

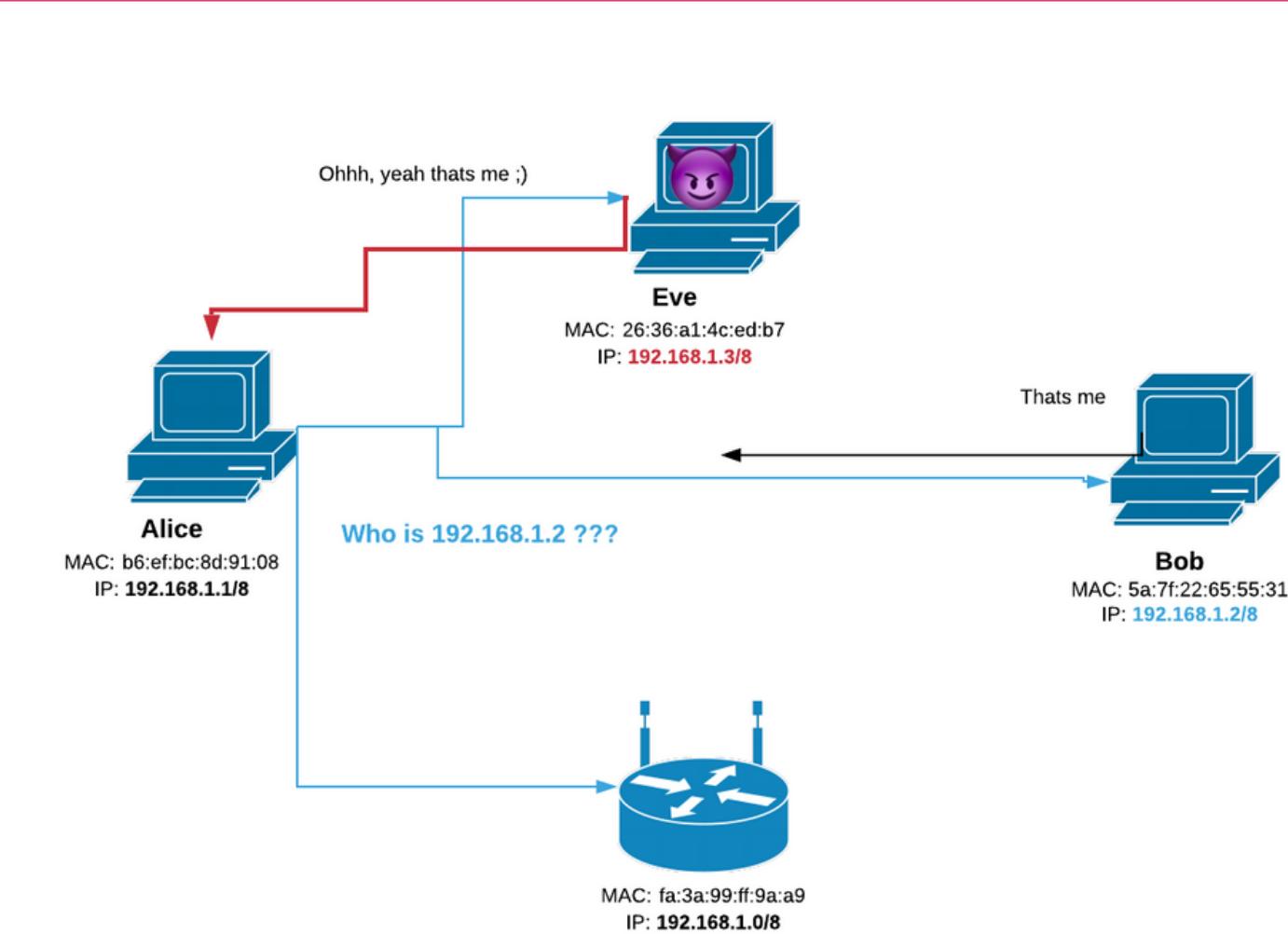
**S6/L1**

MAN-IN-THE-MIDDLE



Nell'esercitazione di oggi andremo ad utilizzare Ettercap per simulare un attacco ARP-Poisoning. La macchina web vittima che ho scelto per quest'esercitazione è vulnweb,

