

The background is a dark blue gradient with a subtle pattern of white dots. Overlaid on the left side are several concentric circles and arcs, some with degree markings (40, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, 260) and arrows, suggesting a circular or rotational theme.

THREAT INTELLIGENCE & IOC

ESERCIZIO S9/L3

ANALIZZIAMO LA CATTURA DI RETE UTILIZZANDO WIRESHARK (UTILIZZIAMO IL DOCUMENTO IN ALLEGATO)



Cattura_U3_W1_L3.pcapng

Cattura_U3_W1_L3.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp.flags.ack and tcp.flags.syn						
No.	Time	Source	Destination	Protocol	Length	Info
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 → 41304 [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 → 56120 [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 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 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	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
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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=810535438 WS=64
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
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=128
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=128
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=128
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 TSecr=810535439 WS=64
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=810535439 WS=64
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=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

Dai pacchetti che vediamo si nota subito che è stato eseguito un tentativo di connessione visto che ci sono numerose richieste TCP(SYN) su varie porte, per alcune ci sono state risposte positive (SYN+ACK) dove la porta era aperta e altre invece con una risposta (RST+ACK) che indicano le porte che sono chiuse.

Ci spostiamo nella path Statistics > Protocol > Conversation per poter controllare tutte le informazioni sui protocolli in modo più dettagliato. Qui vediamo che vengono inviati pacchetti TCP a tutte le porte fino alla porta 1024, ci fa capire che è in corso una port scanning. Tuttavia le porte sono quasi tutte chiuse perché il three-way-handshake non viene completato.

