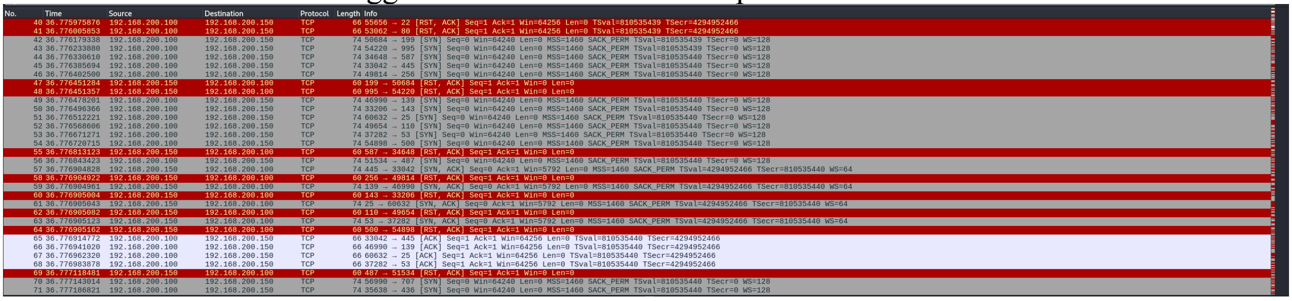
Analizziamo un report wireshark

All'interno del esercizio di oggi abbiamo analizzato un report di wireshark



```
No.  Time         Source           Destination      Protocol Length Info
  40 36.775975876 192.168.200.100  192.168.200.150  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  192.168.200.150  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  192.168.200.150  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  192.168.200.150  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  192.168.200.150  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  192.168.200.150  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  192.168.200.150  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  192.168.200.100  TCP      60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  48 36.776451357 192.168.200.150  192.168.200.100  TCP      60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  49 36.776478201 192.168.200.100  192.168.200.150  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  192.168.200.150  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  192.168.200.150  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  192.168.200.150  TCP      74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
  53 36.776671271 192.168.200.100  192.168.200.150  TCP      74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
  54 36.776720715 192.168.200.100  192.168.200.150  TCP      74 54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
  55 36.776813123 192.168.200.150  192.168.200.100  TCP      60 587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  56 36.776843423 192.168.200.100  192.168.200.150  TCP      74 51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
  57 36.776904828 192.168.200.150  192.168.200.100  TCP      74 445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
  58 36.776904922 192.168.200.150  192.168.200.100  TCP      60 256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  59 36.776904961 192.168.200.150  192.168.200.100  TCP      74 139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
  60 36.776905004 192.168.200.150  192.168.200.100  TCP      60 143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  61 36.776905043 192.168.200.150  192.168.200.100  TCP      74 25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
  62 36.776905082 192.168.200.150  192.168.200.100  TCP      60 110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  63 36.776905123 192.168.200.150  192.168.200.100  TCP      74 53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
  64 36.776905162 192.168.200.150  192.168.200.100  TCP      60 500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  65 36.776914772 192.168.200.100  192.168.200.150  TCP      66 33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
  66 36.776941020 192.168.200.100  192.168.200.150  TCP      66 46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
  67 36.776962320 192.168.200.100  192.168.200.150  TCP      66 60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
  68 36.776983878 192.168.200.100  192.168.200.150  TCP      66 37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
  69 36.777118481 192.168.200.150  192.168.200.100  TCP      60 487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  70 36.777143014 192.168.200.100  192.168.200.150  TCP      74 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
  71 36.777186821 192.168.200.100  192.168.200.150  TCP      74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
```

all'interno di questo report possiamo vedere varie richieste tcp che indicano una probabile scansione.

Per rimediare a questo attacco possiamo impostare delle regole di firewal che bloccano l'indirizzo ip del attaccante, impedendo cosi di acquisire informazioni sullo stato delle porte del sistema.