NMAP

Su questo esercizio vedremo come utilizzare nmap su kali linux. Per prima cosa, apriamo le macchine virtuali Kali e metasploitable.

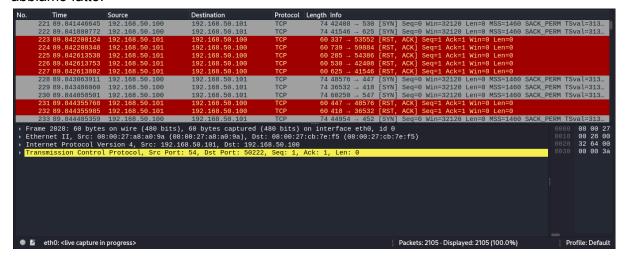
Dopo questo, apriamo kali, e sul terminale lanciamo il comando di nmap, la funzione che vogliamo, se sS o sT, sapendo che il comando sS lancia solo una SYN, quindi questo comando risulta meno "aggressivo" quindi in poche parole andrà solo a controllare se la porta è aperta, e non altro. Invece il comando sT lancia uno scan TCP, questo è più aggressivo, risultando nel controllare tutte le porte aperte e tutte le sue vie.

Come in immagine, eseguiamo il comando di nmap -sS:

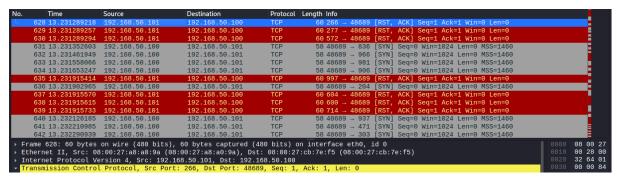
Come in immagine, eseguiamo il comando di nmap -sT:

```
-(kali⊕kali)-[~]
  -$ nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.945VN (https://nmap.org) at 2024-02-07 13:59 EST Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.50.101
Host is up (0.0048s latency).
Not shown: 1012 closed tcp ports (conn-refused)
         STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
Nmap done: 1 IP address (1 host up) scanned in 13.98 seconds
```

E su questl, andiamo anche a fare la cattura su Wireshark, confrontando i due scan che abbiamo fatto:



(Scansione comando sT)



(Scansione comando sS)

Con questo vediamo che quando lanciamo il comando sT, la macchina bersaglio risponde con una SYN, ACK ma la nostra macchina risponde con un rst, così non concludendo il 3WH.

Invece con la scansione sS noi inviamo solamente un SYN e la macchina bersaglio ci risponde soltanto con una RST