PRATICA S6/L1

Lo scopo di questa pratica è di utilizzare Ettercap per simulare un attacco ARP-Poisoning. E poi fare un Report su: cose'è il protocollo ARP, Cosa sono gli attacchi MITM, Cos'è l'attaco ARP-Poisoning, e quale sono le fase dell'attacco.

1) Protocollo ARP

Il Protocolo ARP(Address Resolution Protocol) è un protocollo di rete utilizzato per mappare un indirizzo di livello di collegamento a un indirizzo di livello di rete.

Questo protocollo facilità la comunicazione nella stessa rete locale, aiutando a determinare gli indirizzi MAC associati agli IP all'interno della rete.

2)Attacchi MITM

Gli attacchi MITM(Man In The Middle),sono attachi informatico in cui un aggressore si inserisce in una communicazione tra due parti legitime e la intercetta o controlla attivamente la communicazione.

Questi tipi di attacchi sono molto pericolosi perche permettono all'attacante di: intercettare, inviare e ricevere dati destinati all'entità legittima senza che le parti coinvolte ne siano consapevolli.

3)Attacco ARP-Poisoning

L'Attaco ARP-Poisoning: è un attacco che si può utilizzare per intercettare del traffico su una rete basata su switch.

Questo attacco a per obiettivo di compromettere la tabella ARP di un dispositivo di rete,come per esempio un computer o un router.mandando pacchetti ARP falsificati alla rete al fine di associare

PRATICA S6/L1

il proprio indirizzo MAC a un indirizzo IP legittimo,sostituendo l'associazione coretta presente nella tabella ARP della vittima.

4) Fasi del Attacco

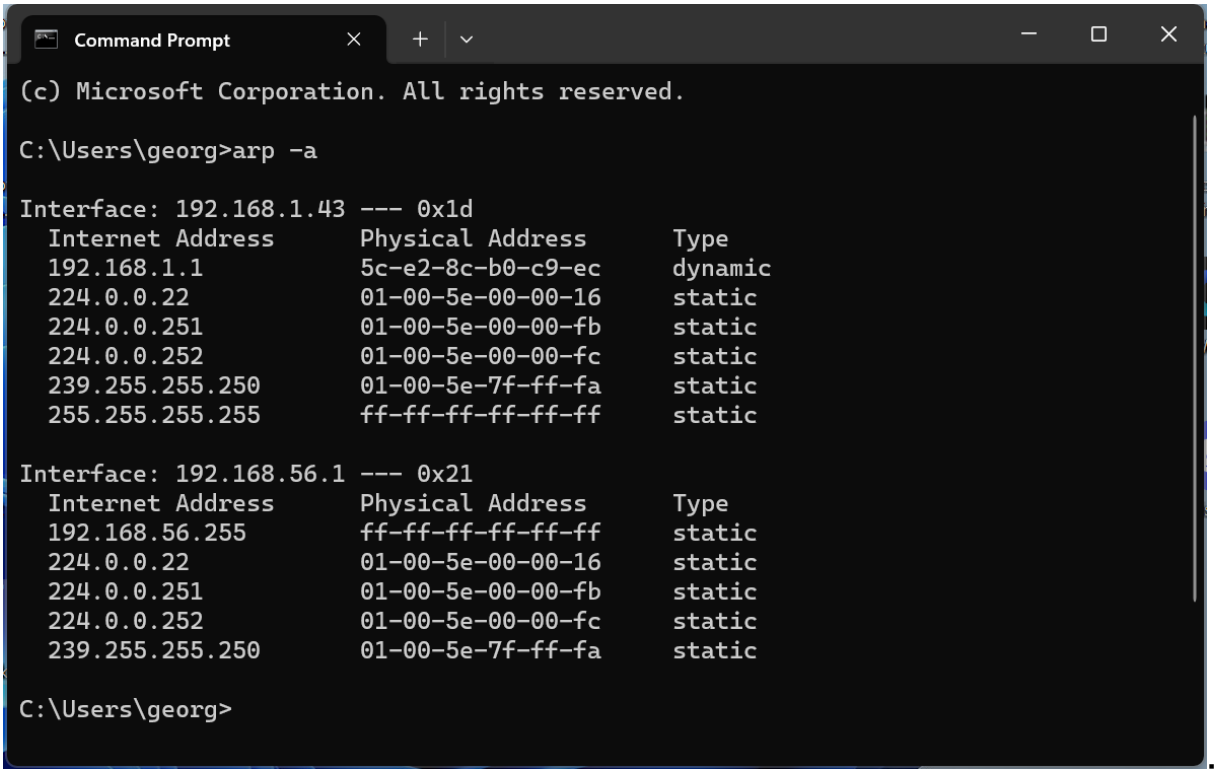
Per l'attacco ARP-Poisoning ,abbiamo utilizzato due sotfware, ETTERCAP e WIRESHARK e abbiamo proseguito come segue:

