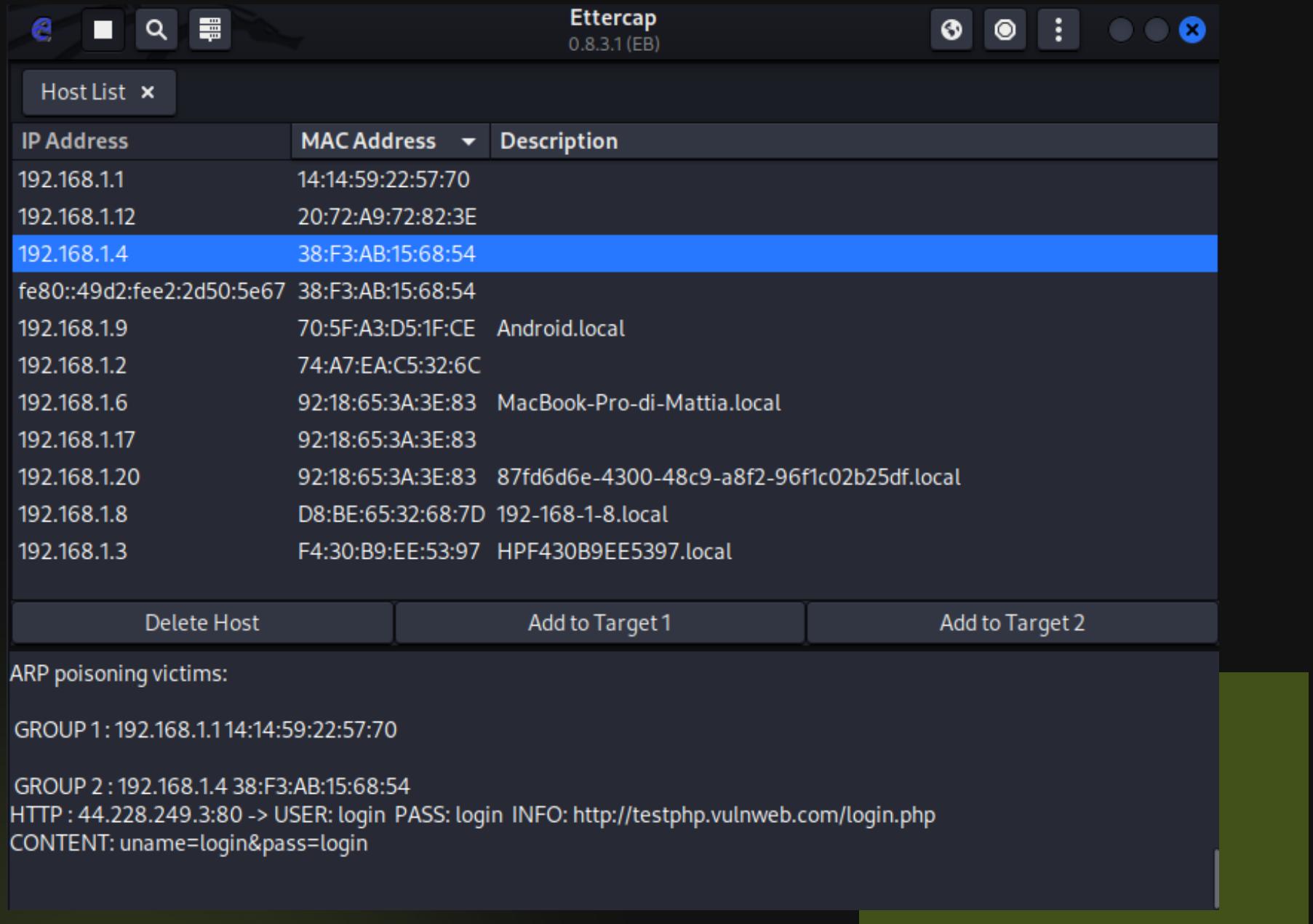




# ETTERCAP

MATTIA PASTORELLI

# CONSEGNA:



Traccia: Utilizzando Ettercap andiamo a simulare un attacco ARP-Poisoning. La macchina web vittima è a piacere, in alternativa si può usare: vulnweb.  
<http://testphp.vulnweb.com/login.php> Fare un report su:

