SIMULAZIONE ATTACCO ETTERCAP

Protocollo ARP

- Il protocollo ARP(Address Resolution Protocol) e un protocollo utilizzato nelle reti per assegnare indirizzi IP a indirizzi MAC all'interno di una rete locale.
  In pratica ARP aiuta a tradurre gli indirizzi IP in indirizzi MAC in una rete locale.

Attacchi MITM

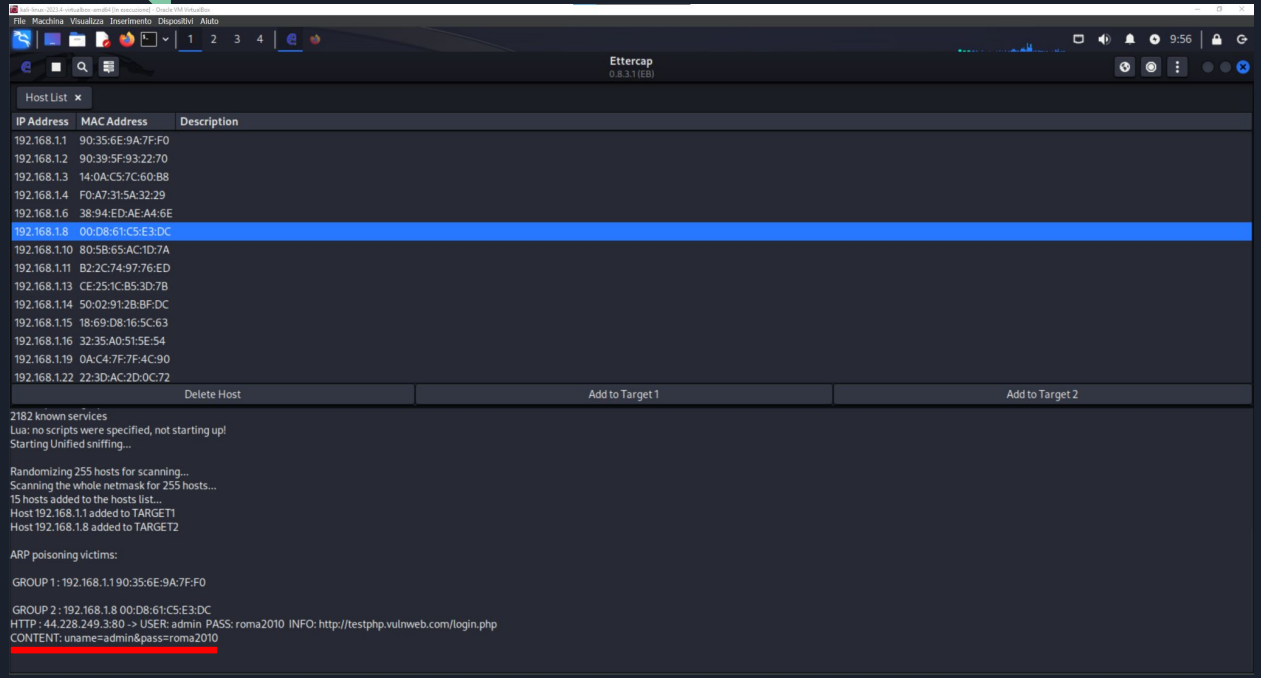
- Gli attacchi MITM(Man in the Middle) sono attacchi informatici in cui l'attaccante si posiziona tra due "parti" comunicanti, intercettando o manipolando la comunicazione tra di esse. Questo attacco può avvenire sia su rete wireless che cablate.

Attacco ARP-Poisoning

- L'attacco ARP-Poisoning e una forma di attacco MITM che sfrutta il protocollo ARP. L’attaccante invia pacchetti ARP falsificati nella rete locale, convincendo le macchine a associare il suo indirizzo MAC a un indirizzo IP legittimo.
  Questo consente all’attaccante di intercettare, modificare o inoltrare il traffico di rete tra le vittime senza il loro consenso.

Fasi Attacco

1. SCELTA DEGLI OBIETTIVI: Identifica delle macchine nella rete locale da attaccare.
2. INVIO DI PACCHETTI ARP FALSIFICATI: L'attaccante invia pacchetti ARP contenenti informazioni di mappatura falsificate alle vittime.
3. INTERCETTAZIONE DEL TRAFFICO: L'attaccante può intercettare o manipolare il traffico della vittima.
4. MANTENIMENTO : L'attaccante invia periodicamente pacchetti ARP falsificati per mantenere l'associazione del indirizzo IP/MAC.



Simulazione usando VulnWeb.
Come possiamo vedere siamo riusciti a intercettare i dati di login.