

# Cattura Wireshark

L'esercizio di oggi consiste nella lettura e comprensione di una cattura effettuata su wireshark, tentando di capire che tipo di attacco sia stato effettuato.

Cattura\_U3\_W1\_L3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Len Info

13	36.774218116	192.168.200.100	192.168....	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....	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....	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....	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....	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....	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.150	192.168....	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....	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168....	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168....	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168....	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168....	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....	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168....	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168....	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168....	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168....	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168....	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168....	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168....	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168....	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168....	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	192.168.200.150	192.168....	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....	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168....	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....	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168....	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168....	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168....	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168....	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168....	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168....	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168....	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402500	192.168.200.100	192.168....	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168....	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168....	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478201	192.168.200.100	192.168....	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168....	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168....	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52	36.776568606	192.168.200.100	192.168....	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128

▶ Frame 42: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface  
▶ Ethernet II, Src: PcsCompu\_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu\_fd:87:1e (00:00:08:00:27:fd:87:1e:08:00:27:39:7d:fe:08:00:45:00:00:10:00:3c:7f:22:40:00:40:06:a9:4d:c0:a8:c8:64:c0:a8:..<."@.@..M...d..

# Lettura

La cattura mostra un gran numero di pacchetti SYN inviati dalla macchina 192.168.200.100 verso la macchina 192.168.200.150, tutti con lo stesso contenuto e indirizzati a porte sempre diverse.

A sua volta la macchina “.150” risponde con dei pacchetti ACK ad alcune di queste richieste.

# Conclusioni

Con tutta probabilità si tratta di una scansione dei servizi attivi sulla macchina 192.168.200.150, che invia risposte ACK quando una sua porta aperta viene richiesta.

Per ridurre l'impatto di questo attacco sarebbe utile un firewall o l'utilizzo di un reverse proxy