Wireshark - Conversations - Cattura_U3_W1_L3.pcapng

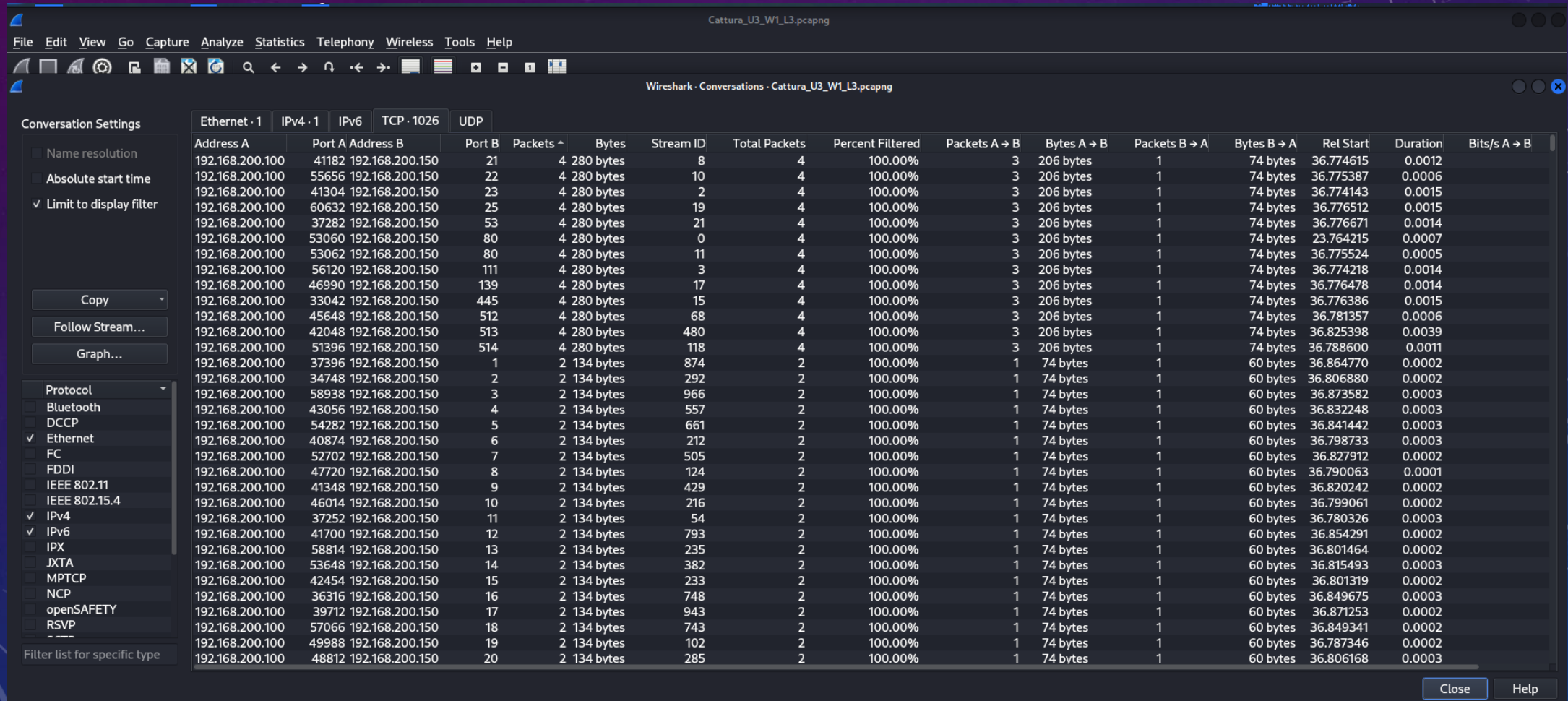
Conversation Settings

- ☐ Name resolution
- ☐ Absolute start time
- ☒ Limit to display filter
- Copy
- Follow Stream...
- Graph...
- Protocol
 - ☐ Bluetooth
 - ☐ DCCP
 - ☒ Ethernet
 - ☐ FC
 - ☐ FDDI
 - ☐ IEEE 802.11
 - ☐ IEEE 802.15.4
 - ☒ IPv4
 - ☒ IPv6
 - ☐ IPX
 - ☐ JXTA
 - ☐ MPTCP
 - ☐ NCP
 - ☐ openSAFETY
 - ☐ RSVP
 - ☐ ---
- Filter list for specific type

Ethernet · 1	IPv4 · 1	IPv6	TCP · 1026	UDP											
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	4	100.00%	3	206 bytes	1	74 bytes	36.774615	0.0012	
192.168.200.100	55656	192.168.200.150	22	4	280 bytes	10	4	100.00%	3	206 bytes	1	74 bytes	36.775387	0.0006	
192.168.200.100	41304	192.168.200.150	23	4	280 bytes	2	4	100.00%	3	206 bytes	1	74 bytes	36.774143	0.0015	
192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	4	100.00%	3	206 bytes	1	74 bytes	36.776512	0.0015	
192.168.200.100	37282	192.168.200.150	53	4	280 bytes	21	4	100.00%	3	206 bytes	1	74 bytes	36.776671	0.0014	
192.168.200.100	53060	192.168.200.150	80	4	280 bytes	0	4	100.00%	3	206 bytes	1	74 bytes	23.764215	0.0007	
192.168.200.100	53062	192.168.200.150	80	4	280 bytes	11	4	100.00%	3	206 bytes	1	74 bytes	36.775524	0.0005	
192.168.200.100	56120	192.168.200.150	111	4	280 bytes	3	4	100.00%	3	206 bytes	1	74 bytes	36.774218	0.0014	
192.168.200.100	46990	192.168.200.150	139	4	280 bytes	17	4	100.00%	3	206 bytes	1	74 bytes	36.776478	0.0014	
192.168.200.100	33042	192.168.200.150	445	4	280 bytes	15	4	100.00%	3	206 bytes	1	74 bytes	36.776386	0.0015	
192.168.200.100	45648	192.168.200.150	512	4	280 bytes	68	4	100.00%	3	206 bytes	1	74 bytes	36.781357	0.0006	
192.168.200.100	42048	192.168.200.150	513	4	280 bytes	480	4	100.00%	3	206 bytes	1	74 bytes	36.825398	0.0039	
192.168.200.100	51396	192.168.200.150	514	4	280 bytes	118	4	100.00%	3	206 bytes	1	74 bytes	36.788600	0.0011	
192.168.200.100	37396	192.168.200.150	1	2	134 bytes	874	2	100.00%	1	74 bytes	1	60 bytes	36.864770	0.0002	
