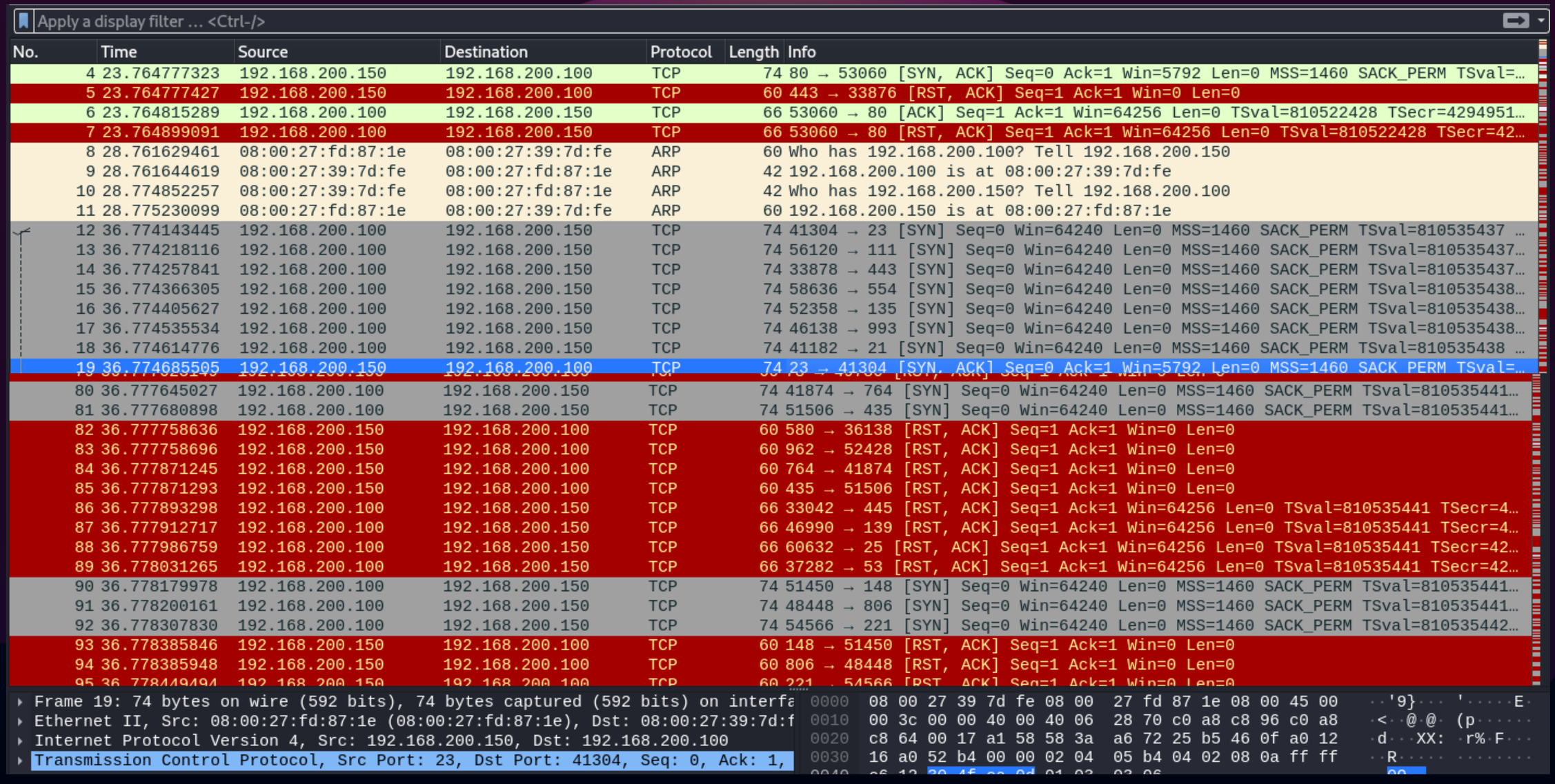
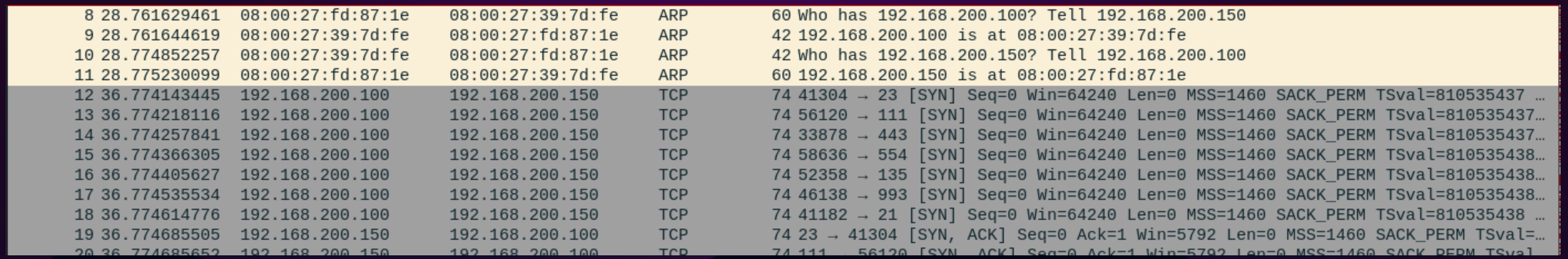

WIRESHARK

Obiettivo dell’esercizio è capire eventuali attacchi, quali sono i vettori di attacco e come ridurre gli impatti dell’attacco



Si noti che intuire chi è attaccante e chi attaccato non è immediato.
Tuttavia osservando lo scan nel dettaglio è possibile vedere che192.168.200.100 sta inoltrando un’ enorme quantità di richieste ARK verso 192.168.200.150.
Molto probabilmente 192.168.200.100 è l’attaccante.



8	28.761629461	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	08:00:27:fd:87:1e	08:00:27:39:7d:fe	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 …
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…
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…
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…
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…
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…
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 …
19	36.774685505	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	36.774685652	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…

Inoltre, "RST" sta per "Reset". Quando un host riceve un segmento TCP con il flag RST impostato, significa che la connessione TCP è stata ripristinata o "azzerata" bruscamente. Questo può avvenire per vari motivi, ad esempio quando si verifica un errore di comunicazione o quando un host desidera interrompere una connessione in modo improvviso.
Questo potrebbe avvenire perchè l’attaccato registra tentativi di connessione anomali.

```
39 36.780577880  192.168.200.150      192.168.200.100      TCP         60 266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40 36.780577981  192.168.200.150      192.168.200.100      TCP         60 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41 36.780578026  192.168.200.150      192.168.200.100      TCP         60 235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42 36.780578074  192.168.200.150      192.168.200.100      TCP         60 739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43 36.780578119  192.168.200.150      192.168.200.100      TCP         60 55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
44 36.780578158  192.168.200.150      192.168.200.100      TCP         60 999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
45 36.780578198  192.168.200.150      192.168.200.100      TCP         60 317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

IL VETTORE UTILIZZATO È IL PROTOCOLLO TCP

TCP è uno dei principali protocolli utilizzati nella comunicazione su Internet e viene utilizzato per trasferire dati in modo affidabile tra computer connessi in una rete.

La soluzione migliore sarebbe impostare regole sul firewall affinchè la comunicazione con 192.168.200.100 non avvenga e qualsiasi pacchetto bloccato.