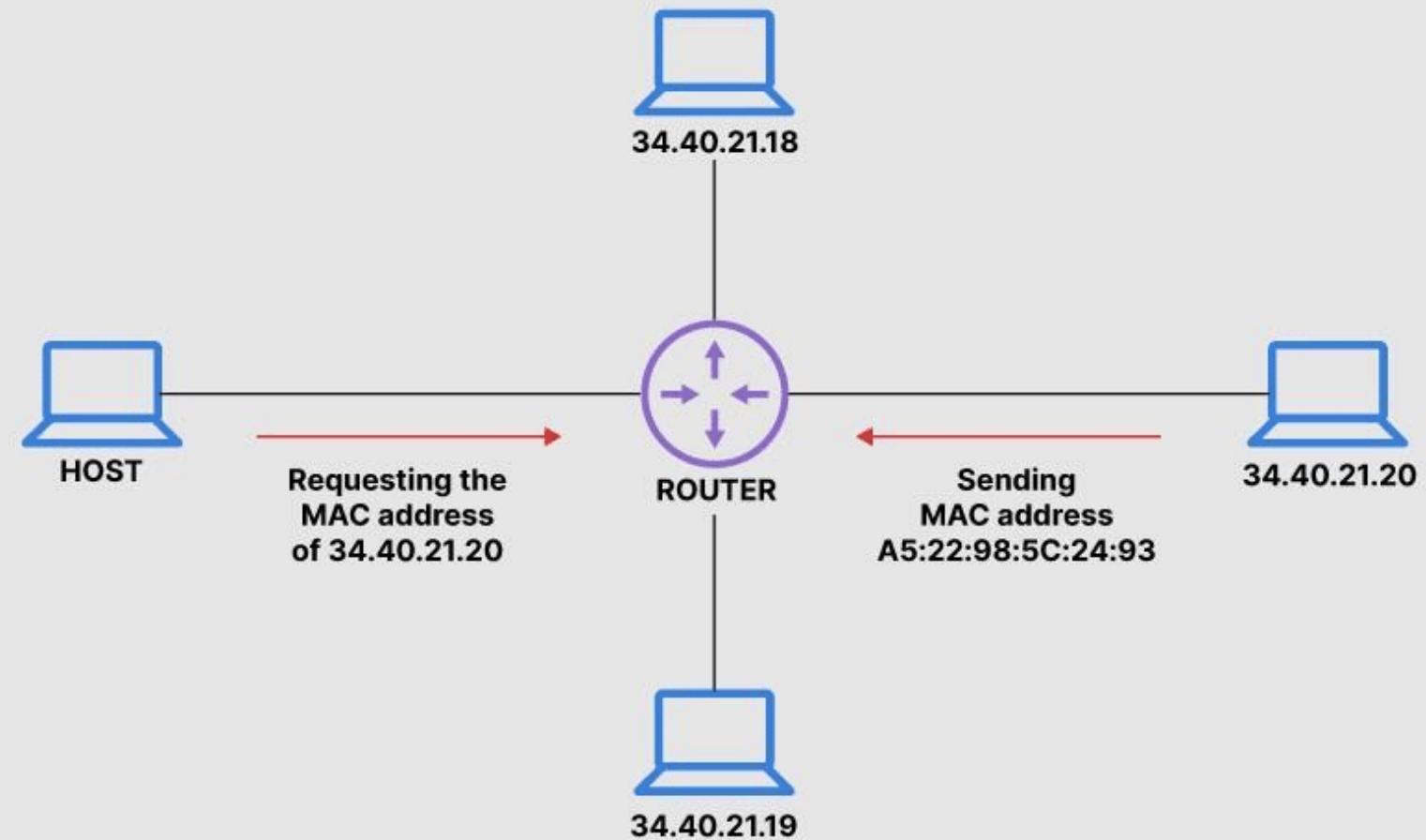
- Cos'è il protocollo ARP.
- Cosa sono gli attacchi MITM.
- Cos'è l'attacco ARP-Poisoning.
- Le fasi dell'attacco.

# COS'È IL MODELLO ARP?

E' un protocollo di rete utilizzato per associare un indirizzo IP a un indirizzo fisico o MAC (Media Access Control) di un dispositivo all'interno di una rete locale.

Quando un dispositivo su una rete vuole comunicare con un altro dispositivo, utilizza l'indirizzo IP di destinazione. Per inviare effettivamente i dati, deve conoscere anche l'indirizzo MAC del dispositivo di destinazione. Il protocollo ARP viene utilizzato per mappare gli indirizzi IP agli indirizzi MAC nella stessa rete locale.

## How Address Resolution Protocol (ARP) Works



# COSA SONO GLI ATTACCHI MITM?



- Un attacco Man-in-the-Middle (MITM) è un tipo di attacco informatico in cui un aggressore inserisce se stesso o i propri dispositivi tra le comunicazioni di due parti legittime.

L'obiettivo principale di un attacco MITM è intercettare, alterare o manipolare la comunicazione tra le due parti senza che loro ne siano consapevoli.

Alcuni esempi di scenari in cui può verificarsi un attacco MITM includono:

- Intercezione delle comunicazioni Wi-Fi
- Interposizione tra un utente e un sito web
- Attacchi su reti cablate
- Attacchi su reti cellulari

# CHE COS'È UN ARP POISONING?

---

- ARP Poisoning, o ARP Spoofing, è una tecnica utilizzata in attacchi Man-in-the-Middle (MITM) per intercettare o manipolare il traffico di rete.

