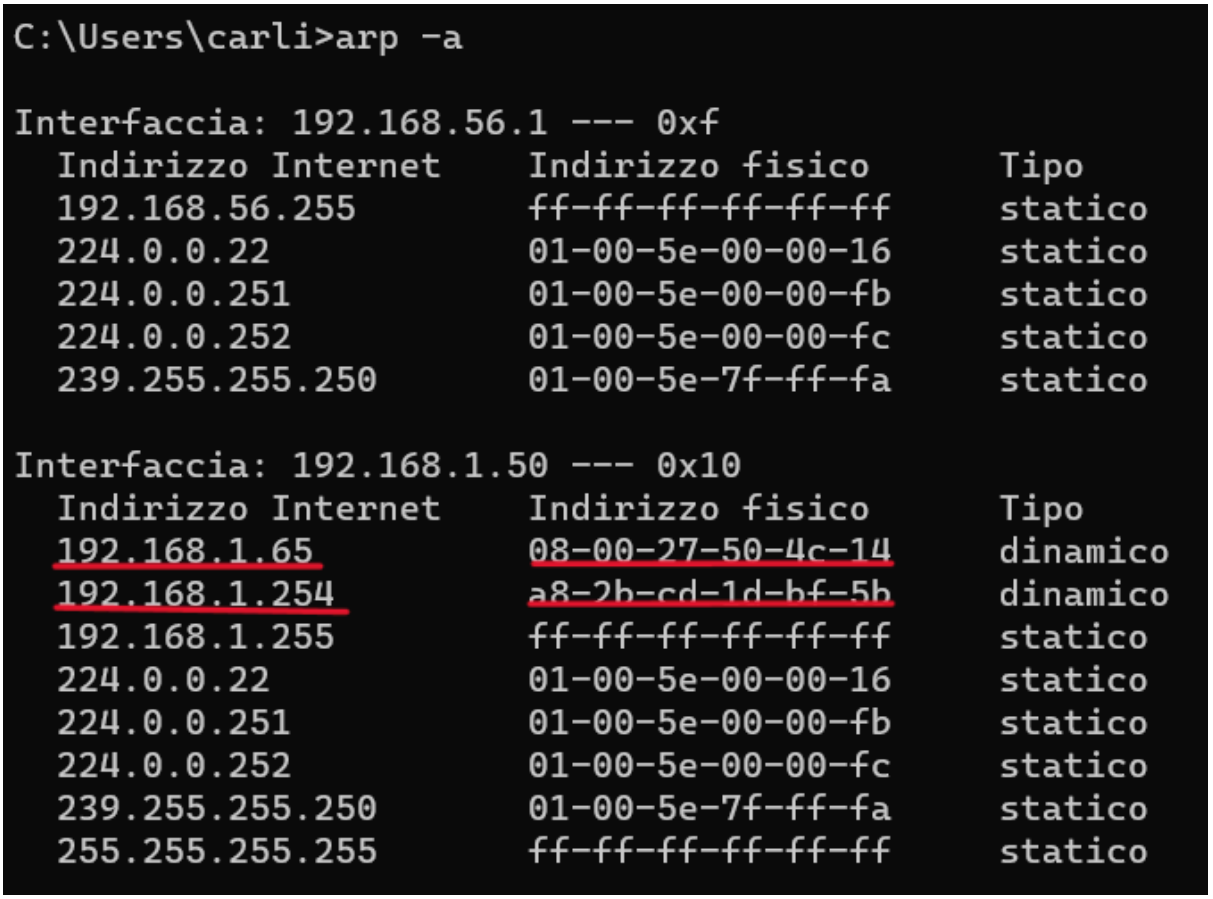
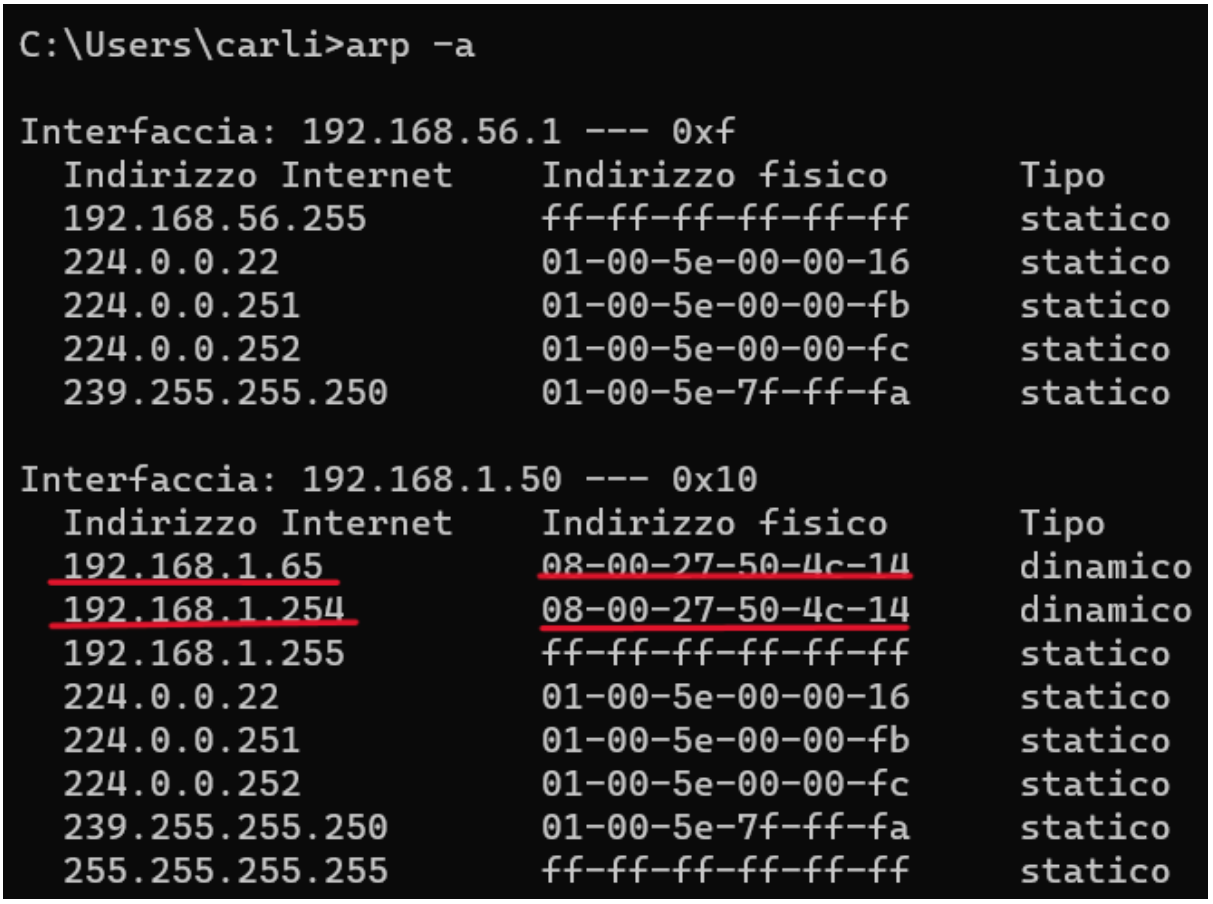
Nell’esercizio di oggi andremo ad eseguire un attacco di ARP poisoning con l’aiuto di un ettercap, un software open source di analisi di rete.
Il protocollo ARP (Address Resolution Protocol) è un protocollo di livello 2 (data link) che traduce gli indirizzi IP in MAC address. Questo protocollo funziona tramite una tabella in cui sono salvate le corrispondenze IP-MAC della propria rete. L’host invierà in broadcast una richiesta ARP con l’indirizzo del destinatario, il quale risponderà con il proprio MAC address.
È possibile alterare le tabelle ARP tramite un attacco ARP poisoning. Questo è un tipo di attacco man in the middle, cioè un attacco informatico che permette di intercettare e manipolare la comunicazione fra due entità, sostituendosi ad una di esse.