1- abbiamo apperto su kali linux il software Ettercap e clicato su pulsante di avvio.come in figura sotto

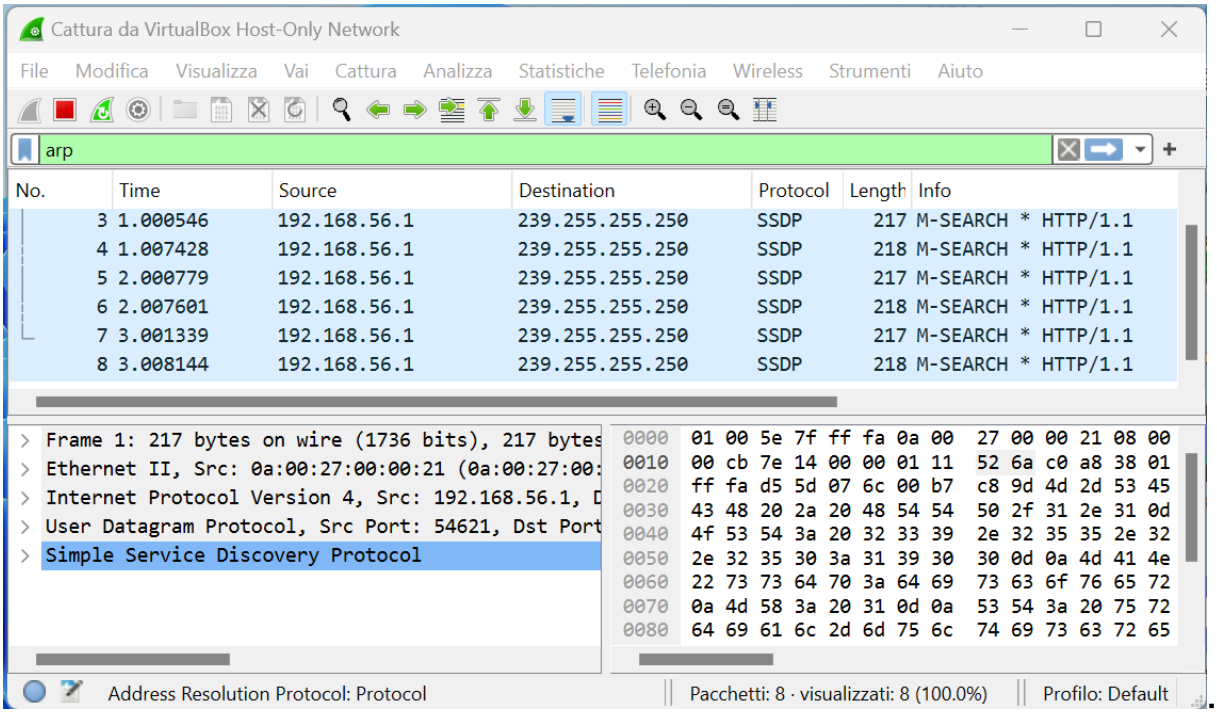
Dopo questo siaomo andati su windows sul nostro command prompt,

E abbiamo inserito la commanda "arp -a" poi ci è venuto questa schermata sotto con una seria di informazione tra quale informazione su indirizzo IP e indirizzo MAC .

PRATICA S6/L1

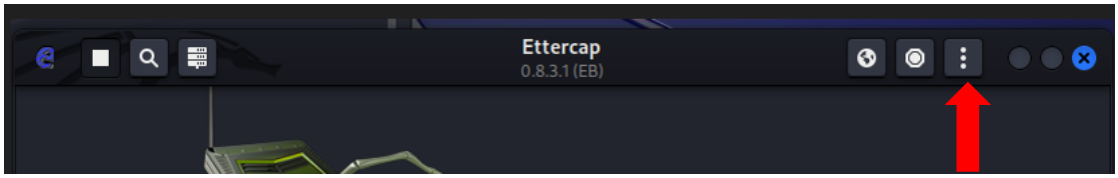


Dopo questo abbiamo aperto wireshark su windows e l'abbiamo avviato,abbiamo ottenuto il risultato seguente:



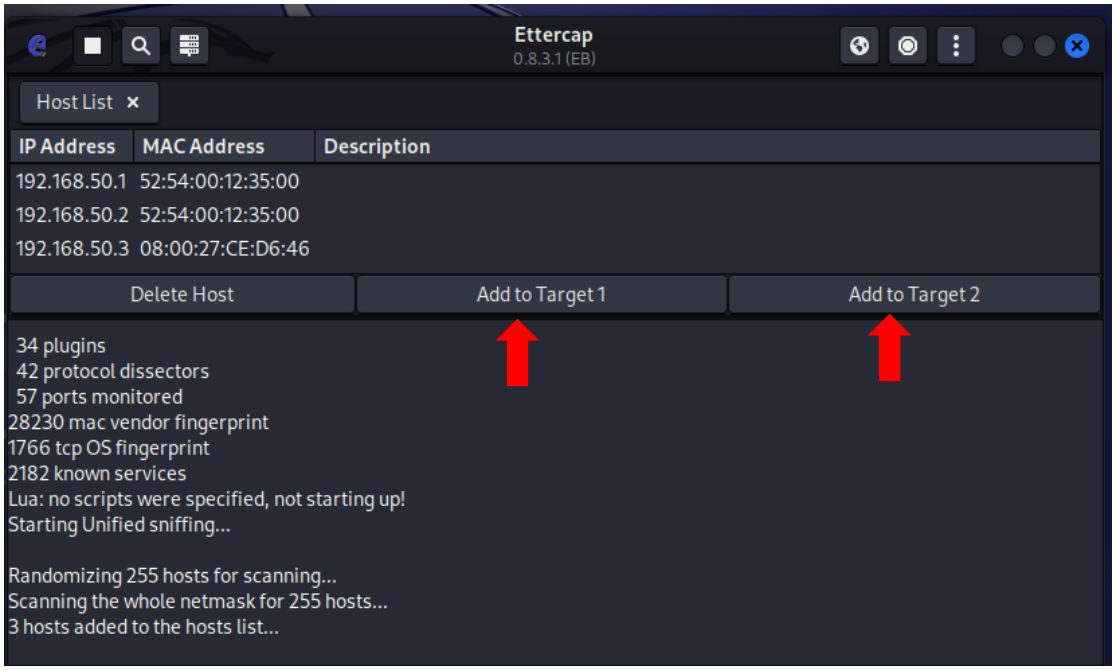
Poi siamo ritornati su Ettercap abbiamo clicato sui tre puntini, selezionato host e poi scan for hosts e in seguito list hosts.

PRATICA S6/L1



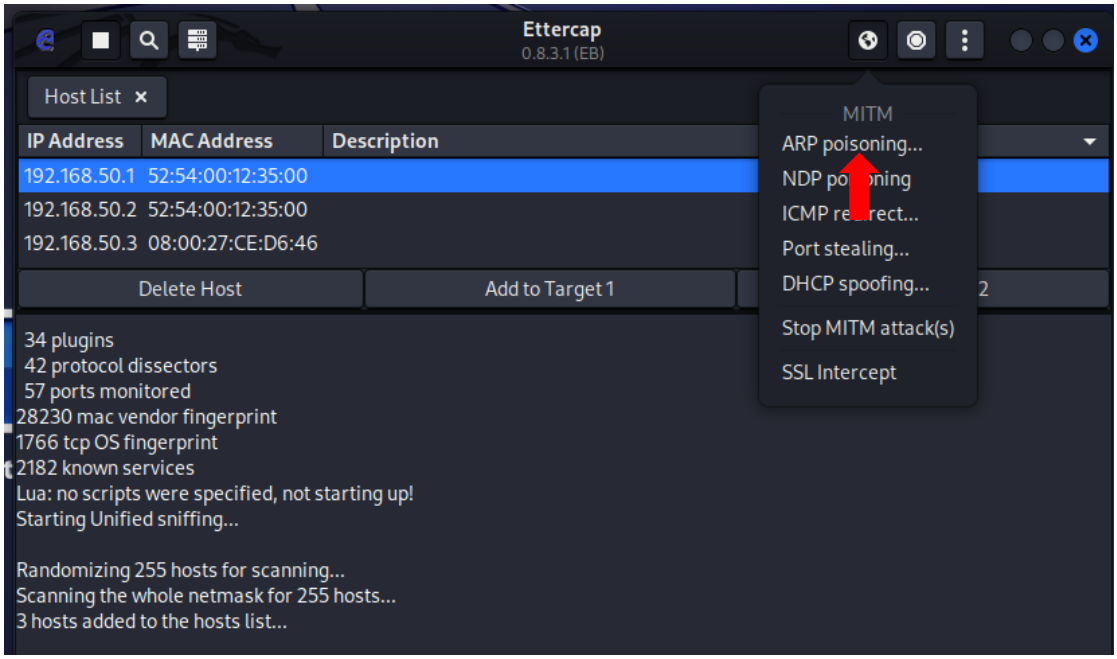
Ci compare la pagina sotto.

A la fine otteniamo questa pagina



PRATICA S6/L1

Poi abbiamo inserito ad Add to Target1 e ad Add to Target2 i diversi indirizzi IP e clicliamo su symbolo del world e poi su ARP Poisoning .



Dopo questo abbiamo nottata che l'indirizzo Mac dell'attacante era associato all'indirizzo ip della vittima. E gli informazioni login che abbiamo inserito su vulnweb erano visibile su Ettercap.