

PRATICA S6/L1

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

1) Protocollo ARP

Il Protocollo 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 facilita 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 attacchi informatici in cui un aggressore si inserisce in una comunicazione tra due parti legittime e la intercetta o controlla attivamente la comunicazione.

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

3)Attacco ARP-Poisoning

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

Questo attacco ha 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

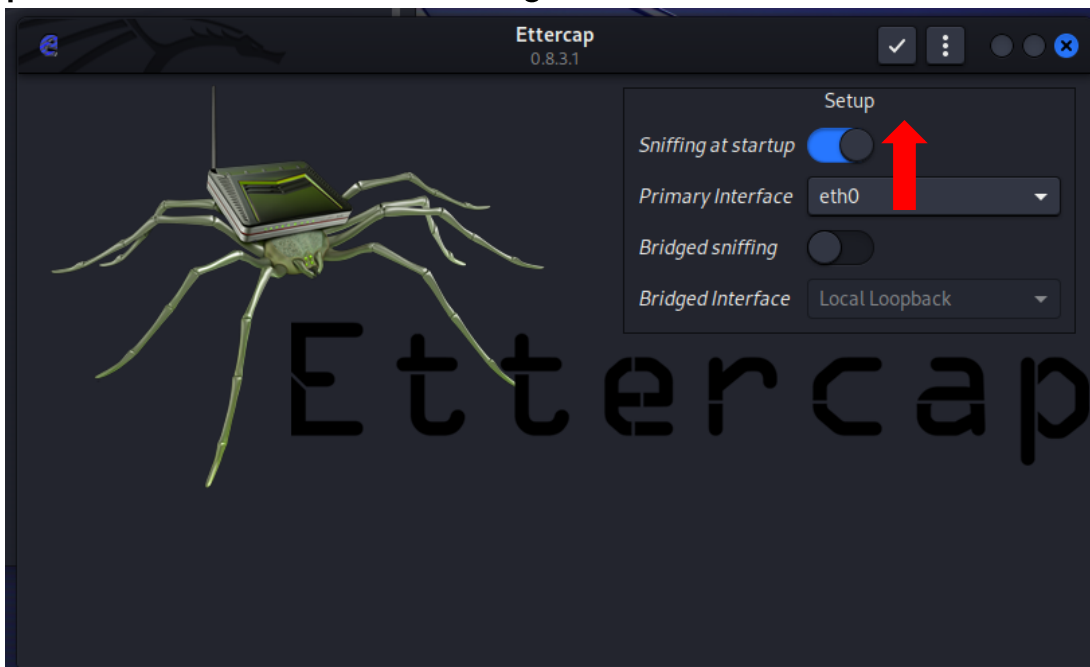
PRATICA S6/L1

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

4) Fasi del Attacco

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

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



Dopo questo siamo 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

```
Command Prompt
(c) Microsoft Corporation. All rights reserved.

C:\Users\georg>arp -a

Interface: 192.168.1.43 --- 0x1d
    Internet Address      Physical Address      Type
    192.168.1.1           5c-e2-8c-b0-c9-ec    dynamic
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x21
    Internet Address      Physical Address      Type
    192.168.56.255       ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static

C:\Users\georg>
```

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

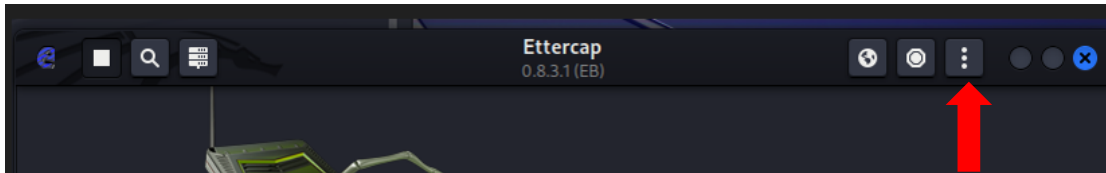
The image shows a Wireshark capture window titled "Cattura da VirtualBox Host-Only Network". The filter bar shows "arp". The packet list shows 8 packets, all of type "SSDP" and "M-SEARCH * HTTP/1.1". The packet details pane shows the structure of the first packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Service Discovery Protocol. The packet bytes pane shows the raw data of the first packet.

