



# THREAT INTELLIGENCE & IOC



MICHELANGELO BORROMEO

# TRACCIA



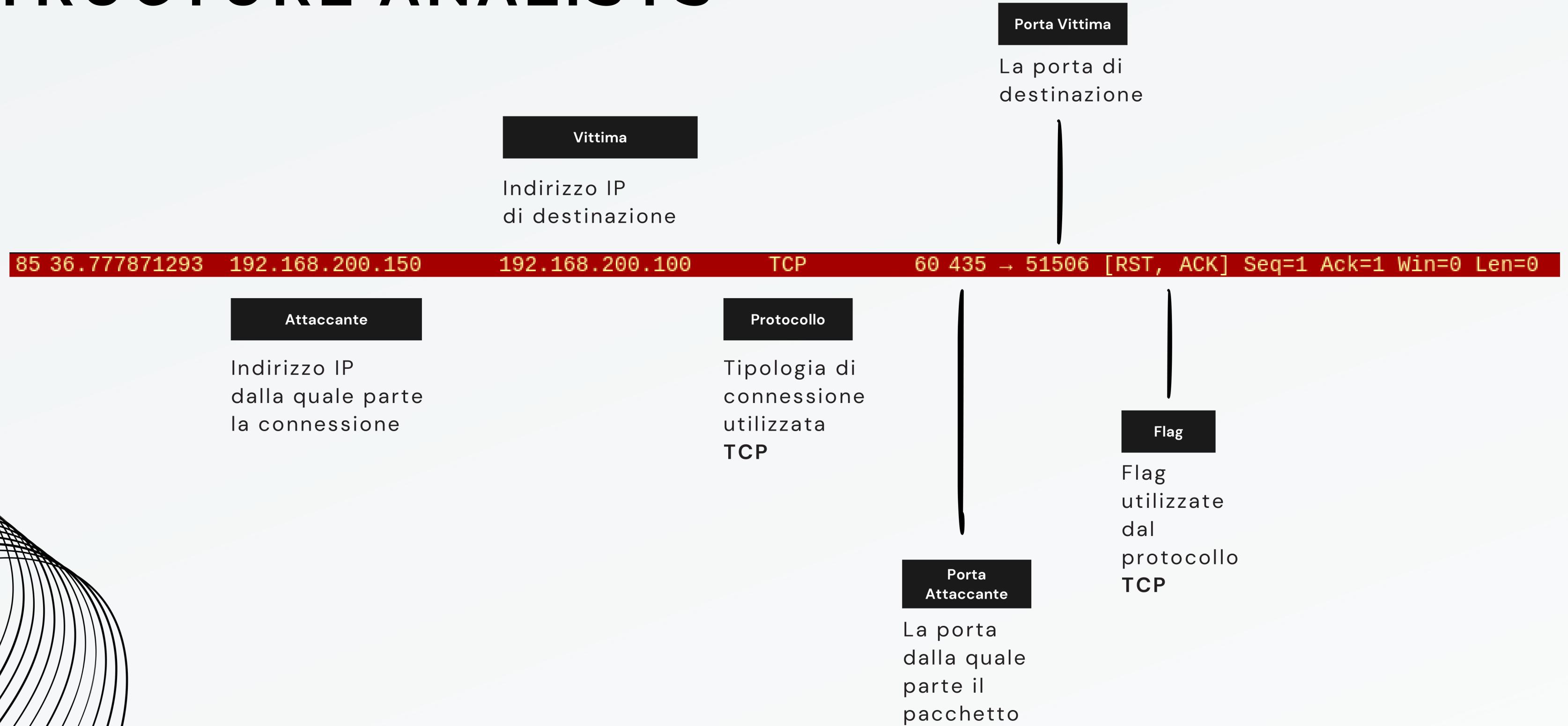
- 1) Identificare eventuali IOC,  
ovvero evidenze di attacchi in  
corso in base agli IOC trovati.**
- 2) fate delle ipotesi sui  
potenziali vettori di attacco  
utilizzati**
- 3) Consigliare un'azione per  
ridurre gli impatti dell'attacco**