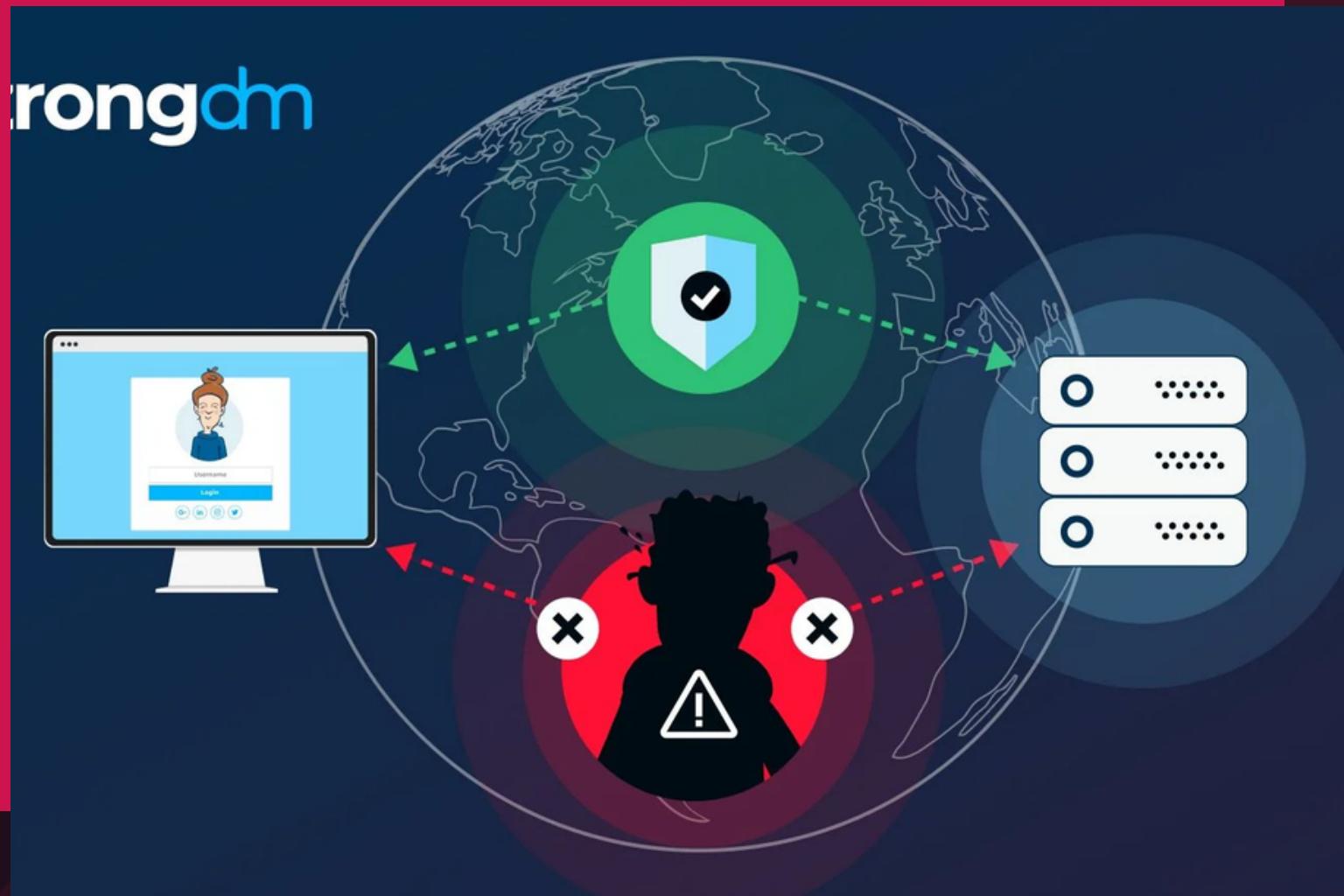
# COS'È IL PROTOCOLLO ARP?



Il protocollo ARP (Address Resolution Protocol) è un protocollo utilizzato nella rete per associare gli indirizzi IP degli host con i rispettivi indirizzi MAC, i quali sono identificatori univoci assegnati alle schede di rete. Quindi il protocollo ARP svolge un ruolo fondamentale per l'instradamento dei pacchetti all'interno di una rete locale.

