[CONSEGNA SETTIMANA 6 LEZIONE 1]

Attacchi alle web app - ARP Poisoning

Uno dei possibili attacchi *MITM* che si possono effettuare alle web app è l'***ARP poisoning***. Prima di proseguire con l'attacco spieghiamo cosa è il protocollo *ARP* e cosa sono gli attacchi *MITM* (man in the middle).

ARP è un protocollo di servizio usato in una rete che permette ad un host di recuperare l'indirizzo fisico *MAC* di un altro host a partire dal suo indirizzo *IP*, per poi inserirlo nella sua tabella *ARP*. Per fare ciò l'host di partenza invia in broadcast una richiesta di *ARP* (contenente il suo indirizzo *MAC* e l'indirizzo IP dell'host di cui vuole conoscere il *MAC*) che verrà indirizzata a tutti gli host della rete.

Per quanto riguarda gli attacchi **man in the middle** (o *MITM*), sono un particolare tipo di attacco dove il malintezionato si pone come intermediario tra due target (nel nostro caso specifico la macchina nativa e il modem), fingendosi la macchina nativa agli occhi del modem e viceversa, questo gli permette di ricevere le informazioni che i due target si scambiano.

Passiamo quindi all'attacco *ARP poisoning*.

La modalità di questo attacco si basa sulla modifica della tabella ARP dei target, infatti sfruttando alcuni software (nel nostro caso **ettercap**) è possibile tramite una ARP request andare a modificare, e quindi infettare (da qui il termine poisoning) la tabella ARP, associando al proprio indirizzo IP lo stesso indirizzo fisico MAC del secondo target (nel nostro caso il modem).

LEGENDA

IP KALI : 192.168.5.80
IP WINDOWS : 192.168.5.243
IP GATEWAY : 192.168.5.1

Per fare ciò, tramite ettercap, occorre passare per 4 fasi:

1. Scansione degli host nella rete

In questa fase si esegue una scansione degli host sulla rete per individuare i 2 target interessati.

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
14 hosts added to the hosts list...
```

2. Selezione dei target

In questa fase si stabiliscono i 2 target da infettare, nel nostro caso la macchina nativa 192.168.5.243 e il modem 192.168.5.1.

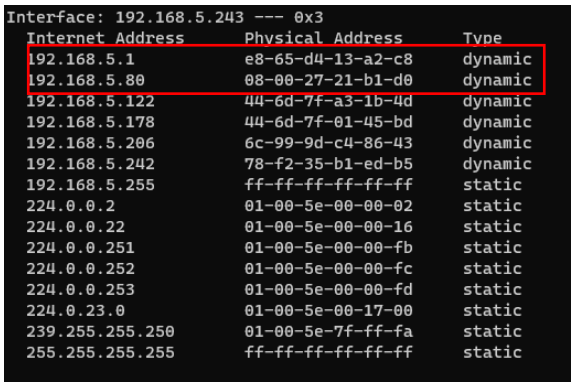
IP Address	MAC Address	Description
192.168.5.1	E8:65:D4:13:A2:C8	
192.168.5.6	E8:65:D4:13:A2:D8	
192.168.5.11	50:0F:F5:59:04:30	
192.168.5.31	2C:71:FF:4F:FC:B9	
192.168.5.32	98:B6:E9:4B:BA:A4	
192.168.5.46	74:EC:B2:0F:8E:7F	
192.168.5.48	F8:B9:5A:B4:77:58	

```
192.168.5.143   42:22:E6:8D:6A:0F
192.168.5.150   E8:C7:CF:37:24:FE
192.168.5.178   44:6D:7F:01:45:BD
192.168.5.206   6C:99:9D:C4:86:43
192.168.5.234   E0:73:E7:87:F1:19
192.168.5.242   78:F2:35:B1:ED:B5
192.168.5.243   E0:C2:64:2F:48:B5
```

3. ARP poisoning

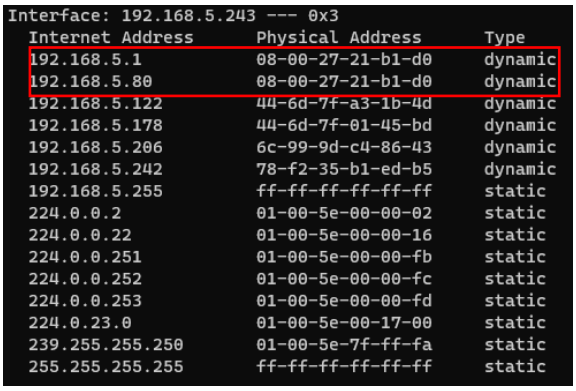
In questa fase si effettua il vero e proprio attacco, dove si modificano le tabelle ARP.

```
ARP poisoning victims:

GROUP 1 : 192.168.5.1 E8:65:D4:13:A2:C8

GROUP 2 : 192.168.5.243 E0:C2:64:2F:48:B5
```



```
Interface: 192.168.5.243 --- 0x3
  Internet Address      Physical Address      Type
  192.168.5.1           e8-65-d4-13-a2-c8     dynamic
  192.168.5.80          08-00-27-21-b1-d0     dynamic
  192.168.5.122         44-6d-7f-a3-1b-4d     dynamic
  192.168.5.178         44-6d-7f-01-45-bd     dynamic
  192.168.5.206         6c-99-9d-c4-86-43     dynamic
  192.168.5.242         78-f2-35-b1-ed-b5     dynamic
  192.168.5.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  224.0.23.0            01-00-5e-00-17-00     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

ARP TABLE prima del poisoning



```
Interface: 192.168.5.243 --- 0x3
  Internet Address      Physical Address      Type
  192.168.5.1           08-00-27-21-b1-d0     dynamic
  192.168.5.80          08-00-27-21-b1-d0     dynamic
  192.168.5.122         44-6d-7f-a3-1b-4d     dynamic
  192.168.5.178         44-6d-7f-01-45-bd     dynamic
  192.168.5.206         6c-99-9d-c4-86-43     dynamic
  192.168.5.242         78-f2-35-b1-ed-b5     dynamic
  192.168.5.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  224.0.23.0            01-00-5e-00-17-00     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

ARP TABLE dopo il poisoning

4. Recupero delle informazioni

Eseguito l'ARP poisoning è ora possibile recuperare le informazioni scambiate tra i 2 target, nel nostro caso, durante il login della paginda di vulnweb è possibile vedere in chiaro username e password.

Da notare che questo attacco, in questa forma consente di recuperare solamente informazioni non criptate.

```
HTTP : 44.228.249.3:80 -> USER: login  PASS: password  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=login&pass=password
```