**Traccia:** Utilizzando Ettercap andiamo a simulare un attacco ARP-Poisoning

Fare un report su:

● Cos’è il protocollo ARP:

Il Protocollo ARP (Address Resolution Protocol) è un protocollo di rete utilizzato per mappare un indirizzo IP (Internet Protocol) a un indirizzo fisico di livello di collegamento (come un indirizzo MAC in una rete Ethernet).

Nella rete informatica, quando un dispositivo vuole inviare dati a un altro dispositivo, ma conosce solo il suo indirizzo IP e non il suo indirizzo fisico, utilizza il Protocollo ARP. Funziona così: il dispositivo invia una richiesta ARP per scoprire l'indirizzo fisico associato a un determinato indirizzo IP; il dispositivo destinatario risponde con il suo indirizzo fisico, e ora i due dispositivi possono comunicare tra loro sulla rete.

In breve, ARP aiuta i dispositivi a trovare gli "indirizzi" corrispondenti nella rete.

● Cosa sono gli attacchi MITM:

Un attacco "Man-in-the-Middle" (MitM) è una forma di attacco informatico in cui un attaccante si colloca tra due parti in comunicazione, intercettando o manipolando il flusso di informazioni tra di esse. L'obiettivo principale di un attacco MitM è intercettare, alterare o iniettare dati nella comunicazione tra le due parti, senza che esse se ne accorgano.

I rischi associati a un attacco MITM sono significativi e includono la compromissione della riservatezza dei dati, la possibilità di furto di informazioni sensibili come le credenziali di accesso, l'intercettazione e la manipolazione dei dati in transito e la potenziale infiltrazione di malware nei dispositivi coinvolti nella comunicazione.

L'utilizzo di reti virtuali private (VPN) e protocolli di sicurezza come HTTPS può contribuire a mitigare i rischi associati agli attacchi MitM.

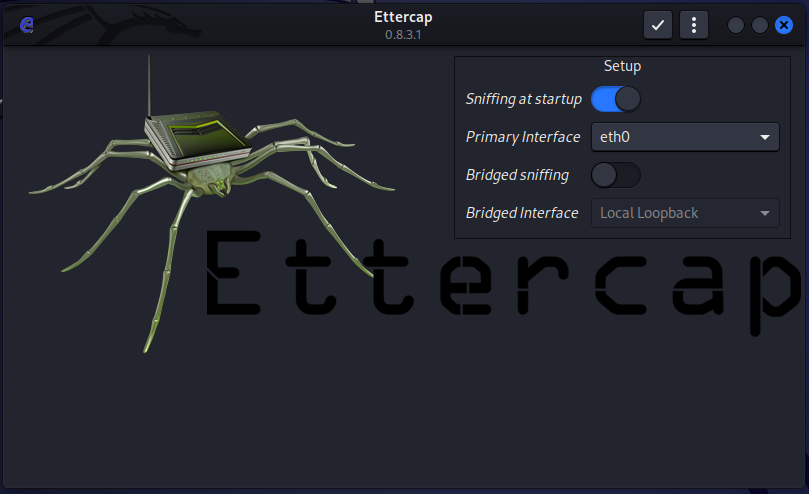
● Cos’è l'attacco ARP-Poisoning:

"ARP poisoning," anche noto come "ARP spoofing," è una tecnica utilizzata negli attacchi Man-in-the-Middle (MitM) per intercettare il traffico di rete tra due dispositivi.

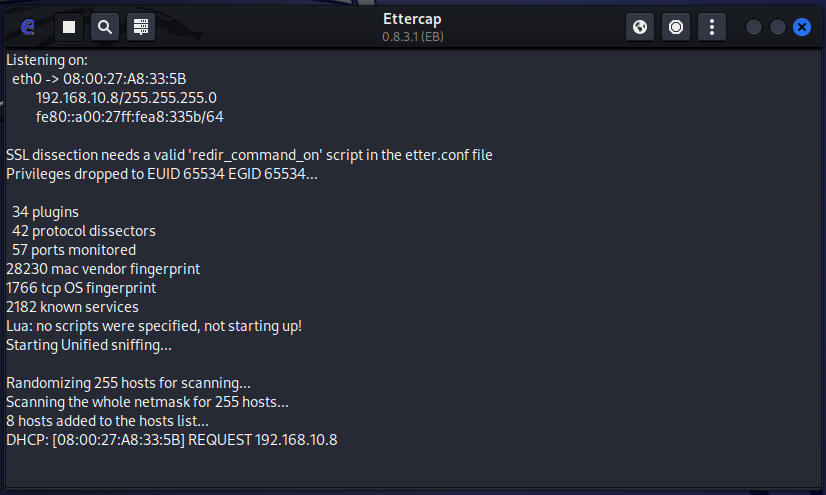
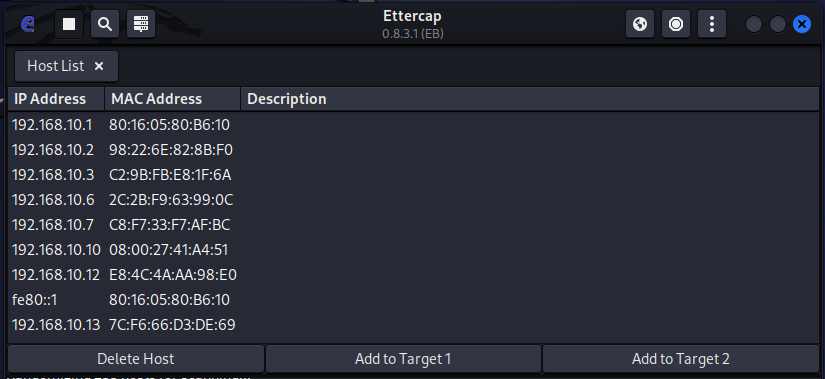
Questa tecnica sfrutta il protocollo ARP (Address Resolution Protocol) per inviare informazioni false in modo che il traffico destinato a un determinato indirizzo MAC venga deviato verso l'attaccante anziché verso il destinatario previsto.