192.168.200.100	34748	192.168.200.150	2	2	134 bytes	292	2	100.00%	1	74 bytes	1	60 bytes	36.806880	0.0002	
192.168.200.100	58938	192.168.200.150	3	2	134 bytes	966	2	100.00%	1	74 bytes	1	60 bytes	36.873582	0.0003	
192.168.200.100	43056	192.168.200.150	4	2	134 bytes	557	2	100.00%	1	74 bytes	1	60 bytes	36.832248	0.0003	
192.168.200.100	54282	192.168.200.150	5	2	134 bytes	661	2	100.00%	1	74 bytes	1	60 bytes	36.841442	0.0003	
192.168.200.100	40874	192.168.200.150	6	2	134 bytes	212	2	100.00%	1	74 bytes	1	60 bytes	36.798733	0.0003	
192.168.200.100	52702	192.168.200.150	7	2	134 bytes	505	2	100.00%	1	74 bytes	1	60 bytes	36.827912	0.0002	
192.168.200.100	47720	192.168.200.150	8	2	134 bytes	124	2	100.00%	1	74 bytes	1	60 bytes	36.790063	0.0001	
192.168.200.100	41348	192.168.200.150	9	2	134 bytes	429	2	100.00%	1	74 bytes	1	60 bytes	36.820242	0.0002	
192.168.200.100	46014	192.168.200.150	10	2	134 bytes	216	2	100.00%	1	74 bytes	1	60 bytes	36.799061	0.0002	
192.168.200.100	37252	192.168.200.150	11	2	134 bytes	54	2	100.00%	1	74 bytes	1	60 bytes	36.780326	0.0003	
192.168.200.100	41700	192.168.200.150	12	2	134 bytes	793	2	100.00%	1	74 bytes	1	60 bytes	36.854291	0.0002	
192.168.200.100	58814	192.168.200.150	13	2	134 bytes	235	2	100.00%	1	74 bytes	1	60 bytes	36.801464	0.0002	
192.168.200.100	53648	192.168.200.150	14	2	134 bytes	382	2	100.00%	1	74 bytes	1	60 bytes	36.815493	0.0003	
192.168.200.100	42454	192.168.200.150	15	2	134 bytes	233	2	100.00%	1	74 bytes	1	60 bytes	36.801319	0.0002	
192.168.200.100	36316	192.168.200.150	16	2	134 bytes	748	2	100.00%	1	74 bytes	1	60 bytes	36.849675	0.0003	
192.168.200.100	39712	192.168.200.150	17	2	134 bytes	943	2	100.00%	1	74 bytes	1	60 bytes	36.871253	0.0002	
192.168.200.100	57066	192.168.200.150	18	2	134 bytes	743	2	100.00%	1	74 bytes	1	60 bytes	36.849341	0.0002	
192.168.200.100	49988	192.168.200.150	19	2	134 bytes	102	2	100.00%	1	74 bytes	1	60 bytes	36.787346	0.0002	
192.168.200.100	48812	192.168.200.150	20	2	134 bytes	285	2	100.00%	1	74 bytes	1	60 bytes	36.806168	0.0003	

