

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

Il protocollo ARP (Address Resolution Protocol) è un protocollo di rete che fa parte del IPv4 ed opera al livello di accesso rete (Livello 3 modello ISO/OSI).

Si basa su di una tabella che contiene l'associazione degli indirizzi logici e fisici degli host della rete collegata. In altre parole, risolve gli indirizzi di rete IPv4 in indirizzi di collegamento MAC.

## Cosa sono gli attacchi MITM

MITM (Man in the Middle) è un attacco informatico che prevede l'inserimento di un attaccante in una comunicazione tra un client e server e la intercetta o ne prende il controllo.

Infatti, l'attaccante si posiziona in mezzo alla comunicazione per intercettare, inviare e ricevere dati destinati all'entità legittima senza che se ne accorga.

I rischi sono molteplici:

- Compromissione dei dati;
- Furto di informazioni sensibili;
- L'intercettazione e manipolazione dei dati;
- Infiltrazione di malware.

## Cos'è l'attacco ARP-Poisoning

L'ARP-POISONING è un attacco che corrompe la mappatura MAC-to-IP di altri dispositivi della rete.

In particolare va a sostituire (avvelenare) la tabella ARP sostituendosi all'indirizzo MAC del Router/Gateway.

### MAC Address Router/Gateway

```
Interfaccia: 192.168.1.214 --- 0x7
```

Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	80-02-9c-48-dc-6f	dinamico
192.168.1.255	ff-ff-ff-ff-ff-ff	statico
224.0.0.2	01-00-5e-00-00-02	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

### Mac Address Attaccante

```
inet 192.168.1.143 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::cd2b:232e:9caf:b494 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
RX packets 267 bytes 33445 (32.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 305 bytes 20016 (19.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

### Mac Address Sostituito

```
Interfaccia: 192.168.1.214 --- 0x7
```

Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	08-00-27-cb-7e-f5	dinamico
192.168.1.143	08-00-27-cb-7e-f5	dinamico
192.168.1.255	ff-ff-ff-ff-ff-ff	statico
224.0.0.2	01-00-5e-00-00-02	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

## Le fasi dell'attacco

**1° Fase:** L'attaccante deve trovarsi all'interno della rete per riuscire a recuperare l'indirizzo IP del Router.

**2° Fase:** Creare un indirizzo IP con la stessa rete

**3° Fase:** Individuare l'host da attaccare utilizzando Ettercap.

**4° Fase:** Avviare Ettercap.

**5° Fase:** Dal menù di Ettercap andare su Hosts -> Scan for Hosts per scannerizzare gli indirizzi IP e Mac collegati in rete.

**6° Fase:** Aggiungere su Target 1 l'indirizzo IP del Router e su Target 2 l'indirizzo IP dell'Host.

IP Address	MAC Address	Description
192.168.1.1	80:02:9C:48:DC:6F	
192.168.1.2	80:02:9C:72:18:C9	
192.168.1.151	60:21:C0:97:51:AB	
192.168.1.166	0A:92:FC:5E:69:2D	
192.168.1.214	98:54:1B:4A:38:BE	
Delete Host		
2182 known services Lua: no scripts were specified, not starting up! Starting Unified sniffing...  Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... 5 hosts added to the hosts list... Host 192.168.1.1 added to TARGET1 Host 192.168.1.214 added to TARGET2		

**7° Fase:** Dal menù MITM cliccare su Arp Poisoning -> OK.

```
ARP poisoning victims:

GROUP 1 : 192.168.1.1 80:02:9C:48:DC:6F

GROUP 2 : 192.168.1.214 98:54:1B:4A:38:BE
```

In questo modo l'host è compromesso.

Per l'esercizio utilizziamo la pagina web <http://testphp.vulnweb.com/login.php> così da testare l'attacco.

Aperto il link ci troviamo ad una pagina di login.

Inserendo Username e Password e cliccando su login, notiamo che le credenziali compariranno sul terminale dell'attaccante.

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

## Conclusione:

Con l'attacco MITM l'attaccante potrà vedere tutti i dati non cifrati durante la comunicazione tra il Router e l'Host, compresi le credenziali di accesso (Username e Password).