

## Settimana 9 esercizio 3 Daniele D'Esposito

Time	Source	Destination	Protocol	Length	Info
10 28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	who has 192.168.200.150? Tell 192.168.200.100
11 28.775230909	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12 36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13 36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14 36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15 36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16 36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17 36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18 36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19 36.774685905	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=6
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=6
21 36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 36.774708464	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
Transmission Control Protocol, Src Port: 443, Dst Port: 33878, Seq: 1, Ack: 1, Len: 0					
Source Port: 443					
Destination Port: 33878					
[Stream index: 4]					
[Conversation completeness: Incomplete (37)]					
...1... = RST: Present					
...0... = FIN: Absent					
...0... = Data: Absent					
...1... = ACK: Present					
...0... = SYN-ACK: Absent					
...1... = SYN: Present					
[Completeness Flags: R..A.S]					
[TCP Segment Len: 0]					
Sequence Number: 1 (relative sequence number)					
Sequence Number (raw): 0					
[Next Sequence Number: 1 (relative sequence number)]					
Acknowledgment Number: 1 (relative ack number)					
Acknowledgment number (raw): 3296938610					
0101... = Header Length: 20 bytes (5)					
[Flags: 0x014 (RST, ACK)]					
000... = Reserved: Not set					
...0... = Accurate ECN: Not set					
...0... = Congestion Window Reduced: Not set					
...0... = ECN-Echo: Not set					
...0... = Urgent: Not set					
...1... = Acknowledgment: Set					
...0... = Push: Not set					
...1... = Reset: Set					
[Expert Info (Warning/Sequence): Connection reset (RST)]					

Aprendo il file fornito dalla traccia, appare una sessione di wireshark che cattura la comunicazione tra gli ip 192.168.200.150(attaccato) e 192.168.200.100(attaccante).

Si puo' notare come l'indirizzo attaccante mandi tante richieste TCP a molte porte. Prendendo in esame la riga 21 si vede che la porta 443 manda alla porta 33878 un segnale di reset(rst) che termina la connessione lasciando incompleto il 3 way handshake iniziato nella riga 14 con un syn. Questo significa che la porta e' chiusa. Se invece la porta risponde con syn/ack allora e' aperta. E' ragionevole concludere che l'attaccante stia usando strumenti di port scanning, come per esempio nmap.

Per ovviare al problema bisogna utilizzare un firewall che impedisca la comunicazione con l'ip attaccante.