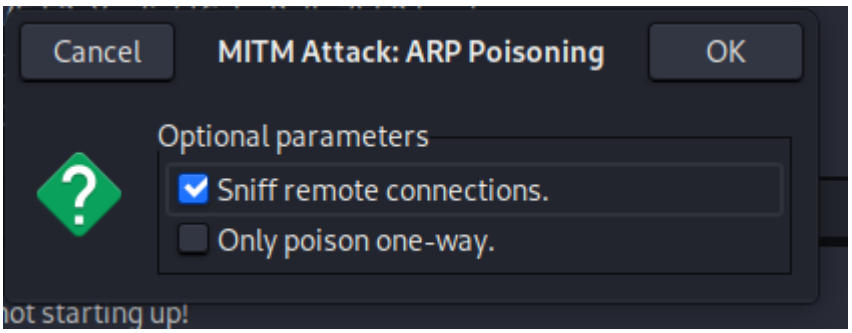
Vedremo che ettercap ci ha dato una lista di host della rete che abbiamo scannerizzato. Ora vado a selezionare il target 1 e 2 che sono la macchina che vogliamo attaccare e l'indirizzo ip del modem-router-gateway.

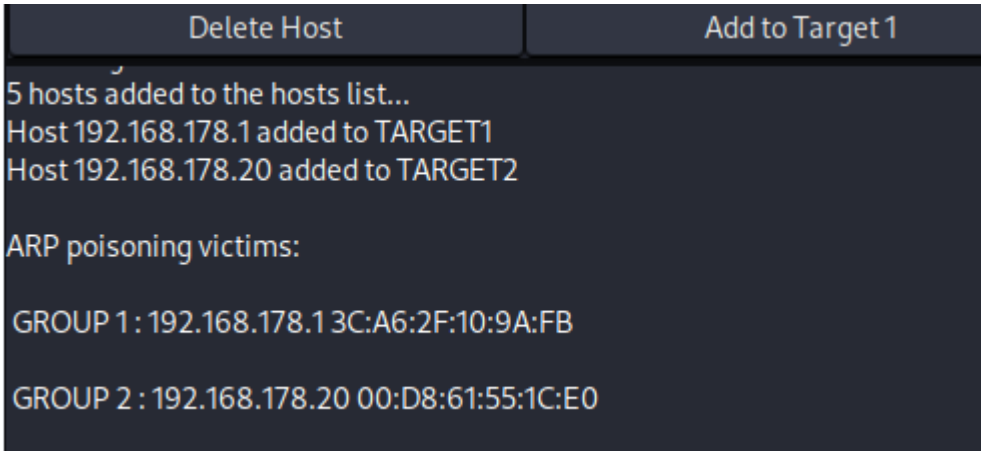


Dopo aver fatto questo cliccare sull'icona del globo in alto a destra e andare su "ARP poisoning".

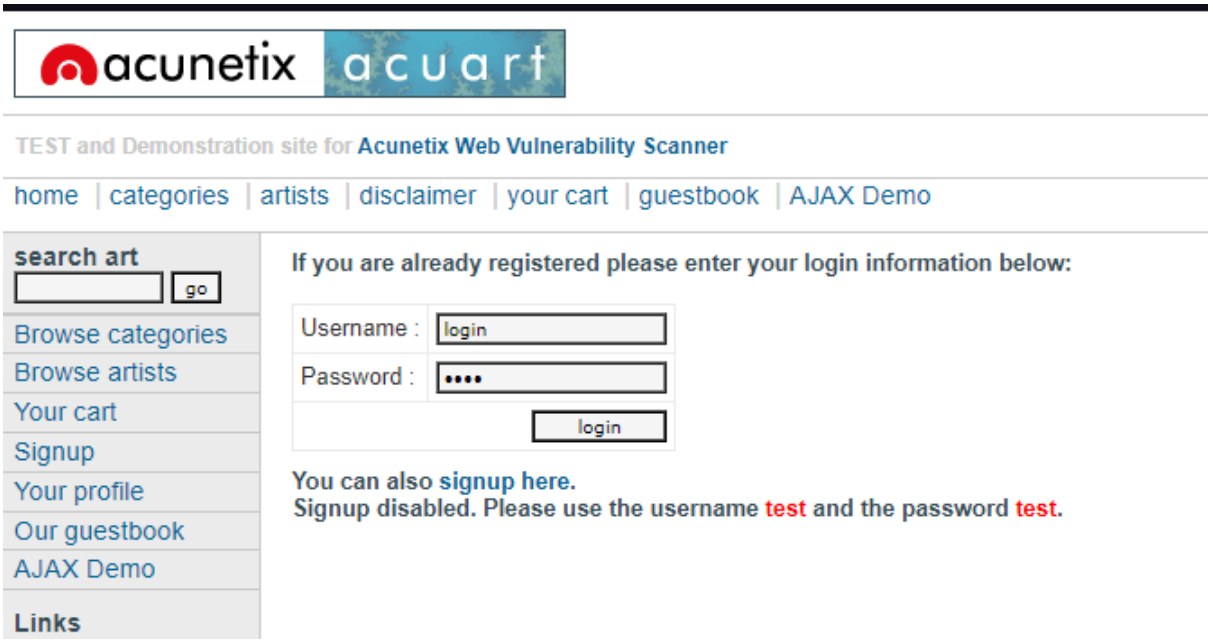


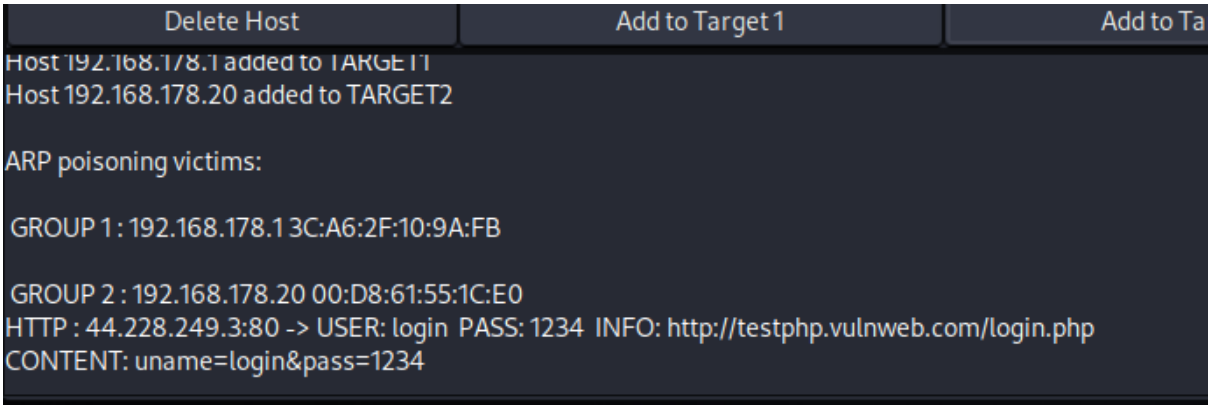
Appare una finestra con selezionato "sniff remote connections." e successivamente premere OK.





Una volta fatto questo, per fare un test vado sulla pagina http://testphp.vulnweb.com/login.php e nella sezione “Your Profile” metto dei dati di login a caso e noto che su ettercap appariranno i dati di login inseriti.





Così facendo sono arrivato ad ottenere i dati di login del sito inseriti dalla macchina che ho intercettato.