# WIRESHARK

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 85 36.777871293 192.168.200.150 192.168.200.100 TCP 69 435 - 51566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 86 36.777893298 192.168.200.100 192.168.200.150 TCP 69 33042 - 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535441 Tscr=4294952460 | 87 36.777912171 192.168.200.100 192.168.200.150 TCP 69 46990 - 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535441 Tscr=4294952466 | 88 36.777986759 192.168.200.100 192.168.200.150 TCP 69 66032 - 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535441 Tscr=4294952466 | 89 36.778031360 192.168.200.100 192.168.200.150 TCP 69 66280 - 35 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535441 Tscr=4294952466 | 90 36.778045578 192.168.200.100 192.168.200.150 TCP 74 43169 - 140 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 91 36.778200161 192.168.200.100 192.168.200.150 TCP 74 48448 - 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535441 Tscr=0 WS=128 | 92 36.778367839 192.168.200.100 192.168.200.150 TCP 74 54566 - 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 93 36.778385846 192.168.200.100 192.168.200.150 TCP 69 148 - 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 94 36.778385948 192.168.200.100 192.168.200.150 TCP 69 808 - 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 95 36.778449494 192.168.200.100 192.168.200.150 TCP 69 221 - 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 96 36.778482798 192.168.200.100 192.168.200.150 TCP 74 42426 - 1097 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 97 36.778500069 192.168.200.100 192.168.200.150 TCP 74 43188 - 1098 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 98 36.778614895 192.168.200.100 192.168.200.150 TCP 74 54296 - 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 99 36.778663864 192.168.200.100 192.168.200.150 TCP 69 1807 - 42428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 100 36.778721088 192.168.200.100 192.168.200.150 TCP 69 291 - 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 101 36.778759638 192.168.200.100 192.168.200.150 TCP 74 40318 - 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 102 36.778781327 192.168.200.100 192.168.200.150 TCP 74 51276 - 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 103 36.778826294 192.168.200.100 192.168.200.150 TCP 69 131 - 54282 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 104 36.778864498 192.168.200.100 192.168.200.150 TCP 69 39562 - 896 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 105 36.778870537 192.168.200.100 192.168.200.150 TCP 69 4082 - 4082 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 106 36.778893427 192.168.200.100 192.168.200.150 TCP 69 677 - 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 107 36.778983153 192.168.200.100 192.168.200.150 TCP 74 4238 - 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 108 36.779029210 192.168.200.100 192.168.200.150 TCP 69 858 - 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 109 36.779055240 192.168.200.100 192.168.200.150 TCP 74 55542 - 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 110 36.779122299 192.168.200.100 192.168.200.150 TCP 69 84 - 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 111 36.779165868 192.168.200.100 192.168.200.150 TCP 74 49138 - 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535442 Tscr=0 WS=128 | 112 36.779200004 192.168.200.100 192.168.200.150 TCP 69 109 - 56012 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 113 36.779275761 192.168.200.100 192.168.200.150 TCP 74 45148 - 216 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535443 Tscr=0 WS=128 | 114 36.779308462 192.168.200.100 192.168.200.150 TCP 74 46888 - 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535443 Tscr=0 WS=128 | 115 36.779354560 192.168.200.100 192.168.200.150 TCP 69 938 - 49138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 116 36.779378633 192.168.200.100 192.168.200.150 TCP 74 50268 - 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535443 Tscr=0 WS=128 | 117 36.779397023 192.168.200.100 192.168.200.150 TCP 74 51260 - 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535443 Tscr=0 WS=128 | 118 36.77965648 192.168.200.100 192.168.200.150 TCP 69 214 - 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 241 36.788094793 192.168.200.100 192.168.200.150 TCP 69 709 - 59932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 242 36.788094793 192.168.200.100 192.168.200.150 TCP 69 234 - 59932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 243 36.788117848 192.168.200.100 192.168.200.150 TCP 74 36266 - 180 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535451 Tscr=0 WS=128 | 244 36.788153892 192.168.200.100 192.168.200.150 TCP 74 51844 - 855 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535451 Tscr=0 WS=128 | 245 36.788170982 192.168.200.100 192.168.200.150 TCP 74 45726 - 232 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535451 Tscr=0 WS=128 | 246 36.788186532 192.168.200.100 192.168.200.150 TCP 74 52724 - 904 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535451 Tscr=0 WS=128 | 247 36.788298677 192.168.200.100 192.168.200.150 TCP 74 49489 - 835 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=0 WS=128 | 248 36.788300761 192.168.200.100 192.168.200.150 TCP 74 40998 - 602 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=0 WS=128 | 249 36.788373483 192.168.200.100 192.168.200.150 TCP 74 54196 - 291 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=0 WS=128 | 250 36.78843559 192.168.200.100 192.168.200.150 TCP 69 709 - 59946 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 251 36.78844356 192.168.200.100 192.168.200.150 TCP 69 271 - 44414 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 252 36.788443696 192.168.200.100 192.168.200.150 TCP 69 470 - 50612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 253 36.788443736 192.168.200.100 192.168.200.150 TCP 69 180 - 36266 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 254 36.788443776 192.168.200.100 192.168.200.150 TCP 69 855 - 51844 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 255 36.788443816 192.168.200.100 192.168.200.150 TCP 69 232 - 45726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 256 36.788443857 192.168.200.100 192.168.200.150 TCP 69 904 - 52724 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 257 36.788443896 192.168.200.100 192.168.200.150 TCP 69 835 - 49489 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 258 36.788490564 192.168.200.100 192.168.200.150 TCP 69 602 - 41098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 259 36.788490603 192.168.200.100 192.168.200.150 TCP 69 291 - 54196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 260 36.788511938 192.168.200.100 192.168.200.150 TCP 74 48350 - 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=0 WS=128 | 261 36.788567765 192.168.200.100 192.168.200.150 TCP 74 36542 - 773 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=0 WS=128 | 262 36.788600279 192.168.200.100 192.168.200.150 TCP 74 51396 - 514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=0 WS=128 | 263 36.788677629 192.168.200.100 192.168.200.150 TCP 74 56758 - 224 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=0 WS=128 | 264 36.788716758 192.168.200.100 192.168.200.150 TCP 74 48824 - 183 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=0 WS=128 | 265 36.788805799 192.168.200.100 192.168.200.150 TCP 69 956 - 48350 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 266 36.788805893 192.168.200.100 192.168.200.150 TCP 69 773 - 36542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 267 36.788865940 192.168.200.100 192.168.200.150 TCP 74 514 - 51396 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=4294952467 | 268 36.788833247 192.168.200.100 192.168.200.150 TCP 69 51396 - 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535452 Tscr=4294952467 | 269 36.788954711 192.168.200.100 192.168.200.150 TCP 69 224 - 56758 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 270 36.789081811 192.168.200.100 192.168.200.150 TCP 74 48182 - 361 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535452 Tscr=0 WS=128 | 271 36.789234182 192.168.200.100 192.168.200.150 TCP 69 183 - 48824 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 272 36.789378458 192.168.200.100 192.168.200.150 TCP 69 361 - 40182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 273 36.789681130 192.168.200.100 192.168.200.150 TCP 69 51396 - 514 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535453 Tscr=4294952467 | 274 36.789840070 192.168.200.100 192.168.200.150 TCP 74 36046 - 617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535453 Tscr=0 WS=128 | 275 36.789887828 192.168.200.100 192.168.200.150 TCP 74 34868 - 62 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535453 Tscr=0 WS=128 | 276 36.790032784 192.168.200.100 192.168.200.150 TCP 69 617 - 36646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 277 36.798962742 192.168.200.100 192.168.200.150 TCP 74 47728 - 8 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535453 Tscr=0 WS=128 | 278 36.790152859 192.168.200.100 192.168.200.150 TCP 69 62 - 34868 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 279 36.790152966 192.168.200.100 192.168.200.150 TCP 69 8 - 47729 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 | 280 36.790171430 192.168.200.100 192.168.200.150 TCP 74 37560 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535453 Tscr=0 WS=128 | 281 36.790198841 192.168.200.100 192.168.200.150 TCP 74 58384 - 121 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK\_PERM Tsv=810535453 Tscr=0 WS=128 | 282 36.790247212 192.168.200.100 192.168. |

