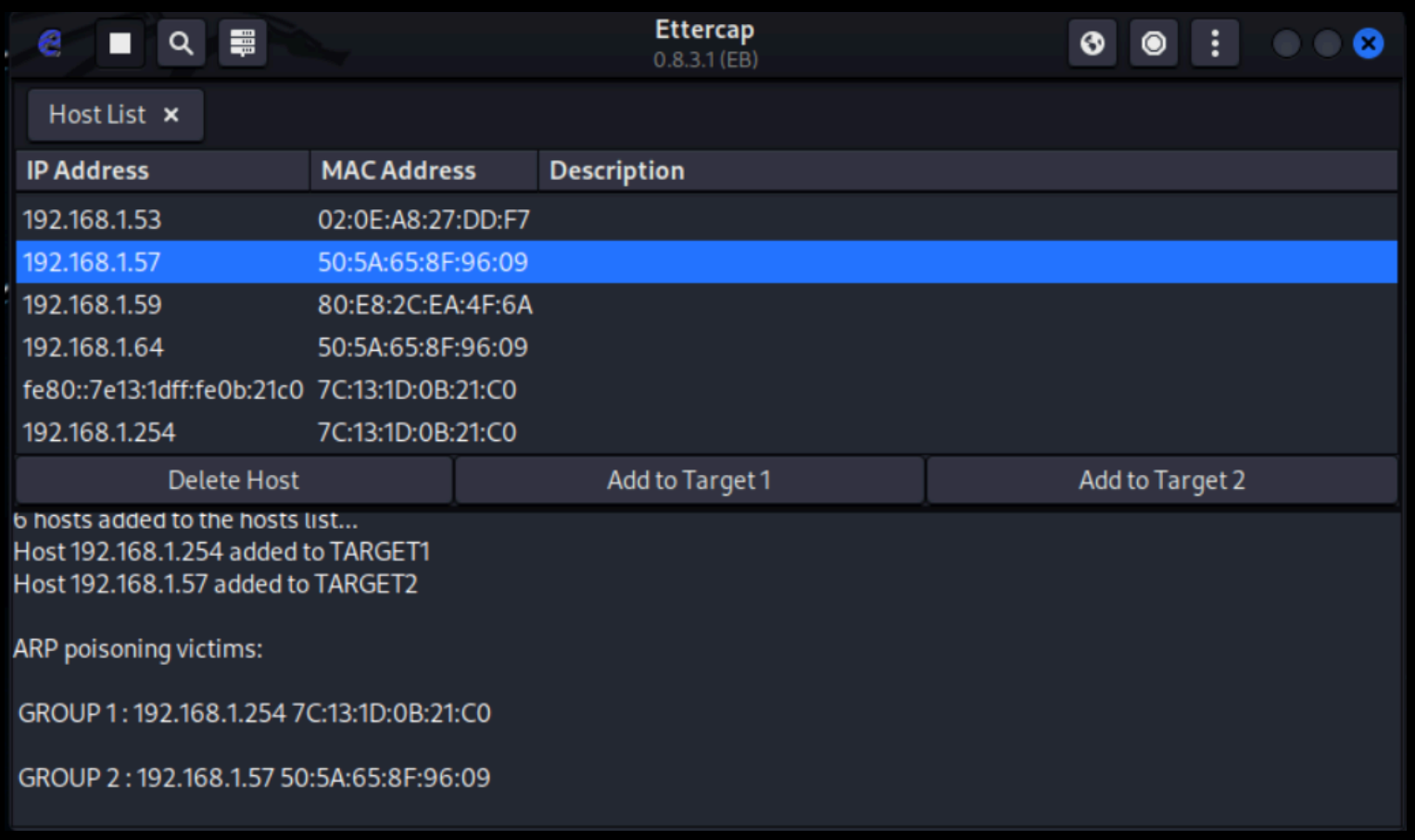
Ettercap

Ettercap si tratta di un programma capace di intercettare il traffico di rete, utilizzato per gli attacchi di tipo “MitM” (Man in the Middle).
Può essere usato per vari scopi, come:

ARP poisoning: Avvelenamento del protocollo ARP, questo attacco permette di alterare o metaforicamente “avvelenare” le tabelle ARP di dispositivi all’interno di una rete LAN, facendo si che il traffico di rete destinato a un certo dispositivo venga inviato all’attaccante invece che al destinatario reale. Questo permette di intercettare informazioni sensibili come credenziali di login.

Le fasi dell’attacco:
1. **Scansione della rete:** Si inizia eseguendo una scansione della rete per indentificare i dispositivi connessi e i loro indirizzi IP e MAC.
2. **Selezione del target:** Si scelgono di dispositivi target, tipicamente si include un gateway e un dispositivo host connesso ad esso.
3. **Avvio ARP Poisoning:** Qui ettercap si finge il gateway per l’host e viceversa, dicendo essenzialmente che il MAC address dell’altro dispositivo è quello dell’attaccante.
4. **Intercezione del traffico:** una volta che i dispositivi sono stati ingannati, iniziano a inviare il traffico destinato l’uno all’altro all’attaccante. Qui il MitM può leggere, registrare o modificare questo traffico.
5. **Reindirizzamento del traffico:** Per non destare sospetti, l’attaccante reindirizza il traffico al destinatario previsto e, se necessario, modificato.

