FASE EXPLOIT

PROTOCOLLO ARP

Protocollo che associa indirizzo IP MAC ad un indirizzo IP address, tramite una tabella definita ARP table.

ATTACCO MITM

Attacco “man in the middle”.

Tipologia di attacco informatico in cui l’attaccante si inserisce in una comunicazione e la controlla. La comunicazione potrà quindi subire DOSs e andare in down.
Ciò è molto pericoloso perchè le due parti della comunicazione sogno ignare dell’attaccante.

ARP POISONING

E’ la manipolazione della tabella di traduzione degli indirizzi IP nei pacchetti di rete.
Come esito si avrà che a due indirizzi IP address corrisponderà un IP MAC

ETTERCAP

Effettuo l’attacco MITM mediante il Tool di analisi di rete Ettercap con e il supporto di Wireshark e del prompt di comandi

- Applico una scansione degli host, e avrò l'elenco degli IP address e IP MAC della mia rete
- Aggiungo i due target che sono il mio PC e il mio router
- Avvio l' ARP poisoning affinchè l'IP MAC della macchina attaccante Linux sia lo stesso del router. (Gli IP address non cambiano).
- Nel prompt comandi col comando arp-a verifico

Host List ×

IP Address	MAC Address	Description
192.168.1.55	94:3A:91:31:A5:35	
192.168.1.56	50:8A:06:43:E2:14	
192.168.1.63	84:F3:EB:3D:A6:28	
192.168.1.73	34:6F:24:56:B5:69	
192.168.1.85	50:EB:F6:49:0A:1F	
192.168.1.101	08:00:27:AE:50:F1	
192.168.1.102	EC:6C:9A:94:61:E4	
fe80::1	A8:2B:CD:1B:96:D1	
fe80::fc28:303d:b49d:29bd	50:EB:F6:49:0A:1F	LAPTOP-6HDH8K0D.local
192.168.1.254	A8:2B:CD:1B:96:D1	

Delete Host | Add to Target 1 | Add to Target 2

GROUP 1 : 192.168.1.85 50:EB:F6:49:0A:1F

GROUP 2 : 192.168.1.254 A8:2B:CD:1B:96:D1
HTTP : 44.228.249.3:80 -> USER: 123 PASS: 1234 INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=123&pass=1234

```
C:\Users\salsa>arp -a

Interfaccia: 192.168.1.85 --- 0xe
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.1.56          50-8a-06-43-e2-14     dinamico
  192.168.1.96          08-00-27-cb-7e-f5     dinamico
  192.168.1.254         08-00-27-cb-7e-f5     dinamico
  192.168.1.255         ff-ff-ff-ff-ff-ff     statico
  224.0.0.22            01-00-5e-00-00-16     statico
  224.0.0.251           01-00-5e-00-00-fb     statico
  224.0.0.252           01-00-5e-00-00-fc     statico
  239.255.255.250       01-00-5e-7f-ff-fa     statico
  255.255.255.255       ff-ff-ff-ff-ff-ff     statico

Interfaccia: 192.168.56.1 --- 0x10
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.56.255        ff-ff-ff-ff-ff-ff     statico
  224.0.0.22            01-00-5e-00-00-16     statico
  224.0.0.251           01-00-5e-00-00-fb     statico
  224.0.0.252           01-00-5e-00-00-fc     statico
  239.255.255.250       01-00-5e-7f-ff-fa     statico
```