No.	Time	Source	Destination	Protocol	Length	Info
3	1.000546	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4	1.007428	192.168.56.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
5	2.000779	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
6	2.007601	192.168.56.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
7	3.001339	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
8	3.008144	192.168.56.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1

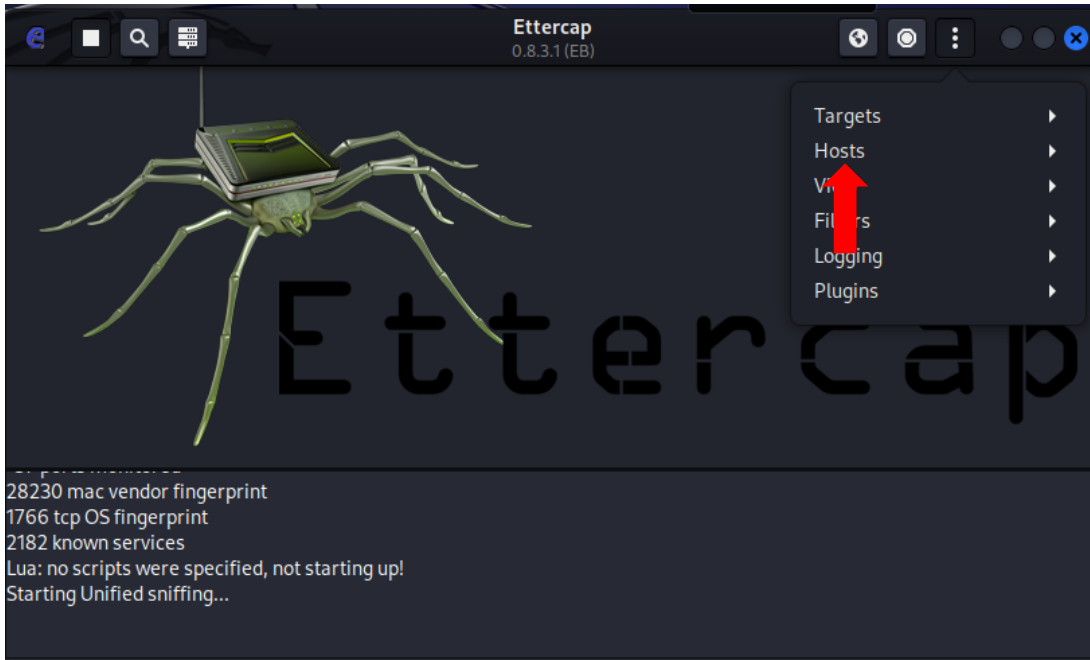
Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
Ethernet II, Src: 0a:00:27:00:00:21 (0a:00:27:00:00:21), Dst: 01:00:5e:7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.56.1, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 54621, Dst Port: 1900
Simple Service Discovery Protocol