# COSA SONO GLI ATTACCHI MITM?

Gli attacchi Man-in-the-Middle (MITM) sono un tipo di attacco informatico in cui un aggressore si inserisce in una posizione intermedia tra due parti in una comunicazione, ottenendo così la capacità di intercettare e potenzialmente modificare o manipolare il flusso di dati tra le parti senza che loro ne siano consapevoli.



# ARP POISONING



## COS'È L'ATTACCO ARP - POISONING?

L'attacco ARP poisoning, noto anche come ARP spoofing, è una forma di attacco informatico in cui l'attaccante modifica in modo fraudolento le tabelle ARP di una rete locale. L'attacco ARP poisoning rappresenta una minaccia significativa per la sicurezza delle reti locali e può consentire agli attaccanti di raccogliere informazioni sensibili o compromettere la comunicazione e la sicurezza dei dispositivi sulla rete.

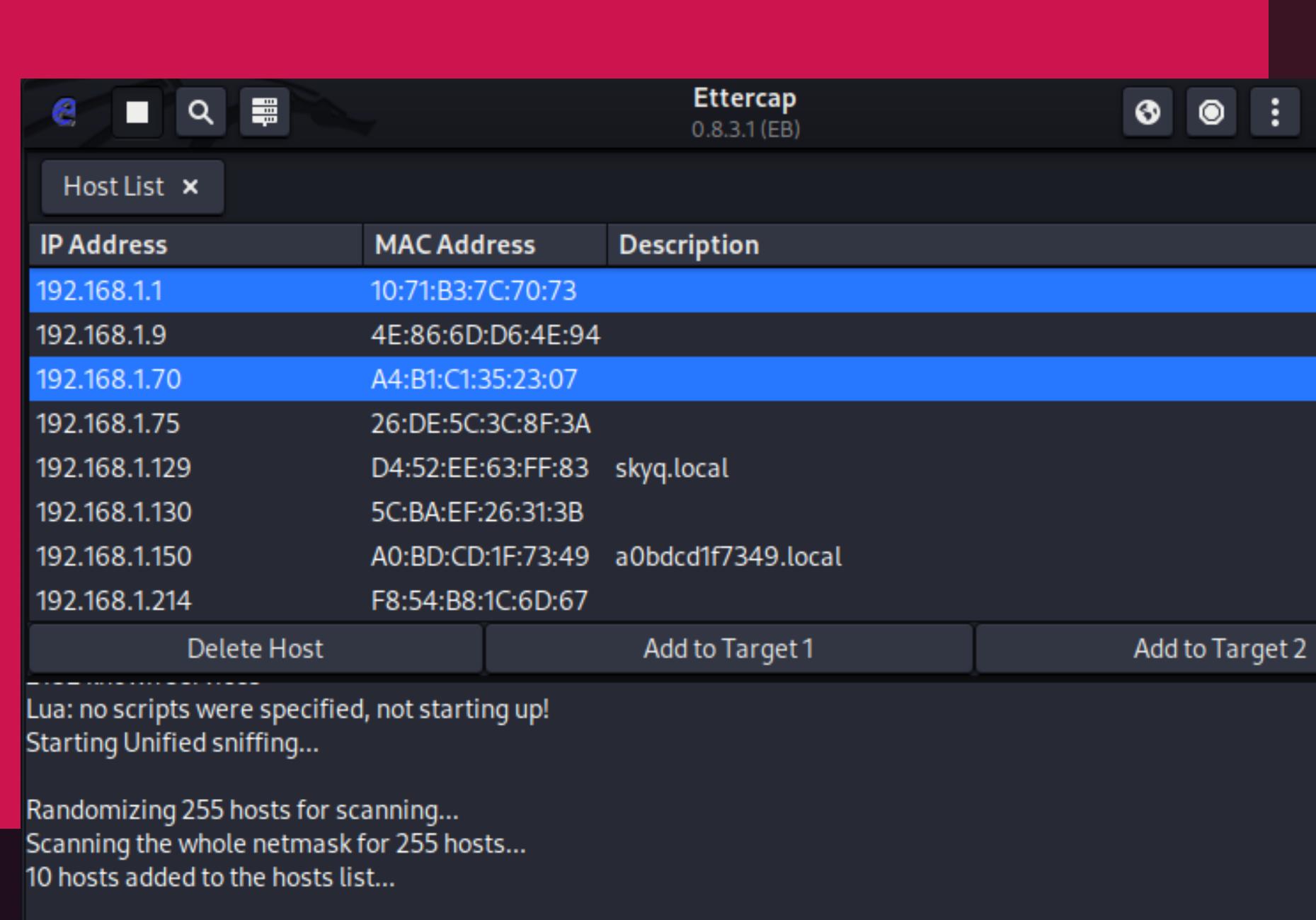
# COME SI ATTUA UN ATTACCO ARP - POISONING?



