

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------------|-------------------|-----------|--------|--|
| 1 | 0.00000000 | 192.168.200.100 | 192.168.200.255 | BROADCAST | 288 | Hell's Announcement: NetASPI01014B15_Vorstellung_Schwermetall_Monitoring_Server_@_Kont_Server_@_NT_Workstation_@_NT_Server_Potential |
| 2 | 23.764214995 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 539060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128 |
| 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=128 |
| 4 | 23.764777323 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 80 → 539060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64 |
| 5 | 23.764777427 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 6 | 23.764815289 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 539060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165 |
| 7 | 23.764899991 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 539060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165 |
| 8 | 28.761629461 | PcsCompu_39:7d:fe | PcsCompu_39:7d:fe | ARP | 60 | Who has 192.168.200.100? Tell 192.168.200.150 |
| 9 | 28.761644419 | PcsCompu_39:7d:fe | PcsCompu_39:7d:fe | ARP | 42 | 192.168.200.100 is at 08:00:27:39:7d:fe |
| 10 | 28.774852257 | PcsCompu_39:7d:fe | PcsCompu_39:7d:fe | ARP | 42 | Who has 192.168.200.150? Tell 192.168.200.100 |
| 11 | 28.775236989 | PcsCompu_39:7d:fe | PcsCompu_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 | 41394 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128 |
| 13 | 36.774218116 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 50120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128 |
| 14 | 36.774257841 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128 |
| 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=128 |
| 16 | 36.774495627 | 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=128 |
| 17 | 36.774535534 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128 |
| 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=128 |
| 19 | 36.774685505 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 23 → 41394 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64 |
| 20 | 36.774685652 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 111 → 50120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64 |
| 21 | 36.774685696 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 22 | 36.774685737 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 954 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 23 | 36.774685776 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 24 | 36.774700464 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 41394 → 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 | 60 | 50120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 |
| 26 | 36.775141104 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 993 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 27 | 36.775141124 | 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=810535438 WS=64 |
| 28 | 36.775174048 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 |
| 29 | 36.775337806 | 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=128 |
| 30 | 36.775386694 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 59556 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128 |
| 31 | 36.775524204 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 539062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128 |

a) Identificare eventuali IOC, ovvero evidenze di attacchi in corso

Analizzando la cattura di rete effettuata con Wireshark, si può notare come ci siano delle **richieste TCP ripetute**, che rappresentano IOC.

b) In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

L'attaccante 192.168.200.100 potrebbe **star scansionando il target** 192.168.200.150, in quanto dalla cattura notiamo che ci sono un numero elevato di richieste TCP (SYN) su porte sempre diverse di destinazione. L'ipotesi dello scansionamento è supportata dal fatto che per alcune righe della cattura si notano risposte positive del target (ovvero [SYN+ACK]) ad indicare che la porta è aperta. Per altre, invece, notiamo che la risposta (ovvero [RST+ACK]) va ad indicare che la porta è chiusa.

c) Consigliate un'azione per ridurre gli impatti dell'attacco

Si potrebbero **configurare le regole del firewall** in maniera tale da bloccare l'accesso a tutte le porte all'attaccante 192.168.200.100, in modo tale da evitare che informazioni riguardanti la porta e i servizi in ascolto finiscano nelle mani dell'attaccante.