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

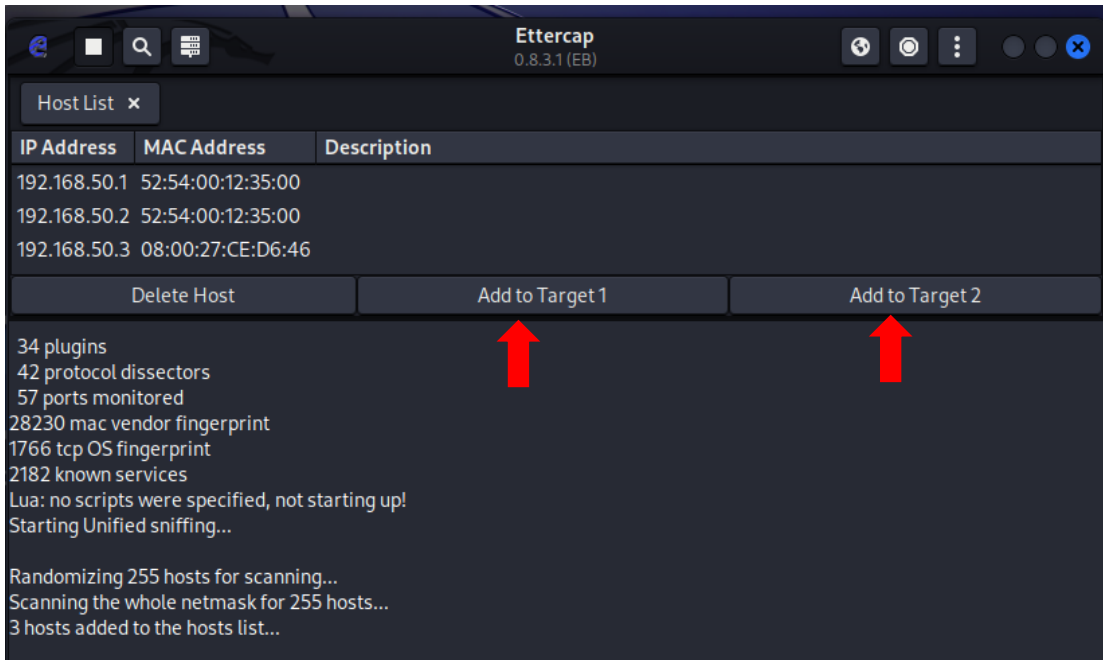
PRATICA S6/L1



Ci compare la pagina sotto.

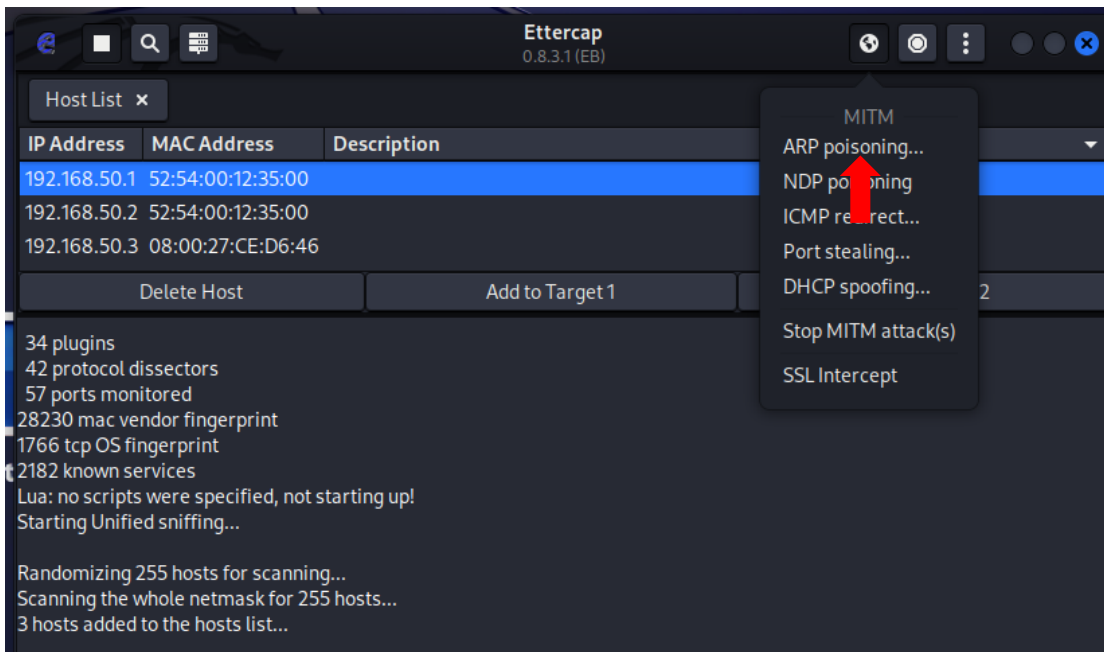


A la fine otteniamo questa pagina



PRATICA S6/L1

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



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