Utilizzando Ettercap andiamo a simulare un attacco ARP-Poisoning. La macchina web vittima è a piacere, in alternativa si può usare: vulnweb. http://testphp.vulnweb.com/login.php

Fare un report su:
- Cos'è il protocollo ARP.
- Cosa sono gli attacchi MITM.
- Cos'è l'attacco ARP-Poisoning.
- Le fasi dell'attacco.

COS'È IL PROTOCOLLO ARP

L'ARP (Address Resolution Protocol) è un protocollo che collega un indirizzo IP (Internet Protocol) in continua evoluzione a un indirizzo fisso del computer fisico, noto anche come indirizzo MAC (Media Access Control). Il protocollo ARP è fondamentale nelle reti locali (LAN) e consente ai dispositivi di comunicare tra loro utilizzando gli indirizzi MAC, che sono specifici per ciascuna scheda di rete.

COSA SONO GLI ATTACCHI MITM

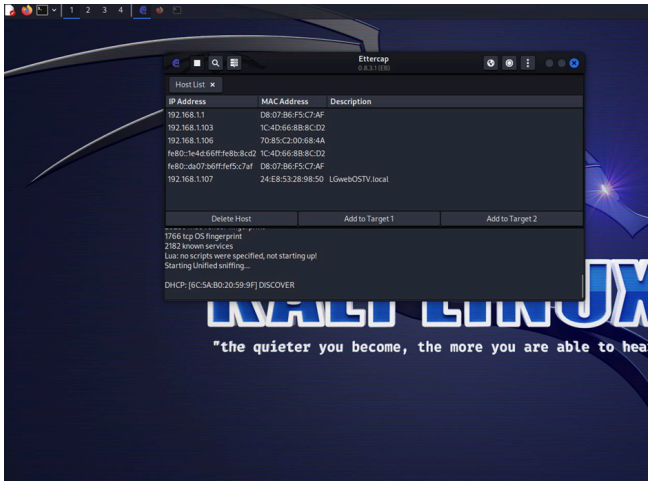
Gli attacchi Man-in-the-Middle (MITM) sono tipologie di attacchi informatici in cui un eventuale hacker si inserisce tra due parti che stanno cercando di comunicare e intercetta o manipola la comunicazione tra di esse. L'obiettivo principale di un attacco MITM è intercettare, alterare o iniettare dati durante la trasmissione tra le due parti senza che queste ultime ne siano consapevoli.

COS'È L'ATTACCO ARP-POISONING

ARP Poisoning, è una tecnica di attacco Man-in-the-Middle in cui un aggressore invia pacchetti ARP falsificati (Address Resolution Protocol) in una rete locale. Questo tipo di attacco è finalizzato a manipolare la tabella ARP di un dispositivo di destinazione, causando la connessione di quest'ultimo attraverso l'attaccante anziché attraverso il gateway predefinito.

LE FASI DELL'ATTACCO

- ***Identificare le macchine da attaccare sulla rete:*** Questo può essere fatto attraverso la scansione di pacchetti di rete o l'uso di altri mezzi per individuare gli indirizzi IP e MAC delle macchine target.

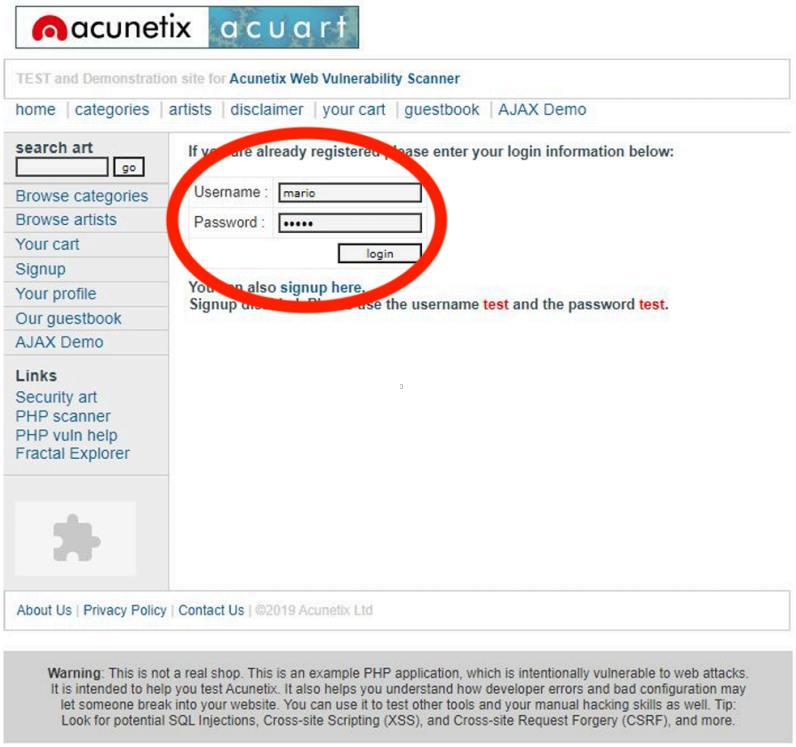


- ***Invio di pacchetti ARP falsificati:*** Una volta che l'attaccante ha identificato le macchine target, invia pacchetti ARP falsificati alla rete. Questi pacchetti ARP contengono informazioni contraffatte associando l'indirizzo IP della vittima all'indirizzo MAC dell'attaccante.

- ***Aggiornamento delle tabelle ARP:*** Le macchine nella rete ricevono questi pacchetti ARP falsificati e aggiornano le proprie tabelle ARP con le informazioni contraffatte fornite dall'attaccante.

- ***Reindirizzamento del traffico:*** Con le tabelle ARP alterate, il traffico destinato alla vittima viene inviato all'indirizzo MAC dell'attaccante invece che al legittimo destinatario. L'attaccante può quindi intercettare, manipolare o iniettare dati nella comunicazione tra la vittima e il suo gateway o altri destinatari.

Fig.1



Es: come possiamo vedere dall'esempio nelle figure a lato, i dati utilizzati per il login sul sito (fig.1) vengono intercettati su ettercap mediante attacco di ARP poisoning (fig.2)

Fig.2