● Le fasi dell'attacco:

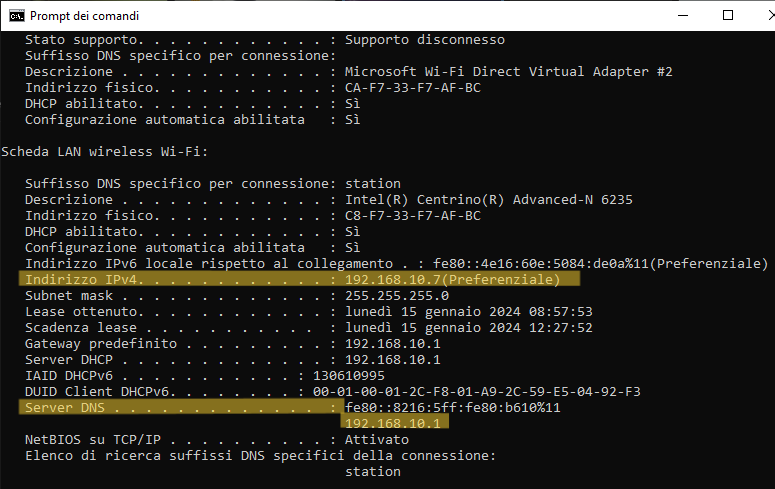
**Ettercap** è uno strumento di analisi di rete e attacco di tipo Man-in-the-Middle (MitM) open-source. È progettato per intercettare, analizzare e manipolare il traffico di rete in tempo reale all'interno di una rete locale. Esso supporta una varietà di funzioni, tra cui l'ARP poisoning, Utilizziamolo per analizzare le fasi dell’ARP spoofing:



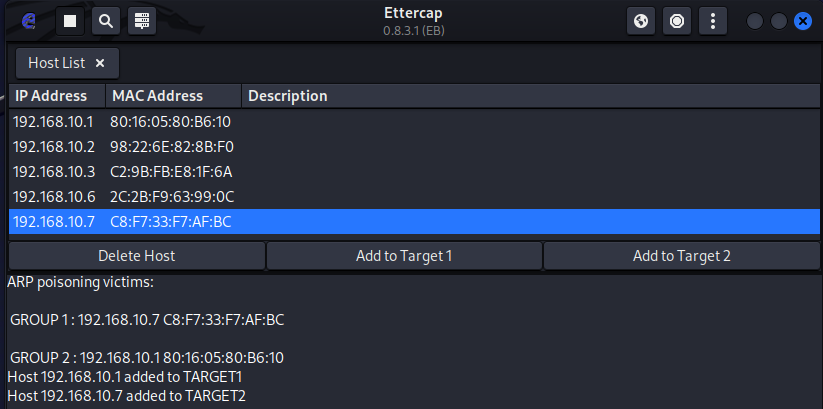
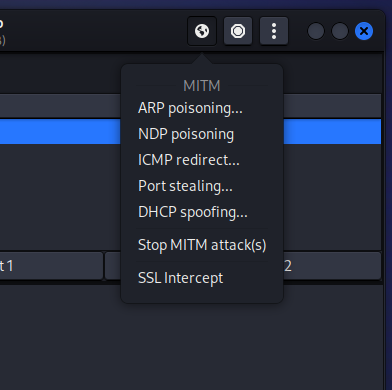
Una volta aperto il programma la prima fase prevede la scannerizzazione degli host e la conseguente visualizzazione della lista degli host trovati:

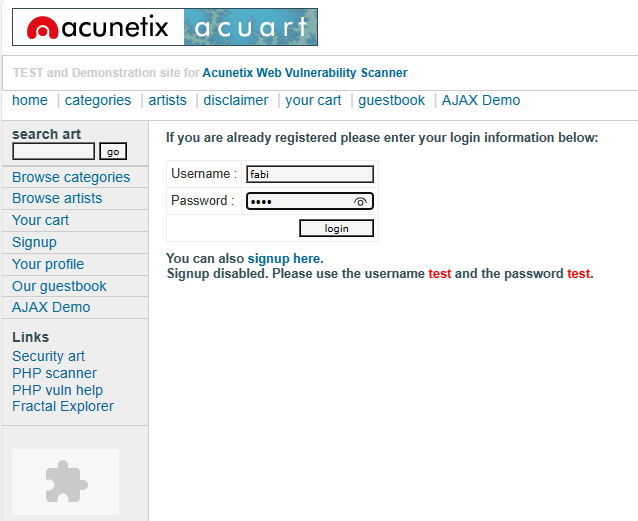
Aprendo il prompt dei comandi del nostro dispositivo possiamo confrontare il nostro indirizzo IPv4 e l’indirizzo del nostro router gateway con la lista host risultante dalla scannerizzazione di Ettercap:



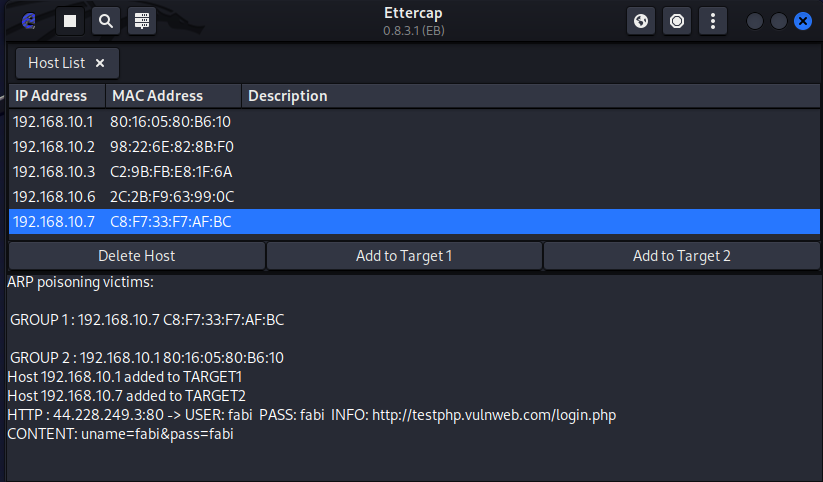
Una volta identificati possiamo impostare i target 🡪 Target1 : impostiamo router gateway, Target2: impostiamo IPv4 e avviamo lo spoofing:

Per testare gli effetti dello spoofing inseriamo user e password su vulnweb, nel mio caso ho utilizzato **user: fabi e pass: fabi**:

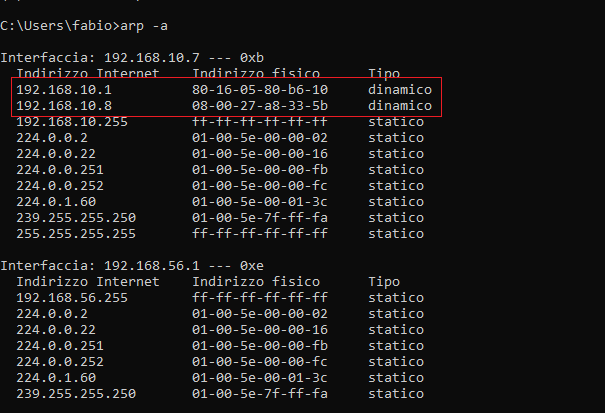
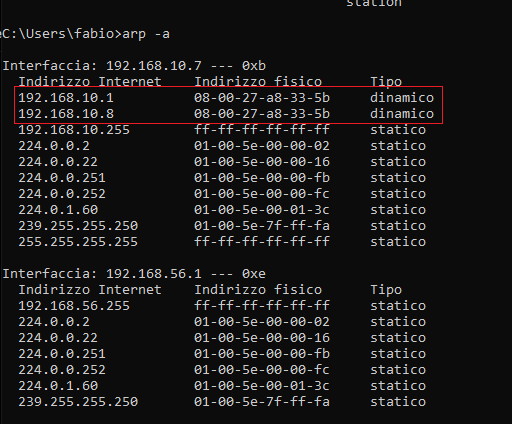


Controllando su Ettercap possiamo vedere come sia stato individuato il sito utilizzato e le credenziali inserite:



Un ulteriore verifica dell’avvenuto spoofing si può constatare confrontando il comando **arp -a** nel prompt dei comandi del nostro dispositivo, prima e dopo l’attacco.

Da tale confronto possiamo notare come l’indirizzo MAC del nostro router sembri clonato:

In un attacco ARP spoofing, l'attaccante invia informazioni ARP false alla rete, associando il suo indirizzo MAC all'indirizzo IP della vittima o di un'altra macchina nella rete. Ciò può causare diversi effetti, tra cui la percezione di un indirizzo MAC "clonato" sul dispositivo attaccato.