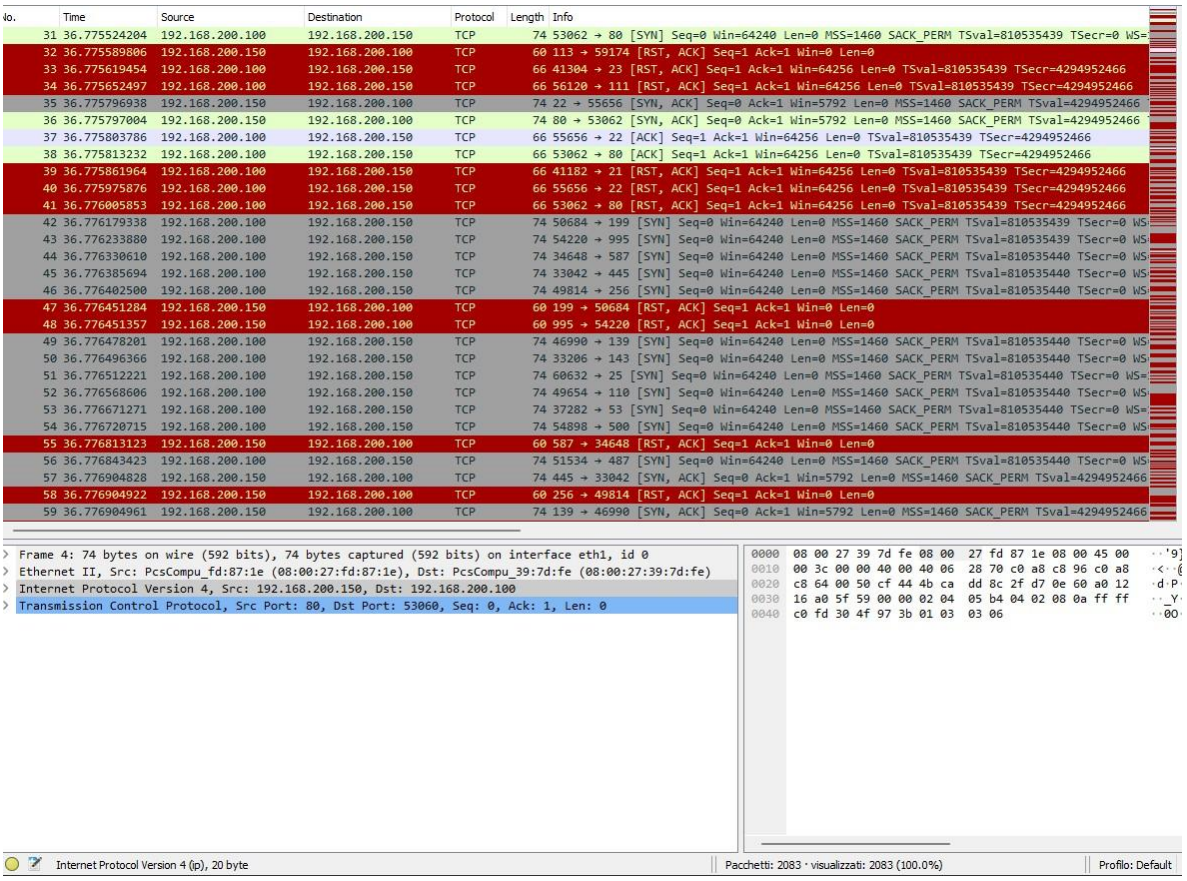
Progetto S9-L3

Studente: Simone MIninni

Task: Identificare eventuali eventi, segnali di compromissione attraverso il network monitoring con wireshark

Evidenze di attacchi in corso:



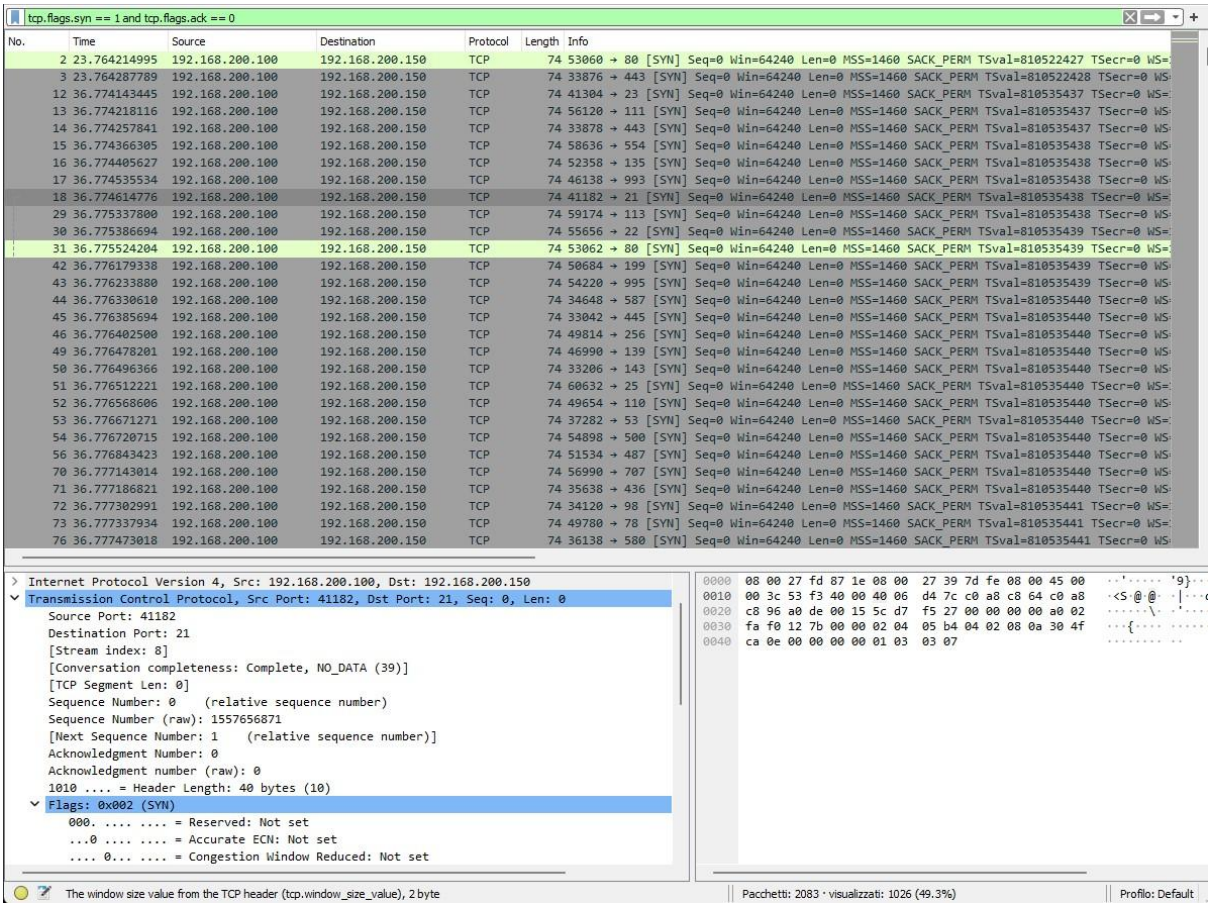
Dalla schermata di wireshark, possiamo notare una situazione insolita, ovvero più di mille pacchetti tcp inviati da uno stesso indirizzo ip(192.168.200.100) verso un range vasto di porte.
Inoltre le richieste sono effettuate in un range di tempo ristretto e la lunghezza dei pacchetti è uguale, ovvero ‘len=0’.

