Network Scan IoC

Nel file di cattura ci sono piú di 2000 pacchetti, a primo impatto sembra essere un port scan.
Per filtrare tutte le porte scansionate con conferma dobbiamo filtrare i pacchetti [SYN ACK].
Utilizziamo il filtro tcp.flags==0x12 fonte qui sotto. Vediamo il risultato
https://osqa-ask.wireshark.org/questions/60995/how-do-i-filter-tcp-connection-with-syn-and-syn-ack-without-ack-response/

That's not an easy task because Wireshark can't filter on packet dependencies between multiple packets without some tricks. What I would do is try this filter:

```
(tcp.flags==0x12) and not tcp.analysis.initial_rtt
```

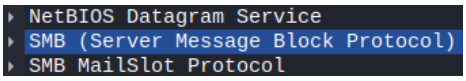
"tcp.flags==0x12" looks for SYN/ACK packets (you could also use "tcp.flags.syn==1 and tcp.flags.ack==1", or, if you want SYN and SYN/ACK, use "tcp.flags.syn==1 or (tcp.flags.syn==1 and tcp.flags.ack==1)".

tcp.flags==0x12

No.	Time	Source	Destination	Protocol	Length	Info
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
267	36.788805940	192.168.200.150	192.168.200.100	TCP	74	514 → 51396 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42048 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64

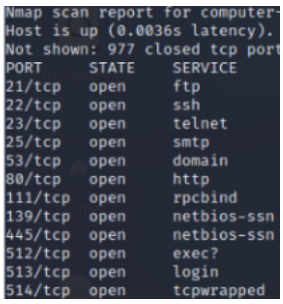
Qui sotto il primo pacchetto

Source	Destination	Protocol	Length	Info
192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE,



Info del pacchetto

Da tutte le porte aperte sembra che sia una Metasploitable 2 sotto la scansione fatta:



Nmap

Quindi possiamo dedurre che:

attacker = kali 192.168.200.150

victim = metasploitable 2 192.168.200.100

Scansione fatta probabilmente con il modulo auxiliary scanner come obiettivo NetBIOS porta 139/445 SMB o in ogni caso é stata effettuata una scansione sulla macchina metasploitable 2 192.168.200.100.