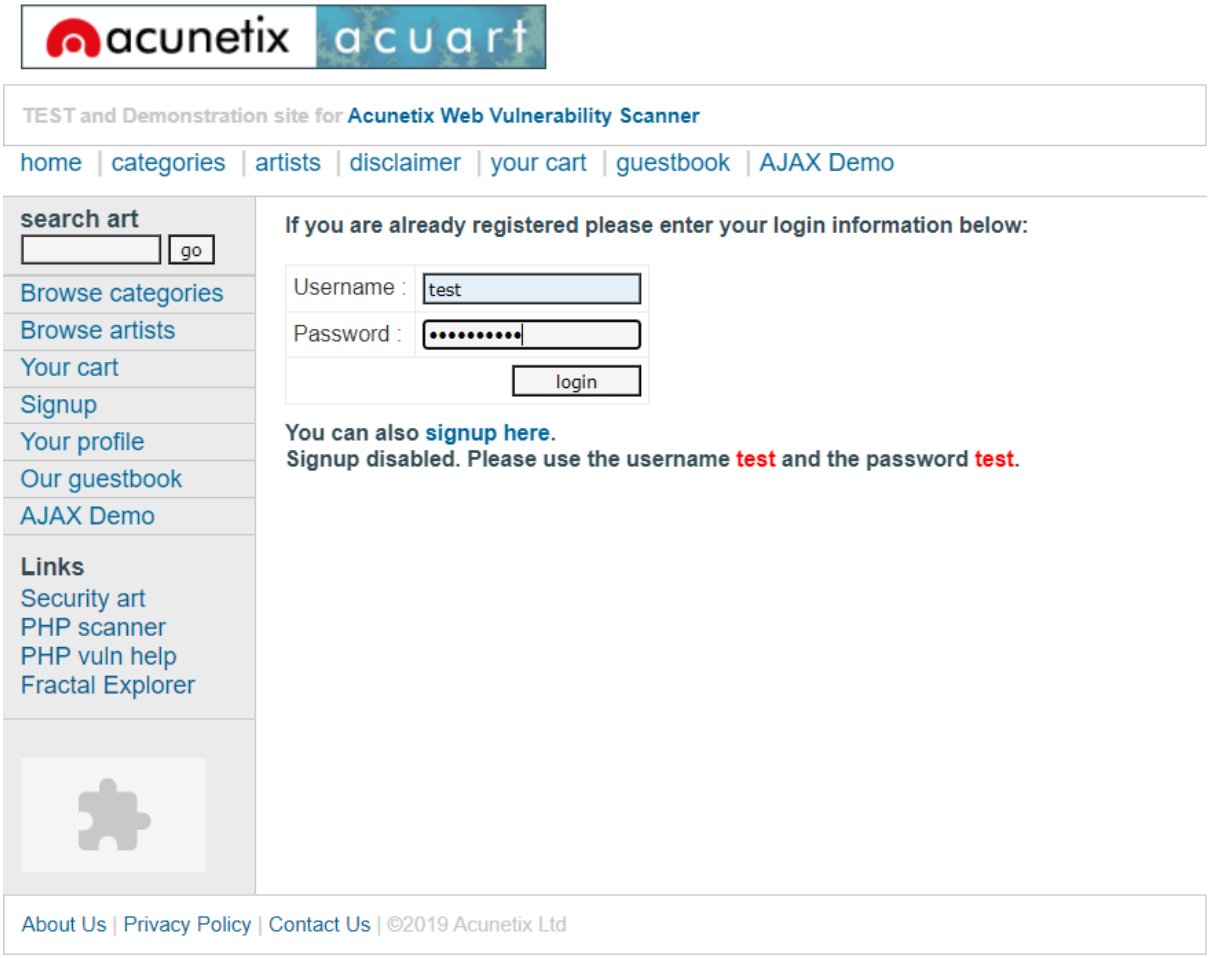


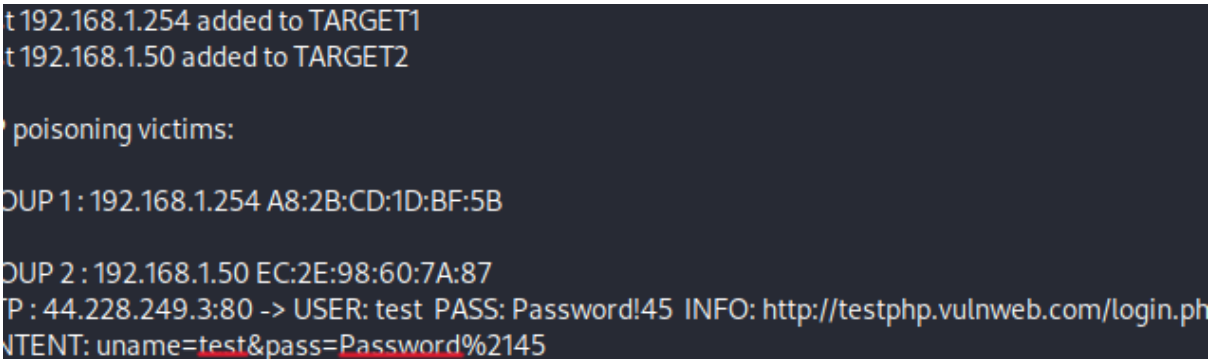
Andiamo a vedere le fasi dell’attacco.
Inizialmente possiamo vedere, nell’immagine qui sopra, che nella tabella ARP non ci sono anomalie. In questa prima fase, in cui non siamo stati ancora colpiti, l’attaccante sta impostando i target e sta creando le informazioni da iniettare nella nostra tabella ARP.



Nella seconda fase parte l’attacco e, come possiamo vedere nell'immagine sopra, la cache ARP viene modificata. A questo punto tutto il traffico passante per il default gateway sarà intercettato dall'attaccante. Questo definisce la terza fase.

Proviamo a vedere cosa succede se effettuiamo l’accesso ad un sito non criptato.





Come possiamo vedere le credenziali di accesso non criptate sono state intercettate.