In un attacco ARP Poisoning, un attaccante invia falsi pacchetti ARP alla rete, fornendo informazioni ARP erronee agli altri dispositivi nella stessa rete. Questa manipolazione ARP può avere diverse finalità, inclusa l'intercettazione del traffico di rete o la reindirizzazione del traffico attraverso il dispositivo dell'attaccante.



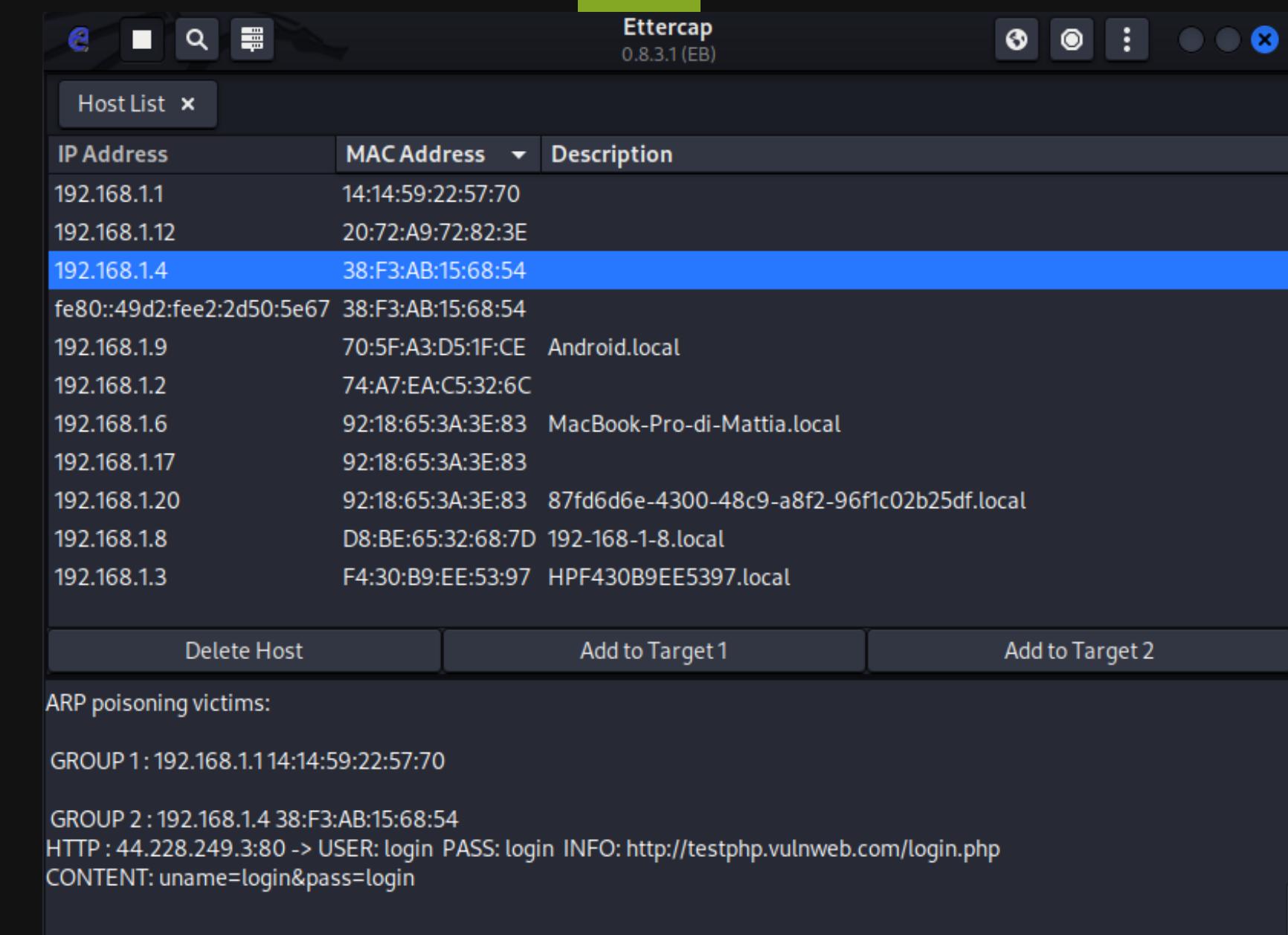
# LE FASI DI ATTACCO

01

Apriamo Ettercap e attiviamolo, dopodichè lo utilizziamo attraverso la funzione scan per ottenere gli IP dei vari HOST presenti sulla rete interna.