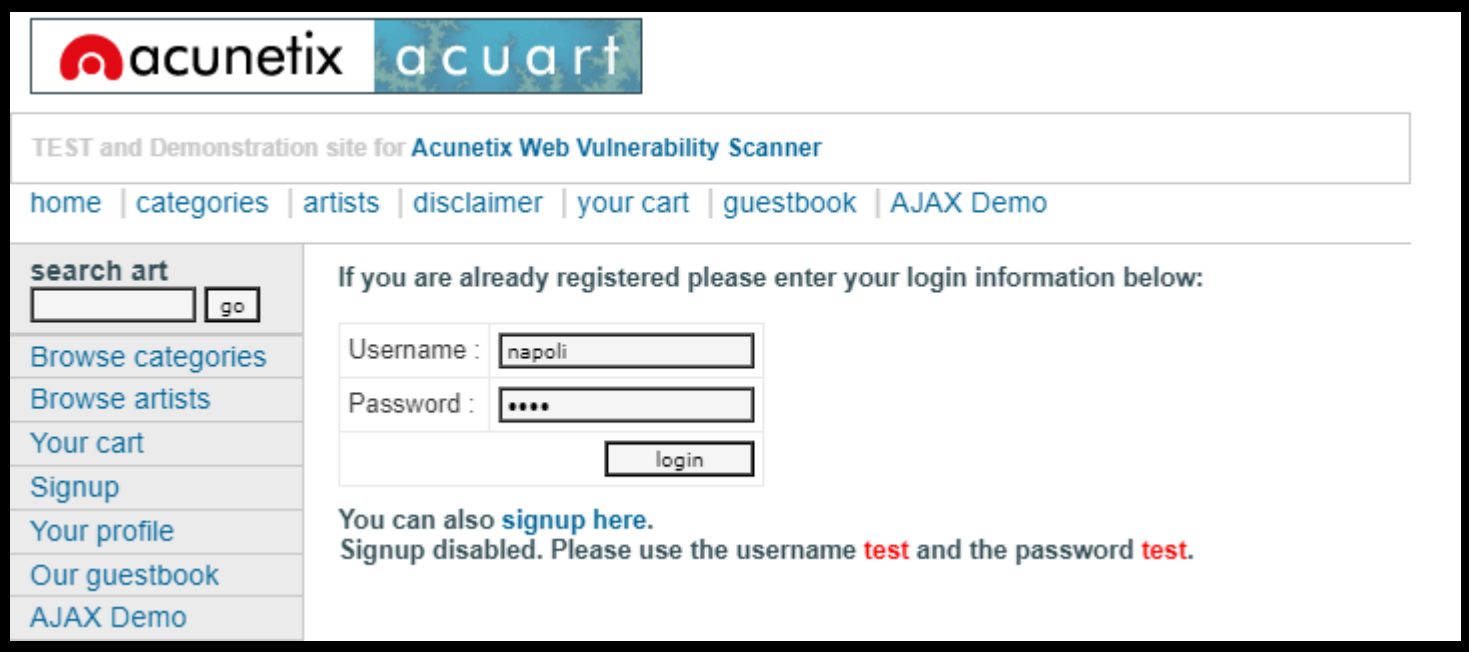
Vediamo un esempio pratico utilizzando Ettercap:



Dopo aver effettuato la scansione degli host all'interno della rete, scegliamo 2 target di riferimento per eseguire il test, in questo caso l'address IP e MAC del gateway e quello dell'host di riferimento.

Una volta avviato l'attacco, verifichiamo l'effettiva efficacia tramite la pagina vulnweb, una pagina volutamente vulnerabile.

Procediamo provando a inserire le credenziali nella sezione login:



Adesso verifichiamo che siano state trasmesse in chiaro e intercettate da Ettercap:

```
GROUP 1 : 192.168.1.59 80:E8:2C:EA:4F:6A

GROUP 2 : 192.168.1.254 7C:13:1D:0B:21:C0
HTTP : 44.228.249.3:80 -> USER: napoli  PASS: roma  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=napoli&pass=roma
```

Come si può osservare, l'attacco di ARP poisoning è stato un successo.

Protocollo ARP: Address Resolution Protocol, viene utilizzato per associare un indirizzo IP a un indirizzo MAC. Questo processo è fondamentale per il trasferimento dei dati fisico all'interno di una rete locale.

MitM: Man in the middle è un tipo di attacco in cui un eventuale attaccante si inserisce nella comunicazione tra due parti (come un utente e un sito web). Con questo tipo di attacco si riesce ad intercettare, leggere e potenzialmente modificare i dati scambiati.