EPICODE

Esercizio S6 – L1

TRACCIA

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.

SOLUZIONE

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Si è proceduto con Ettercap nella scansione degli host e nell’apertura della lista degli host scansionati. Successivamente si sono scelti i due target in cui effettuare l’attacco Man in the Middle (MITM). In questo caso si è scelto il gateway della rete e Windows 7 dentro Virtualbox.

Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente

Si sono poi inseriti i dati per il login da Windows 7.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Qui è possibile vedere la buona riuscita dell’attacco MITM con la comparsa dei dati login.

Immagine che contiene testo, schermata, schermo, software

Descrizione generata automaticamente

Qui è invece possibile notare che l’indirizzo MAC di Kali da cui si è effettuato l’attacco è uguale a quello del gateway.

Immagine che contiene testo, schermata, software, Carattere

Descrizione generata automaticamente

Con Wireshark è possibile notare la sovrapposizione evidenziata in giallo direttamente da Wireshark.

Report:

* Il protocollo ARP è colui che permette il collegamento di un indirizzo ip con un indirizzo MAC (indirizzo fisico) di un host. Livello 2 ISO/OSI.
* Gli attacchi MITM sono attacchi in cui l’attaccante si inserisce in mezzo alla comunicazione, come visto in questo esercizio.
* L’attacco ARP-Poisoning è un tipo di attacco MITM che utilizza il protocollo ARP. Per effettuarlo è necessario essere già connessi alla rete LAN della vittima.
* Le fasi dell’attacco sono:  
  1. Inserirsi nella rete LAN.

2. Seguire i passaggi effettuati in questo esercizio.