02

Selezioniamo i due target, in questo caso il nostro **Target 1** era il nostro IP gateway ed il **Target 2** era l'IP del nostro PC. Avviamo l'Arp poisoning.



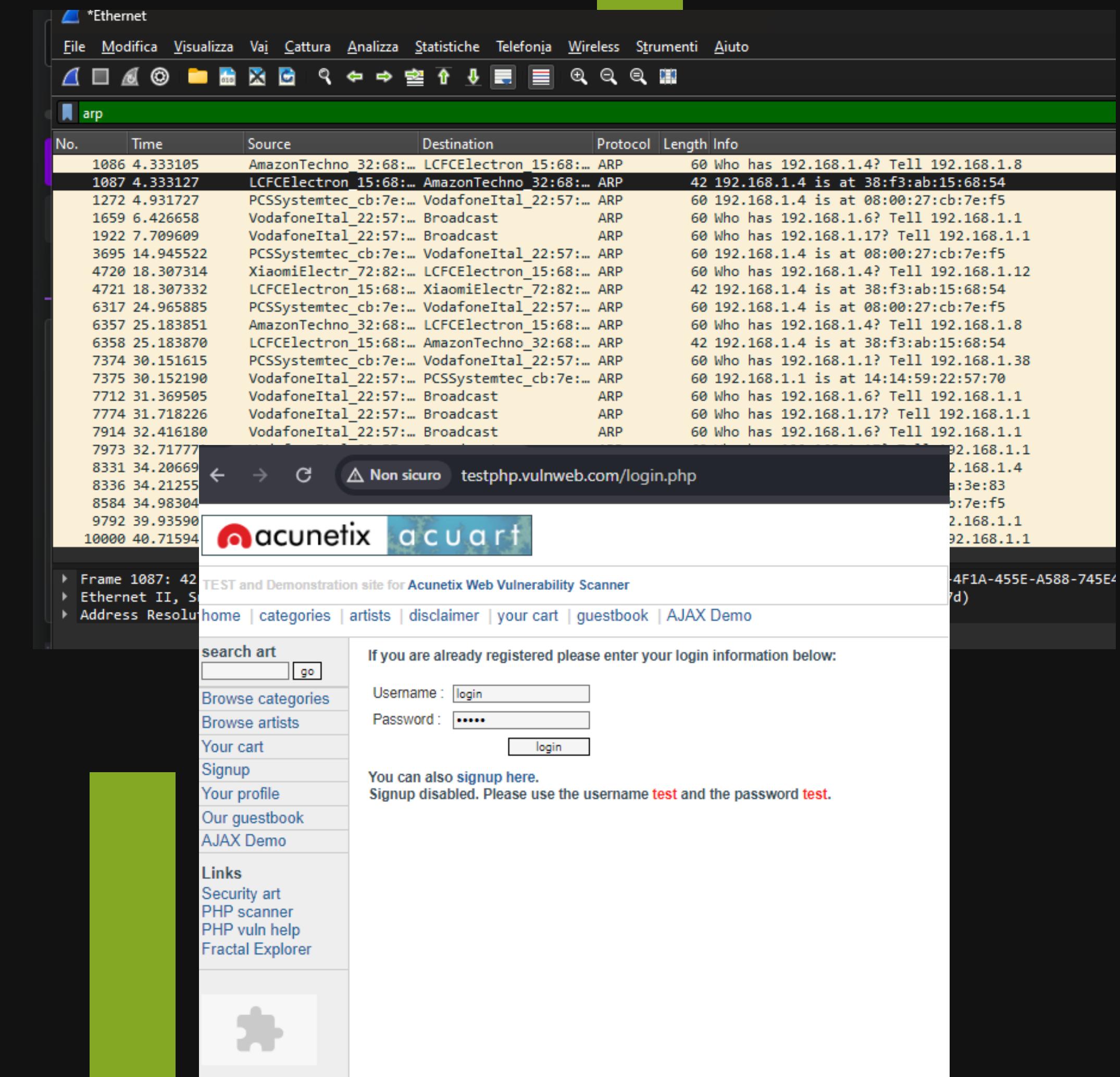
# LE FASI DI ATTACCO

03

Una volta attivato Ettercap, apriamo sul nostro computer il programma WIRESHARK per tenere d'occhio il flusso del protocollo Arp sulla nostra rete.

04

Apriamo una pagina web, in questo caso viene utilizzata la pagina di Vulnweb al fine di scopi didattici, effettuiamo il login sulla pagina Profilo.



# LE FASI DI ATTACCO

04

Una volta effettuato l'accesso, torniamo su Ettercap e potremo notare che il software avrà intercettato USERNAME(login) e PASSWORD(login) del profilo utente.

05

Da WIRESHARK possiamo notare che l'arp poisoning è andato a buon fine in quanto rileverà una duplicazione dell'indirizzo IP.

06