Schermata principale di Ettercap

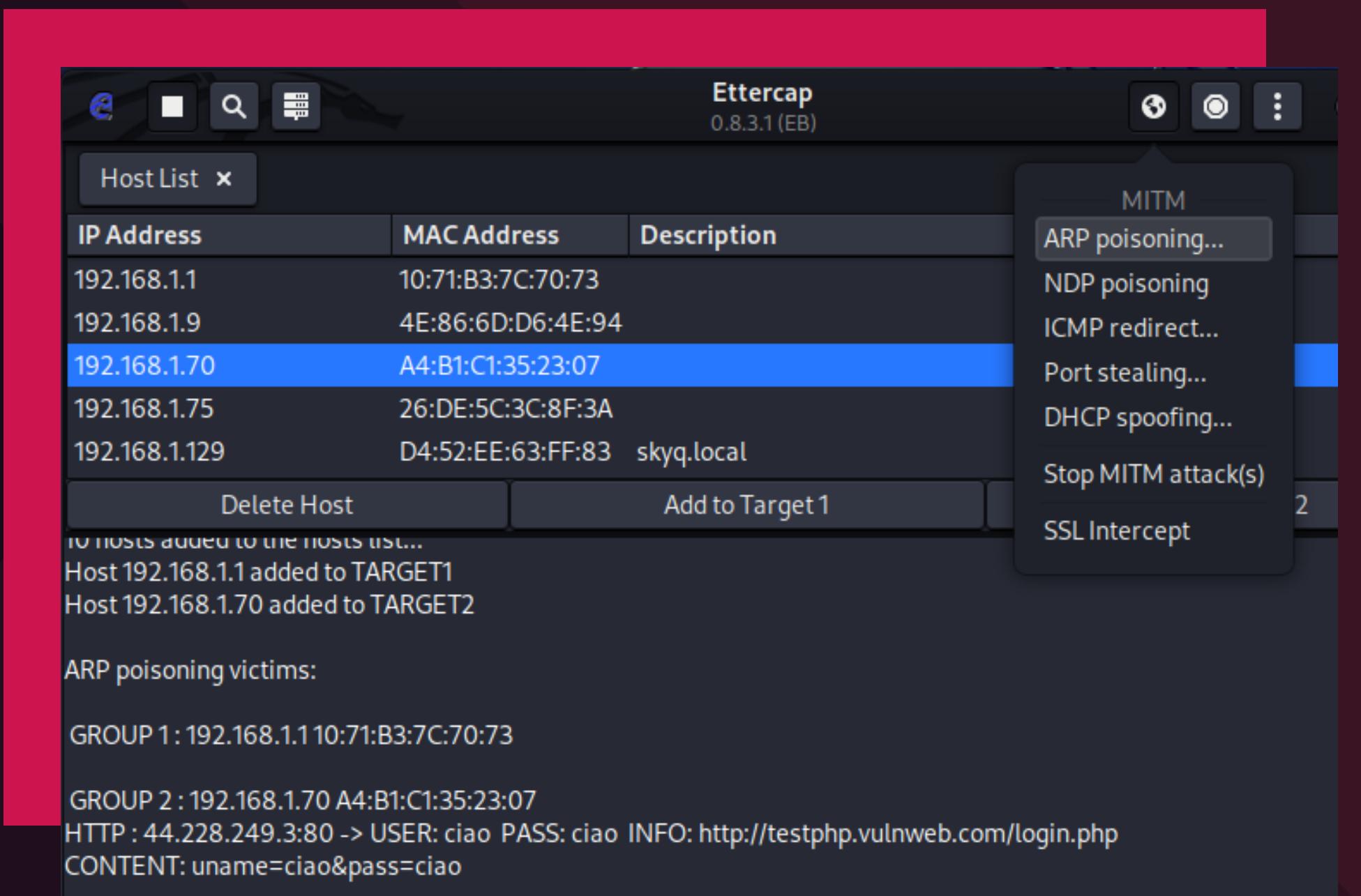
Per eseguire questo attacco avremo la necessità di trovarci all'interno della rete che vogliamo bersagliare, in quanto stiamo operando tra il livello 2 e 3 del modello ISO/OSI, una volta all'interno possiamo procedere avviando l'applicazione Ettercap su Kali, Ettercap è uno strumento di sicurezza informatica ampiamente utilizzato per condurre attacchi di tipo [MITM] all'interno di reti locali.