# WIRESHARK PACKET STRUCTURE ANALYSIS



# IOC ANALISYS

## (INDICATOR OF COMPROMISSION)

86 36.777893298 192.168.200.100 → 192.168.200.150 TCP 66 33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466  
87 36.777912717 192.168.200.100 → 192.168.200.150 TCP 66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466  
88 36.777986759 192.168.200.100 → 192.168.200.150 TCP 66 60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466  
89 36.778031265 192.168.200.100 → 192.168.200.150 TCP 66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466

L'IP 192.168.200.150 sta inviando una serie di pacchetti con i flag RST e ACK all'IP 192.168.200.100.

RST = Questo flag indica che la connessione deve essere terminata immediatamente. Viene solitamente inviato quando un pacchetto viene ricevuto su una connessione che non esiste più o non è mai esistita. È una sorta di messaggio di errore che dice "termina questa connessione".

ACK = Questo flag viene utilizzato per riconoscere la ricezione di pacchetti nel protocollo TCP.

Una quantità enorme di richieste Syn potrebbe esaurire le risorse di memoria della macchina bersaglio, di conseguenza potrebbe portare un rallentamento del sistema o al blocco completo rendendo la macchina incapace di gestire le nuove connessioni legittime.

Il che pensare che sia un attacco DoS ovvero Denial of Service

# RIDUZIONE IMPATTO

## Firewall

Utilizzare un firewall per limitare il numero di nuove connessioni da una singola origine. Questo può prevenire che un singolo attaccante sovraccarichi il server.

## Reverse Proxy

Utilizzare un reverse proxy per filtrare il traffico prima che raggiunga il server principale.

## IDS/IPS

Implementare sistemi di rilevamento e prevenzione delle intrusioni che possono identificare e bloccare automaticamente il traffico sospetto.

