

Per fare l'ARP-POISONING ho implementato l'uso di ettercap. Iniziamo verificando l'IP del target (192.168.1.168) e l'IP del router (192.168.1.1)

```
Microsoft Windows [Versione 10.0.22621.3007]
(c) Microsoft Corporation. Tutti i diritti riservati.

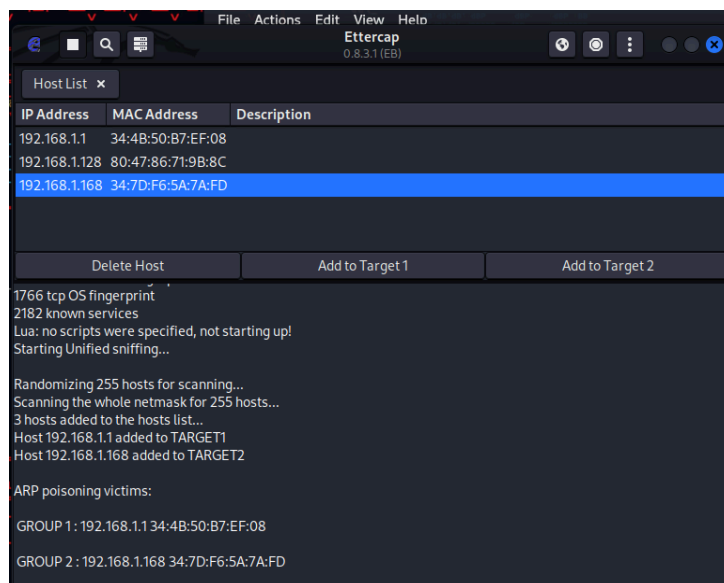
C:\Users\stefa>arp -a

Interfaccia: 192.168.56.1 --- 0x5
    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
    255.255.255.255       ff-ff-ff-ff-ff-ff  statico

Interfaccia: 192.168.1.168 --- 0x11
    Indirizzo Internet    Indirizzo fisico    Tipo
    192.168.1.1           34-4b-50-b7-ef-08  dinamico
    192.168.1.128         80-47-86-71-9b-8c  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

C:\Users\stefa>
```

Successivamente tramite ettercap siamo andati ad “avvelenare” la tabella di ARP in modo tale da poter intercettare le informazioni in chiaro inviate dall'utente




Tutto questo facendo in modo che il mac address della macchina attaccante vada a sostituirsi a quello del router (cioè ci siamo messi tra il router e il target)

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.181 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:feeb:7ef5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 238 bytes 17846 (17.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 3940 (3.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Verificato il mac address della macchina attaccante in questo caso kali linux siamo andati a verificare che fosse andato correttamente nella tabella arp

Interfaccia: 192.168.1.168 --- 0x11		
Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	08-00-27-cb-7e-f5	dinamico
192.168.1.128	80-47-86-71-9b-8c	dinamico
192.168.1.181	08-00-27-cb-7e-f5	dinamico

E come possiamo vedere notiamo che troviamo 2 volte il mac address di kali, sia sul IP del router che sul IP della macchina kali, dopo ho fatto un test su Vulnweb per intercettare le credenziali in chiaro




TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)

Links
[Security art](#)
[PHP scanner](#)
[PHP vuln help](#)
[Fractal Explorer](#)



If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Le quali andiamo poi a trovare sull'interfaccia di ettercap

```
GROUP 1 : 192.168.1.1 34:4B:50:B7:EF:08

GROUP 2 : 192.168.1.168 34:7D:F6:5A:7A:FD
HTTP : 44.228.249.3:80 -> USER: admin PASS: 1234asd INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=admin&pass=1234asd
```

Un protocollo ARP è quello che associa un indirizzo IP ad un indirizzo mac che si può verificare tramite il confronto con la tabella (arp -a)

Gli attacchi MitM sono una tipologia di attacco in cui una terza persona si mette nel mezzo tra la connessione di altre 2 in modo da intercettare pacchetti, dati, informazioni, ecc

L'attacco ARP Poisoning è quando andiamo ad "ingannare" il pc target e il router, facendo in modo di metterci in mezzo ad essi tramite la sostituzione con il nostro indirizzo MAC, in modo tale da intercettare tutte le informazioni in chiaro

Le fasi dell'attacco sono:

- inserimento nella LAN del target
- individuiamo il dispositivo del target (IP)
- tramite ettercap "avveleniamo" la tabella ARP facendo passare il nostro IP (attaccante) al posto di quello del router
- attesa che il target entri nel sito di interesse e inserisca le credenziali
- intercettazione delle stesse e visione tramite l'interfaccia di ettercap