Time	Source	Destination	Protocol	Length	Info
1 0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE,

La prima cosa che notiamo è che la macchina su indirizzo host .150 esegue un broadcast. Analizzando il pacchetto nel dettaglio possiamo vedere sia il servizio che la macchina, in questo caso un server SMB in esecuzione su Metasploitable.

```
·\MAILSL OT\BROWS
E····· METASPLO
ITABLE·· ·····
U·metasp loitable
 server  (Samba 3
.0.20-De bian)·
```

Analizzando nei dettagli i pacchetti notiamo che avviene una connessione su porta 80 dall'host .100 con tanto di completamento della sequenza di handshake.

23.764214995	192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0
23.764287789	192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=0
23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 → 53060 [SYN, ACK] Se
23.764777427	192.168.200.150	192.168.200.100	TCP	60 443 → 33876 [RST, ACK] S
23.764815289	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1 A

Andando avanti notiamo una serie di richieste SYN tra gli host .100 e .150 su varie porte, possiamo ipotizzare che sia una scansione TCP Connect Scan effettuata probabilmente tramite NMAP.

11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60 192.168.200.150 is at 08
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74 41304 → 23 [SYN] Seq=0 W
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74 56120 → 111 [SYN] Seq=0
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74 33878 → 443 [SYN] Seq=0
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74 58636 → 554 [SYN] Seq=0
16	36.774405027	192.168.200.100	192.168.200.150	TCP	74 52358 → 135 [SYN] Seq=0
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74 46138 → 993 [SYN] Seq=0
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74 41182 → 21 [SYN] Seq=0 W
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Se
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74 111 → 56120 [SYN, ACK] S
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60 443 → 33878 [RST, ACK] S
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60 554 → 58636 [RST, ACK] S
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60 135 → 52358 [RST, ACK] S

Analizzando più a fondo notiamo la natura randomica e l'elevato numero di richieste in poco tempo; questo ci da la quasi certezza che si tratti di una scansione NMAP con modalità -sT.

1970	36.873906267	192.168.200.100	192.168.200.150	TCP	74 57518 → 525 [SYN]
1971	36.873927281	192.168.200.100	192.168.200.150	TCP	74 48420 → 925 [SYN]
1972	36.874010804	192.168.200.100	192.168.200.150	TCP	74 60958 → 618 [SYN]
1973	36.874028994	192.168.200.100	192.168.200.150	TCP	74 41876 → 73 [SYN]
1974	36.874106428	192.168.200.150	192.168.200.100	TCP	60 525 → 57518 [RST

Per ridurre il rischio di tali scansioni una possibilità è quella di filtrare le porte tramite servizio firewall andando così a bloccare il ping su quelle porte che non vogliamo siano raggiungibili dall'esterno in quanto potrebbero essere usate per eventuali attacchi.