Potenziali vettori di attacco:

Probabilmente la macchina attaccante(192.168.200.100) sta effettuando una scansione delle porte sul target(192.168.200.150).

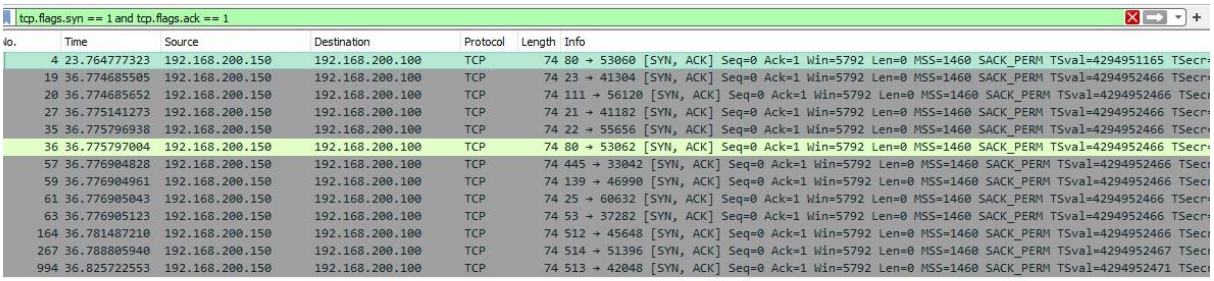
Infatti se andiamo a filtrare i pacchetti notiamo un comportamento tipico della scansione full tcp.

Pacchetti syn inviati dall‘ attaccante:



n. pacchetti inviati: 1026 (si può presumere una scansione sulle common well known ports).

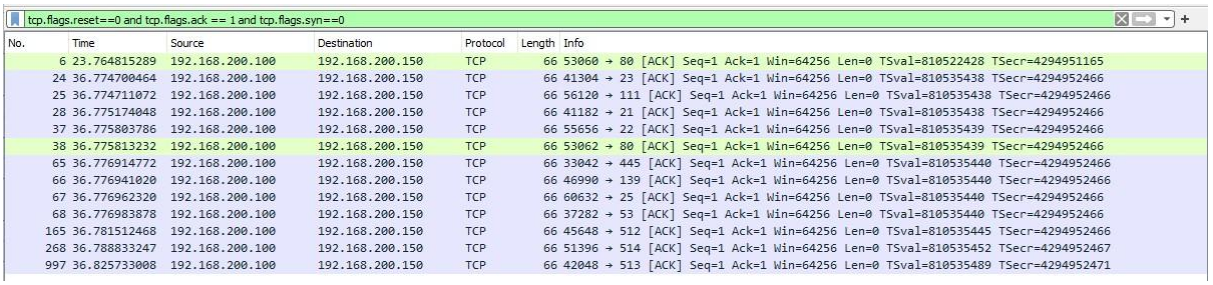
Risposta syn,ack da parte del target:



n. porte aperte: 13. Il target ha risposto confermando che la porta è aperta, mentre dal primo screenshot si può notare una serie di risposte rst,ack confermando che la porta relativa è chiusa.

Risposta ack dell’ attaccante:

.



No.	Time	Source	Destination	Protocol	Length	Info
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
268	36.788833247	192.168.200.100	192.168.200.150	TCP	66	51396 → 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535452 TSecr=4294952467
997	36.825733008	192.168.200.100	192.168.200.150	TCP	66	42048 → 513 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535489 TSecr=4294952471

L’ attaccante chiude la connessione tcp inviando il pacchetto di ack.

Azioni di rimedio:

Per ridurre i tentativi di attacco, si potrebbe impostare una regola sul firewall per bloccare le connessioni con la macchina attaccante(192.168.200.100).
Inoltre si potrebbero bloccare le porte su cui sono esposti servizi critici, dove un eventuale exploit su questi comporterebbe un danno importante per l’azienda.