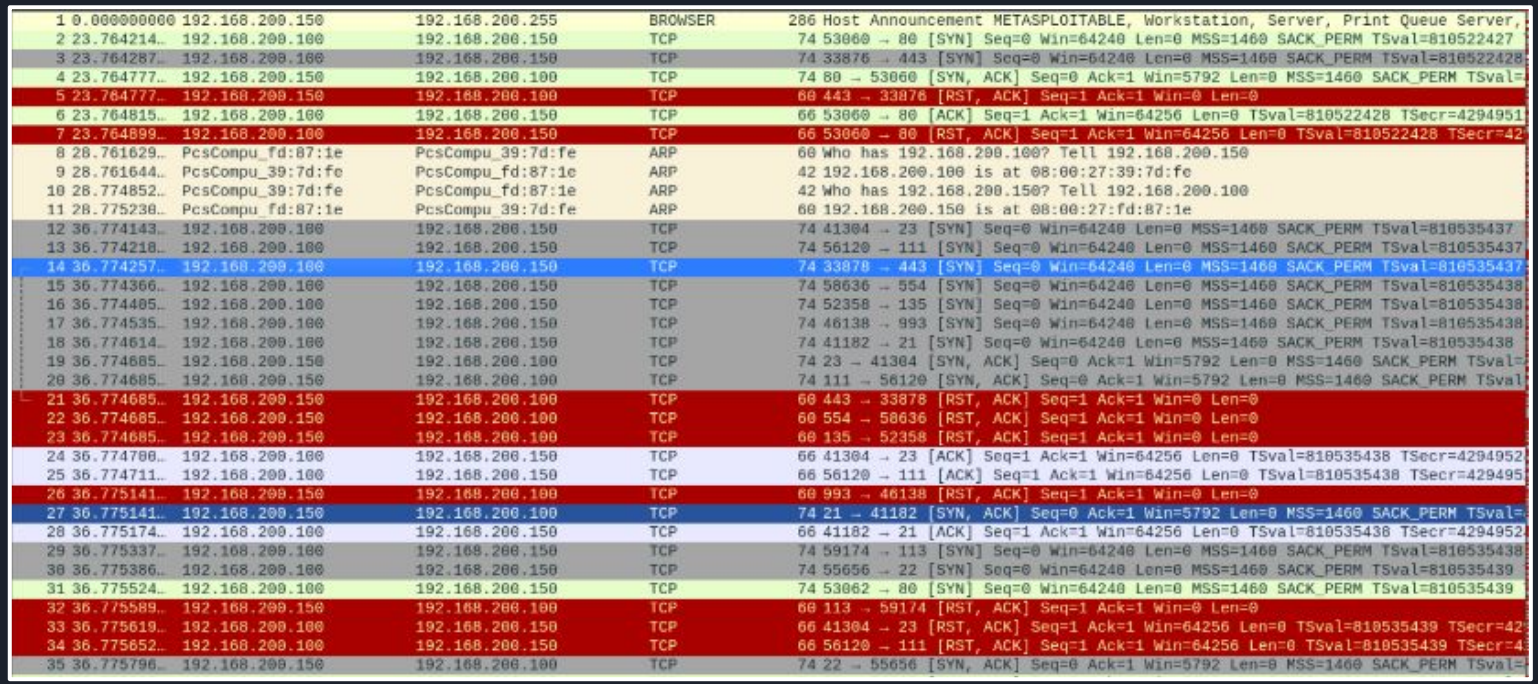

1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server,
2	23.764214…	192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427
3	23.764287…	192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428
4	23.764777…	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=
5	23.764777…	192.168.200.150	192.168.200.100	TCP	60 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815…	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951
7	23.764899…	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=42
8	28.761629…	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644…	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852…	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230…	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143…	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
13	36.774218…	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
14	36.774257…	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
15	36.774366…	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
16	36.774405…	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
17	36.774535…	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
18	36.774614…	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
19	36.774685…	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=
20	36.774685…	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
21	36.774685…	192.168.200.150	192.168.200.100	TCP	60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685…	192.168.200.150	192.168.200.100	TCP	60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685…	192.168.200.150	192.168.200.100	TCP	60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700…	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952
25	36.774711…	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=429495
26	36.775141…	192.168.200.150	192.168.200.100	TCP	60 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141…	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=
28	36.775174…	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952
29	36.775337…	192.168.200.100	192.168.200.150	TCP	74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438
30	36.775386…	192.168.200.100	192.168.200.150	TCP	74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439
31	36.775524…	192.168.200.100	192.168.200.150	TCP	74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439
32	36.775589…	192.168.200.150	192.168.200.100	TCP	60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619…	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=42
34	36.775652…	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4
35	36.775796…	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=

Nell'analisi eseguita con Wireshark, si evidenzia la presenza di numerose richieste TCP ripetute, suggerendo verosimilmente un'attività di scansione in corso. Per contrastare questa potenziale minaccia, potremmo adottare un'approccio preventivo attraverso l'impostazione di regole nel firewall. Queste regole avrebbero il compito di bloccare le scansioni provenienti dall'indirizzo IP dell'attaccante, impedendogli così di acquisire informazioni sullo stato delle porte aperte nel sistema.