



Ettercap



ARP

Il Protocollo ARP (Address Resolution Protocol) serve a trovare gli indirizzi MAC associati agli indirizzi IP in una rete locale. Quando un dispositivo vuole comunicare con un altro nella stessa rete, utilizza ARP per scoprire il corrispondente indirizzo MAC del destinatario. Ovviamente il tutto si basa su una tabella, che si può vedere col comando `arp -a`.



MITM

Gli attacchi MITM, acronimo di "Man-in-the-Middle" (Uomo nel mezzo), sono tipologie di attacchi informatici in cui un aggressore inserisce se stesso tra la comunicazione di due parti, riuscendo a intercettare il flusso di dati tra di esse. L'obiettivo principale di un attacco MITM è quello di ottenere informazioni sensibili o di compromettere la sicurezza della comunicazione, o addirittura riportarli in altri siti creati da loro o addirittura portarli in un malware. Ci sono due tipi di attacchi che abbiamo studiato:

ARP Poisoning e DNS Poisoning.



DNS Poisoning

Il DNS Poisoning, è un tipo di attacco informatico in cui un aggressore manipola la cache del server DNS o del client inserendo informazioni di mapping DNS falsificate. Questo porta a un'errata associazione tra nomi di dominio e indirizzi IP, inducendo gli utenti a essere reindirizzati a siti Web dannosi o pagine fasulle controllate dall'attaccante.

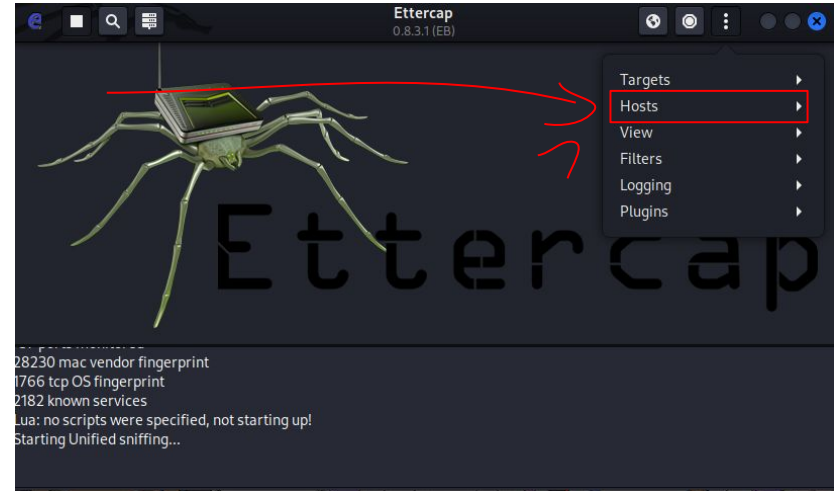
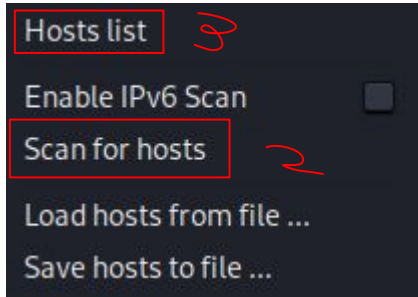


ARP Poisoning

In un attacco ARP Poisoning, l'attaccante manipola la tabella di traduzione degli indirizzi IP nei pacchetti di rete utilizzando pacchetti ARP falsificati. Il processo coinvolge la modifica della risoluzione degli indirizzi MAC in modo che il traffico di rete destinato a un particolare indirizzo MAC venga deviato attraverso l'attaccante anziché verso il destinatario previsto. In altre parole, l'attaccante invia pacchetti ARP falsificati nella rete locale, convincendo gli altri dispositivi a credere che il suo indirizzo MAC sia associato all'indirizzo IP di un altro dispositivo legittimo. Di conseguenza, quando i dispositivi cercano di comunicare tra loro, il traffico viene deviato attraverso l'attaccante. Vediamolo nel pratico.

ARP Poisoning

Andiamo su kali e scriviamo Ettercap, dopodichè andiamo su Hosts > Scan for hosts > Aspettare > Host List.



