

# S9/L3

Stefano Di Prospero

No.	Time	Source	Destination	Protocol	Length	Info
244	36.788153892	192.168.200.100	192.168.200.150	TCP	74	51844 → 855 [SYN] Seq=0 Win=64240 Len=0
245	36.788170982	192.168.200.100	192.168.200.150	TCP	74	45726 → 232 [SYN] Seq=0 Win=64240 Len=0
246	36.788186352	192.168.200.100	192.168.200.150	TCP	74	52724 → 904 [SYN] Seq=0 Win=64240 Len=0
247	36.788298677	192.168.200.100	192.168.200.150	TCP	74	49480 → 835 [SYN] Seq=0 Win=64240 Len=0
248	36.788330073	192.168.200.100	192.168.200.150	TCP	74	41098 → 602 [SYN] Seq=0 Win=64240 Len=0
249	36.788373483	192.168.200.100	192.168.200.150	TCP	74	54196 → 291 [SYN] Seq=0 Win=64240 Len=0
250	36.788443559	192.168.200.150	192.168.200.100	TCP	60	709 → 59046 [RST, ACK] Seq=1 Ack=1 Win=0
251	36.788443656	192.168.200.150	192.168.200.100	TCP	60	271 → 44414 [RST, ACK] Seq=1 Ack=1 Win=0
252	36.788443696	192.168.200.150	192.168.200.100	TCP	60	470 → 50612 [RST, ACK] Seq=1 Ack=1 Win=0
253	36.788443736	192.168.200.150	192.168.200.100	TCP	60	180 → 36266 [RST, ACK] Seq=1 Ack=1 Win=0
254	36.788443776	192.168.200.150	192.168.200.100	TCP	60	855 → 51844 [RST, ACK] Seq=1 Ack=1 Win=0
255	36.788443816	192.168.200.150	192.168.200.100	TCP	60	232 → 45726 [RST, ACK] Seq=1 Ack=1 Win=0
256	36.788443857	192.168.200.150	192.168.200.100	TCP	60	904 → 52724 [RST, ACK] Seq=1 Ack=1 Win=0
257	36.788443896	192.168.200.150	192.168.200.100	TCP	60	835 → 49480 [RST, ACK] Seq=1 Ack=1 Win=0
258	36.788490564	192.168.200.150	192.168.200.100	TCP	60	602 → 41098 [RST, ACK] Seq=1 Ack=1 Win=0
259	36.788490603	192.168.200.150	192.168.200.100	TCP	60	291 → 54196 [RST, ACK] Seq=1 Ack=1 Win=0
260	36.788511936	192.168.200.100	192.168.200.150	TCP	74	48350 → 956 [SYN] Seq=0 Win=64240 Len=0
261	36.788567765	192.168.200.100	192.168.200.150	TCP	74	36542 → 773 [SYN] Seq=0 Win=64240 Len=0
262	36.788600279	192.168.200.100	192.168.200.150	TCP	74	51396 → 514 [SYN] Seq=0 Win=64240 Len=0
263	36.788677629	192.168.200.100	192.168.200.150	TCP	74	56758 → 224 [SYN] Seq=0 Win=64240 Len=0
264	36.788716758	192.168.200.100	192.168.200.150	TCP	74	48824 → 183 [SYN] Seq=0 Win=64240 Len=0

Frame 251: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
Ethernet II, Src: PCSSystemtec\_fd:87:1e (08:00:27:fd:87:1e), Dst: 192.168.200.150 (08:00:00:00:00:00)  
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100  
Transmission Control Protocol, Src Port: 271, Dst Port: 44414

in **Giallo** abbiamo le richieste TCP da parte di un IP:  
192.168.200.100

in **Celeste** la risposta negativa da parte dell'IP:  
192.168.200.150

Da questo possiamo dedurre che stia avvenendo una scansione da parte dell'IP 192.168.200.100 verso l'IP 192.168.200.150

Per evitare che tramite la scansione l'attaccante possa trovare informazioni utili, si possono implementare delle regole firewall in modo che chi sta facendo la scansione non possa avere accesso alle porte della macchina vittima.

