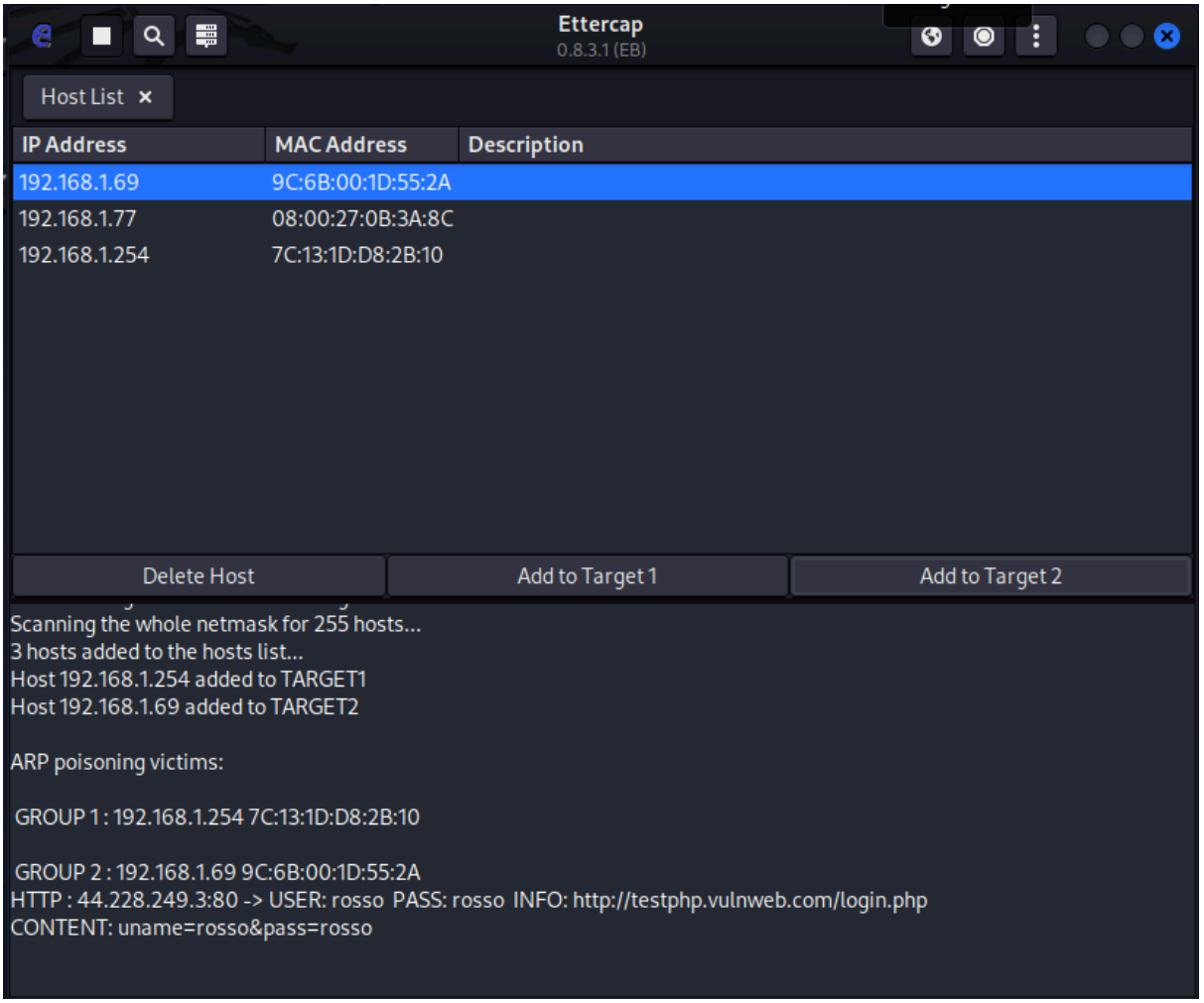
ARP POISONING

Effettuiamo un attacco alla pagina vulnweb tramite Ettercap e come possiamo vedere intercettiamo le credenziali di accesso



Cos’è il protocollo ARP?

Il protocollo ARP, acronimo di Address Resolution Protocol, è un protocollo di rete utilizzato per associare un indirizzo di livello di collegamento (come un indirizzo MAC) a un indirizzo di rete (come un indirizzo IP). In breve, il suo scopo principale è quello di mappare gli indirizzi IP a quelli MAC all'interno di una rete locale.

Quando un dispositivo all'interno di una rete deve comunicare con un altro dispositivo nella stessa rete, utilizza l'indirizzo IP di destinazione. Tuttavia, per inviare effettivamente i dati al dispositivo di destinazione, è necessario conoscere il suo indirizzo MAC. In questo contesto, il protocollo ARP entra in gioco.

Il funzionamento di base del protocollo ARP coinvolge la trasmissione di un pacchetto ARP da parte di un dispositivo che richiede la corrispondenza tra un indirizzo IP e un indirizzo MAC. Gli altri dispositivi nella rete ricevono questo pacchetto e, se l'indirizzo IP cercato è nella stessa rete, il dispositivo corrispondente risponde con il suo indirizzo MAC.

Una volta ottenuta la corrispondenza, il mittente può utilizzare l'indirizzo MAC per indirizzare direttamente i pacchetti al dispositivo di destinazione nella stessa rete locale. Il protocollo ARP è fondamentale per il funzionamento delle reti locali (LAN) e contribuisce a garantire che i dati vengano inviati correttamente tra i dispositivi all'interno della stessa rete.

Cosa sono gli attacchi MITM?

Un attacco Man-in-the-Middle (MITM) è una forma di attacco informatico in cui un attaccante si posiziona tra le comunicazioni tra due parti legittime. L'obiettivo principale di un attacco MITM è intercettare, alterare o manipolare il flusso di informazioni tra le parti coinvolte senza che loro se ne accorgano.

Per proteggersi dagli attacchi MITM, è importante utilizzare connessioni sicure, come HTTPS per le comunicazioni web, e adottare misure di sicurezza aggiuntive come l'autenticazione a due fattori. Inoltre, è essenziale essere consapevoli delle minacce potenziali e monitorare attentamente il traffico di rete per individuare comportamenti sospetti.

Cos'è l'attacco ARP-Poisoning?

L'attacco ARP poisoning, noto anche come ARP spoofing, è una tecnica di attacco informatico che sfrutta il protocollo ARP (Address Resolution Protocol) all'interno di una rete locale. In breve, questo attacco coinvolge la manipolazione delle tabelle ARP sui dispositivi di una rete per associare indirizzi IP legittimi a indirizzi MAC (Media Access Control) falsificati. Questo consente all'attaccante di intercettare o manipolare il flusso di dati all'interno della rete.

Gli attacchi ARP poisoning possono essere utilizzati per condurre attacchi di tipo "Man-in-the-Middle" (MITM), dove l'attaccante può intercettare, modificare o iniettare dati nelle comunicazioni tra due parti legittime senza il loro consenso. Per mitigare questo tipo di attacco, le reti possono implementare tecniche di sicurezza, come la firma ARP, l'uso di VLAN (Virtual Local Area Network) e monitoraggio attivo per rilevare anomalie nelle tabelle ARP.