ARP Poisoning

A questo punto mettiamo in Target 1 e Target 2 l'ip del mio router e del mio PC.

Poi facciamo il menu > arp poisoning e diamo l'ok.

The screenshot shows a network tool interface with a 'Host List' window and a 'MITM' menu.

Host List

IP Address	MAC Address	Description
192.168.1.1	4C:F5:5B:57:1D:6F	
192.168.1.30	2C:F0:5D:22:B2:F3	
192.168.1.98	D8:FB:D6:2E:3B:A1	
192.168.1.135	AA:1A:F7:70:20:9F	
192.168.1.148	68:B6:91:FC:51:C4	
192.168.1.168	08:00:27:A9:A5:FB	

Buttons: Delete Host, Add to Target 1, Add to Target 2

MITM Menu

- ARP poisoning...
- NDP poisoning
- ICMP redirect...
- Port stealing...
- DHCP spoofing...
- Stop MITM attack(s)
- SSL Intercept

Host 192.168.1.30 added to TARGET1
Host 192.168.1.1 added to TARGET2

ARP poisoning victims:

GROUP 1 : 192.168.1.30 2C:F0:5D:22:B2:F3

GROUP 2 : 192.168.1.1 4C:F5:5B:57:1D:6F

ARP Poisoning

Come possiamo vedere Wireshark ci dirà che ha trovato un duplicato di indirizzo mac, possiamo anche vedere se eseguiamo il comando `arp -a` nel mio pc nel prompt dei comandi e corrisponderà al indirizzo mac di kali.

```
239 33.562098044 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
240 34.402362141 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.147? Tell 192.168.1.1
241 34.579708495 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
242 34.880064073 PcsCompu_cb:7e:f5 Micro-St_22:b2:f3 ARP 42 192.168.1.1 is at 08:00:27:cb:7e:f5
243 34.880243794 PcsCompu_cb:7e:f5 HuaweiTe_57:1d:6f ARP 42 192.168.1.30 is at 08:00:27:cb:7e:f5
244 35.402256460 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.147? Tell 192.168.1.1
247 35.572029352 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
250 36.402064692 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.147? Tell 192.168.1.1
251 36.572536626 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
252 37.587580664 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
253 38.434654057 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.147? Tell 192.168.1.1
254 38.582863993 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
261 39.432528395 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.147? Tell 192.168.1.1
308 39.582621634 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
425 40.433520609 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.147? Tell 192.168.1.1
432 40.606623801 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
487 41.602023124 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
488 42.468944992 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.147? Tell 192.168.1.1
489 42.602906332 HuaweiTe_57:1d:6f Broadcast ARP 60 Who has 192.168.1.137? Tell 192.168.1.1
```

```
» Frame 204: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
» Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: HuaweiTe_57:1d:6f (4c:f5:5b:57:1d:6f)
» Address Resolution Protocol (reply)
» [Duplicate IP address detected for 192.168.1.30 (08:00:27:cb:7e:f5) - also in use by 2c:f0:5d:22:b2:f3 (frame 203)]
```


ARP Poisoning

Come possiamo vedere il mio indirizzo fisico è esattamente quello di kali (fate ifconfig per vedere) esattamente come ci aspettavamo.

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

```
Interfaccia: 192.168.1.30 --- 0x9
```

Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	08-00-27-cb-7e-f5	dinamico
192.168.1.167	08-00-27-cb-7e-f5	dinamico

```
~$ ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.167 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 22704 bytes 10694721 (10.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16661 bytes 6229528 (5.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



ARP Poisoning

Adesso andiamo nel sito <http://testphp.vulnweb.com/login.php> e vediamo cosa accade se inserisco i miei dati di login.

```
GROUP 2 : 192.168.1.1 4C:F5:5B:57:1D:6F  
HTTP : 44.228.249.3:80 -> USER: Void PASS: Biscotto INFO: http://testphp.vulnweb.com/login.php  
CONTENT: uname=Void&pass=Biscotto
```

Come possiamo notare si vedono in chiaro sia l'username **Void** che la password **Biscotto**. Per evitare questo tipo di problema basta avere il servizio https, perchè è in grado di intercettare ma non ci capirà nulla perchè è criptato.