# COME SI ATTUA UN ATTACCO ARP - POISONING?



Una volta in questa schermata possiamo proseguire andando ad eseguire una scansione degli host presenti sulla rete, dopodichè il nostro intento sarà quello di inserirci nel percorso comunicativo tra il router e un host scelto come bersaglio, andando a “spoofare” gli indirizzi MAC. Una volta che questo è avvenuto saremo in grado di intercettare tutto il traffico che verrà scambiato su quel percorso, andiamo a fare una prova con un pacchetto HTTP, in quanto non siamo in grado di decifrare le comunicazioni cifrate ma solo di intercettarle.

# COME SI ATTUA UN ATTACCO ARP - POISONING?



Scelti i nostri bersagli non ci resterà che selezionarli e clickare sull'icona del mondo come in figura per poter dar inizio all'attacco, quindi selezioniamo ARP-poisoning. L'output che vediamo in figura è un tentativo di accesso che ho effettuato io su Vulnweb in HTTP, come possiamo vedere l'attacco è riuscito, nella prossima slide vedremo come si presenterà la situazione sulla macchina vittima.

Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	08-00-27-cb-7e-f5	dinamico
192.168.1.67	08-00-27-cb-7e-f5	dinamico
192.168.1.129	d4-52-ee-63-ff-83	dinamico
192.168.1.255	ff-ff-ff-ff-ff-ff	statico
224.0.0.22	01-00-5e-00-00-16	statico
224.0.0.251	01-00-5e-00-00-fb	statico
224.0.0.252	01-00-5e-00-00-fc	statico
239.255.255.250	01-00-5e-7f-ff-fa	statico
255.255.255.255	ff-ff-ff-ff-ff-ff	statico

arp

No.	Time	Source	Destination	Protocol	Length	Info
• 2054	4.678175486	PcsCompu_cb:7e:f5	ZyxelCom_7c:70:73	ARP	42	192.168.1.70 is the PcsCompu
2055	4.678199084	PcsCompu_cb:7e:f5	IntelCor_35:23:07	ARP	42	192.168.1.1 is the IntelCor
2681	5.737684139	PcsCompu_cb:7e:f5	ZyxelCom_7c:70:73	ARP	42	Who has 192.168.1.70?
2685	5.738917348	ZyxelCom_7c:70:73	PcsCompu_cb:7e:f5	ARP	60	192.168.1.1 is the ZyxelCom
2696	14.691540481	PcsCompu_cb:7e:f5	ZyxelCom_7c:70:73	ARP	42	192.168.1.70 is the PcsCompu
2697	14.691603001	PcsCompu_cb:7e:f5	IntelCor_35:23:07	ARP	42	192.168.1.1 is the IntelCor

```

> Frame 2055: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface br0
> Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: ZyxelCom_7c:70:73 (08:00:27:cb:7e:f5)
> Address Resolution Protocol (reply)
> [Duplicate IP address detected for 192.168.1.70]
> [Duplicate IP address detected for 192.168.1.1]

```

Come possiamo notare su macchina vittima, andando a fare i giusti controlli possiamo renderci conto di essere vittime di ARP-poisoning, sia grazie al software Wireshark, il quale ci permette di controllare il traffico di rete, sia grazie al comando di terminale arp -a.