

Progetto S9-L3

Studente: Simone Mininni

Task: Identificare eventuali eventi, segnali di compromissione attraverso il network monitoring con wireshark

Evidenze di attacchi in corso:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|--|
| 31 | 36.775524204 | 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 TSecr=0 WS= |
| 32 | 36.775589806 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 33 | 36.775619454 | 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=4294952466 |
| 34 | 36.775652497 | 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=4294952466 |
| 35 | 36.775796938 | 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=4294952466 |
| 36 | 36.775797004 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 |
| 37 | 36.775803786 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 38 | 36.775813232 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 39 | 36.775861964 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 54 | 36.776728715 | 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= |
| 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= |
| 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 |
| 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 |

> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0

> Ethernet II, Src: PcsCompu_fd:87:1e (08:00:27:fd:87:1e), Dst: PcsCompu_39:7d:fe (08:00:27:39:7d:fe)

> Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100

> Transmission Control Protocol, Src Port: 80, Dst Port: 53060, Seq: 0, Ack: 1, Len: 0

0000 08 00 27 39 7d fe 08 00 27 fd 87 1e 08 00 45 00 ...9

0010 00 3c 00 00 40 00 06 28 70 c0 a8 c8 96 c0 a8 ...<

0020 c8 64 00 50 cf 44 4b ca dd 8c 2f d7 0e 60 a0 12 ...d P

0030 16 a0 5f 59 00 00 02 04 05 b4 04 02 08 0a ff ff ...Y

0040 c0 fd 30 4f 97 3b 01 03 03 06

Internet Protocol Version 4 (ip), 20 byte

Pacchetti: 2083 - visualizzati: 2083 (100.0%)

Profilo: Default

Dalla schermata di wireshark, possiamo notare una situazione insolita, ovvero più di mille pacchetti tcp inviati da uno stesso indirizzo ip(192.168.200.100) verso un range vasto di porte.

Inoltre le richieste sono effettuate in un range di tempo ristretto e la lunghezza dei pacchetti è uguale, ovvero 'len=0'.

Potenziati vettori di attacco:

Probabilmente la macchina attaccante(192.168.200.100) sta effettuando una scansione delle porte sul target(192.168.200.150).

Infatti se andiamo a filtrare i pacchetti notiamo un comportamento tipico della scansione full tcp.

Pacchetti syn inviati dall' attaccante:

| tcp.flags.syn == 1 and tcp.flags.ack == 0 | | | | | | | |
|---|--------------|-----------------|-----------------|----------|--------|-------------------|--|
| No. | Time | Source | Destination | Protocol | Length | Info | |
| 2 | 23.764214995 | 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 TSecr=0 WS= |
| 3 | 23.764287789 | 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 TSecr=0 WS= |
| 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 TSecr=0 WS= |
| 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 TSecr=0 WS= |
| 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 TSecr=0 WS= |
| 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 TSecr=0 WS= |
| 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 TSecr=0 WS= |
| 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 TSecr=0 WS= |
| 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 TSecr=0 WS= |
| 29 | 36.775337800 | 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 TSecr=0 WS= |
| 30 | 36.775386694 | 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 TSecr=0 WS= |
| 31 | 36.775524204 | 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 TSecr=0 WS= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 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= |
| 72 | 36.777302991 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 34120 → 98 [SYN] | Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS= |
| 73 | 36.777337934 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49780 → 78 [SYN] | Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS= |
| 76 | 36.777473018 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 36138 → 580 [SYN] | Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS= |

> Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150

▼ Transmission Control Protocol, Src Port: 41182, Dst Port: 21, Seq: 0, Len: 0

Source Port: 41182
Destination Port: 21
[Stream index: 8]
[Conversation completeness: Complete, NO_DATA (39)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1557656871
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 = Header Length: 40 bytes (10)

▼ Flags: 0x002 (SYN)

000. = Reserved: Not set
...0 = Accurate ECN: Not set
.... 0.... = Congestion Window Reduced: Not set

0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00 ...'9)..
0010 00 3c 53 f3 40 00 00 06 d4 7c c0 a8 c8 64 c0 a8 ...<S@ @ |...
0020 c8 96 a0 de 00 15 5c d7 f5 27 00 00 00 00 a0 02 ... \.....
0030 fa f0 12 7b 00 00 02 04 05 b4 04 02 08 0a 30 4f ...{.....
0040 ca 0e 00 00 00 00 01 03 03 07

The window size value from the TCP header (tcp.window_size_value), 2 byte

Pacchetti: 2083 - visualizzati: 1026 (49.3%)

Profilo: Default

n. pacchetti inviati: 1026 (si può presumere una scansione sulle common well known ports).

Risposta syn,ack da parte del target:

| tcp.flags.syn == 1 and tcp.flags.ack == 1 | | | | | | | |
|---|--------------|-----------------|-----------------|----------|--------|------------------------|---|
| Io. | Time | Source | Destination | Protocol | Length | Info | |
| 4 | 23.764777323 | 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=4294951165 TSecr= |
| 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=4294952466 TSecr= |
| 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=4294952466 TSecr= |
| 27 | 36.775141273 | 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=4294952466 TSecr= |
| 35 | 36.775796938 | 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=4294952466 TSecr= |
| 36 | 36.775797004 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 80 → 53062 [SYN, ACK] | Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr= |
| 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= |
| 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= |
| 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= |
| 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= |
| 164 | 36.781487210 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 512 → 45648 [SYN, ACK] | Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr= |
| 267 | 36.788805940 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 514 → 51396 [SYN, ACK] | Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr= |
| 994 | 36.825722553 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 513 → 42048 [SYN, ACK] | Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr= |

n. porte aperte: 13. Il target ha risposto confermando che la porta è aperta, mentre dal primo screenshot si può notare una serie di risposte rst,ack confermando che la porta relativa è chiusa.

Risposta ack dell' attaccante:

tcp.flags.reset==0 and tcp.flags.ack == 1 and tcp.flags.syn==0

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|--|
| 6 | 23.764815289 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165 |
| 24 | 36.774700464 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 |
| 25 | 36.774711072 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 |
| 28 | 36.775174048 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 |
| 37 | 36.775803786 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 38 | 36.775813232 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 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 |
| 165 | 36.781512468 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466 |
| 268 | 36.788833247 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 51396 → 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535452 TSecr=4294952467 |
| 997 | 36.825733008 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 42048 → 513 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535489 TSecr=4294952471 |

L' attaccante chiude la connessione tcp inviando il pacchetto di ack.

Azioni di rimedio:

Per ridurre i tentativi di attacco, si potrebbe impostare una regola sul firewall per bloccare le connessioni con la macchina attaccante(192.168.200.100).

Inoltre si potrebbero bloccare le porte su cui sono esposti servizi critici, dove un eventuale exploit su questi comporterebbe un danno importante per l'azienda.