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

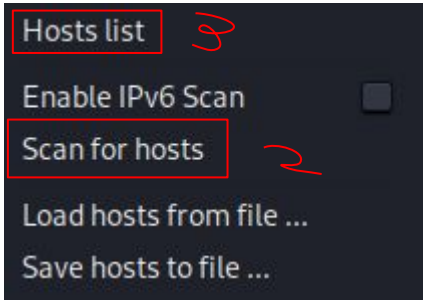
Il DNS Poisoning, è un tipo di attacco informatico in cui un aggressore manipola la cache del server DNS o del client inserendo informazioni di mapping DNS falsificate. Questo porta a un'errata associazione tra nomi di dominio e indirizzi IP, inducendo gli utenti a essere reindirizzati a siti Web dannosi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

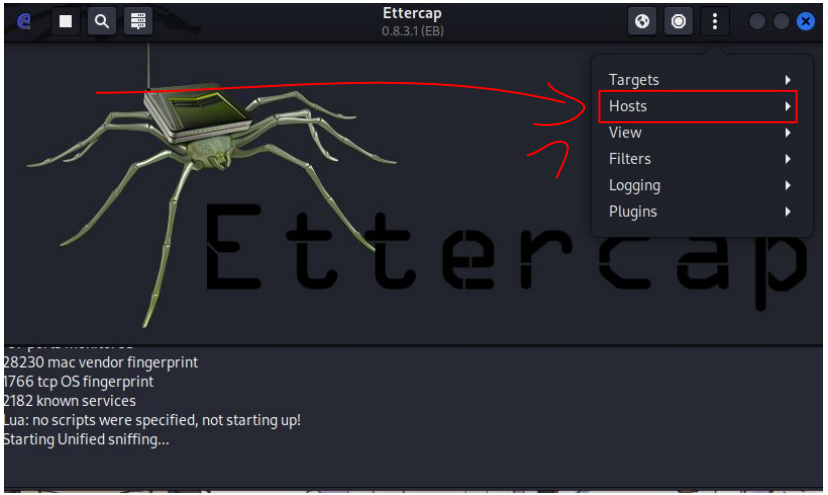
ARP Poisoning

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.

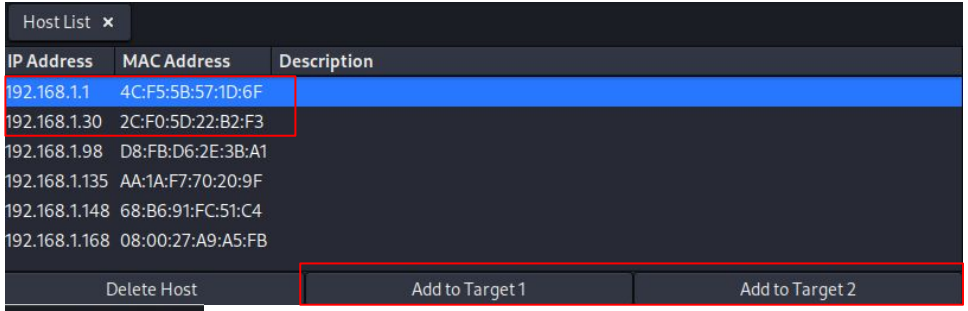


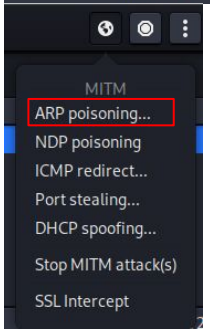


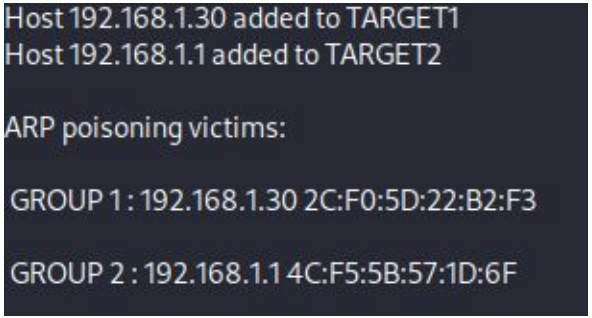
ARP Poisoning

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.

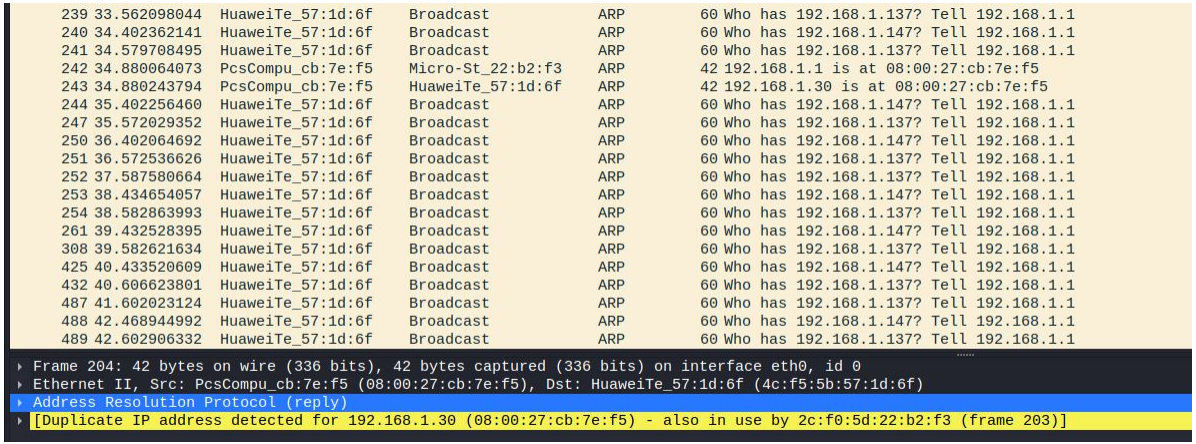






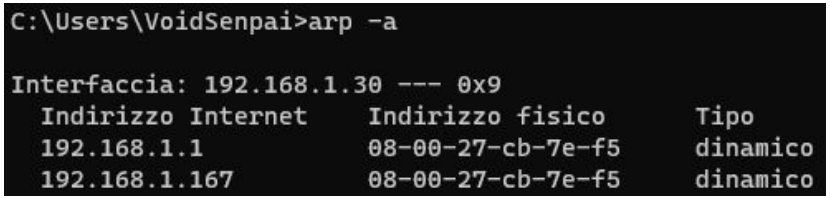
ARP Poisoning

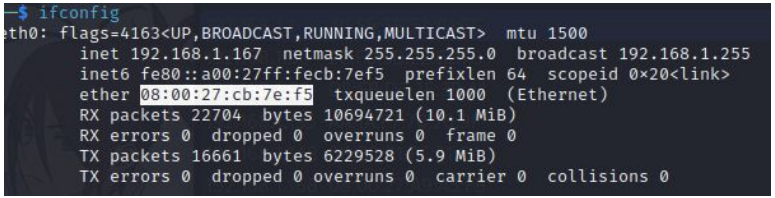
Come possiamo vedere Wireshark ci dirà che ha trovato un duplicato di indirizzo mac, possiamo anche vedere se eseguiamo il comando `arp -a` nel mio pc nel prompt dei comandi e corrisponderà al indirizzo mac di kali.



ARP Poisoning

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





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.