Close Help

Cambiando l'ordine dei pacchetti in modo decrescente, vediamo che quelli con 4 pacchetti, sono tutte le porte dove è stato completato il three-way-handshake. Siamo quindi certi di aver tracciato un tentativo di port scanning eseguito sulla macchina 192.168.200.100 verso la macchina Meta dove sono state individuate 13 porte aperte.



Wireshark - Conversations - Cattura_U3_W1_L3.pcapng

Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	4	100.00%	3	206 bytes	1	74 bytes	36.774615	0.0012	
192.168.200.100	55656	192.168.200.150	22	4	280 bytes	10	4	100.00%	3	206 bytes	1	74 bytes	36.775387	0.0006	
192.168.200.100	41304	192.168.200.150	23	4	280 bytes	2	4	100.00%	3	206 bytes	1	74 bytes	36.774143	0.0015	
192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	4	100.00%	3	206 bytes	1	74 bytes	36.776512	0.0015	
192.168.200.100	37282	192.168.200.150	53	4	280 bytes	21	4	100.00%	3	206 bytes	1	74 bytes	36.776671	0.0014	
192.168.200.100	53060	192.168.200.150	80	4	280 bytes	0	4	100.00%	3	206 bytes	1	74 bytes	23.764215	0.0007	
192.168.200.100	53062	192.168.200.150	80	4	280 bytes	11	4	100.00%	3	206 bytes	1	74 bytes	36.775524	0.0005	
192.168.200.100	56120	192.168.200.150	111	4	280 bytes	3	4	100.00%	3	206 bytes	1	74 bytes	36.774218	0.0014	
192.168.200.100	46990	192.168.200.150	139	4	280 bytes	17	4	100.00%	3	206 bytes	1	74 bytes	36.776478	0.0014	
192.168.200.100	33042	192.168.200.150	445	4	280 bytes	15	4	100.00%	3	206 bytes	1	74 bytes	36.776386	0.0015	
192.168.200.100	45648	192.168.200.150	512	4	280 bytes	68	4	100.00%	3	206 bytes	1	74 bytes	36.781357	0.0006	
192.168.200.100	42048	192.168.200.150	513	4	280 bytes	480	4	100.00%	3	206 bytes	1	74 bytes	36.825398	0.0039	
192.168.200.100	51396	192.168.200.150	514	4	280 bytes	118	4	100.00%	3	206 bytes	1	74 bytes	36.788600	0.0011	
192.168.200.100	37396	192.168.200.150	1	2	134 bytes	874	2	100.00%	1	74 bytes	1	60 bytes	36.864770	0.0002	
192.168.200.100	34748	192.168.200.150	2	2	134 bytes	292	2	100.00%	1	74 bytes	1	60 bytes	36.806880	0.0002	
192.168.200.100	58938	192.168.200.150	3	2	134 bytes	966	2	100.00%	1	74 bytes	1	60 bytes	36.873582	0.0003	
192.168.200.100	43056	192.168.200.150	4	2	134 bytes	557	2	100.00%	1	74 bytes	1	60 bytes	36.832248	0.0003	
192.168.200.100	54282	192.168.200.150	5	2	134 bytes	661	2	100.00%	1	74 bytes	1	60 bytes	36.841442	0.0003	
192.168.200.100	40874	192.168.200.150	6	2	134 bytes	212	2	100.00%	1	74 bytes	1	60 bytes	36.798733	0.0003	
192.168.200.100	52702	192.168.200.150	7	2	134 bytes	505	2	100.00%	1	74 bytes	1	60 bytes	36.827912	0.0002	
192.168.200.100	47720	192.168.200.150	8	2	134 bytes	124	2	100.00%	1	74 bytes	1	60 bytes	36.790063	0.0001	
192.168.200.100	41348	192.168.200.150	9	2	134 bytes	429	2	100.00%	1	74 bytes	1	60 bytes	36.820242	0.0002	
192.168.200.100	46014	192.168.200.150	10	2	134 bytes	216	2	100.00%	1	74 bytes	1	60 bytes	36.799061	0.0002	
192.168.200.100	37252	192.168.200.150	11	2	134 bytes	54	2	100.00%	1	74 bytes	1	60 bytes	36.780326	0.0003	
192.168.200.100	41700	192.168.200.150	12	2	134 bytes	793	2	100.00%	1	74 bytes	1	60 bytes	36.854291	0.0002	
192.168.200.100	58814	192.168.200.150	13	2	134 bytes	235	2	100.00%	1	74 bytes	1	60 bytes	36.801464	0.0002	
192.168.200.100	53648	192.168.200.150	14	2	134 bytes	382	2	100.00%	1	74 bytes	1	60 bytes	36.815493	0.0003	
192.168.200.100	42454	192.168.200.150	15	2	134 bytes	233	2	100.00%	1	74 bytes	1	60 bytes	36.801319	0.0002	
192.168.200.100	36316	192.168.200.150	16	2	134 bytes	748	2	100.00%	1	74 bytes	1	60 bytes	36.849675	0.0003	
192.168.200.100	39712	192.168.200.150	17	2	134 bytes	943	2	100.00%	1	74 bytes	1	60 bytes	36.871253	0.0002	
192.168.200.100	57066	192.168.200.150	18	2	134 bytes	743	2	100.00%	1	74 bytes	1	60 bytes	36.849341	0.0002	
192.168.200.100	49988	192.168.200.150	19	2	134 bytes	102	2	100.00%	1	74 bytes	1	60 bytes	36.787346	0.0002	
192.168.200.100	48812	192.168.200.150	20	2	134 bytes	285	2	100.00%	1	74 bytes	1	60 bytes	36.806168	0.0003	

Adottare le azioni necessarie per ridurre gli impatti degli attacchi futuri:

- Configuriamo un Firewall in grado di rilevare e bloccare le connessioni quando c'è una quantità di richieste TCP elevata.
- Per limitare l'accesso, lasciamo accessibili solo le porte necessarie, chiudiamo quelle che non vengono utilizzate.
- Eseguiamo sempre un sistema di monitoraggio per poter identificare le attività sospette e altri port scanning.
- Cercare di avere le password aggiornate e sicure per gli account.

Rispondiamo ai seguenti quesiti una volta finita la nostra analisi:

- ✓ identificare eventuali IOC, evidenze di attacchi in corso In base agli IOC trovati
 - ✓ fare delle ipotesi sui potenziali vettori di attacco utilizzati
 - ✓ consigliare un'azione per ridurre gli impatti dell'attacco