

Consegna 11 ottobre

Analizzando i dati catturati con Wireshark, l'IP 192.168.200.100 sembra effettuare connessioni TCP verso varie porte dell'IP 192.168.200.150, che si trova nella stessa rete. Tuttavia, l'IP sorgente interrompe la connessione dopo la risposta del server, senza completare il "three-way handshake" TCP, suggerendo una scansione di porte con SYN Scan (Half-Open Scan) tramite Nmap (opzione -sS).

Questa tecnica consiste nell'inviare un pacchetto SYN per iniziare la connessione, ma senza completarla, riducendo così la probabilità di rilevamento da parte di sistemi di sicurezza. L'attaccante può ottenere informazioni sulle porte aperte consumando poche risorse e lasciando tracce minime nei log di rete. Ad esempio, un tentativo di connessione alla porta 21 mostra l'invio di SYN, la risposta del server con SYN/ACK, e poi la chiusura immediata della connessione con un pacchetto RST/ACK. L'attaccante può dedurre che il servizio sulla porta è attivo senza dover completare la connessione.

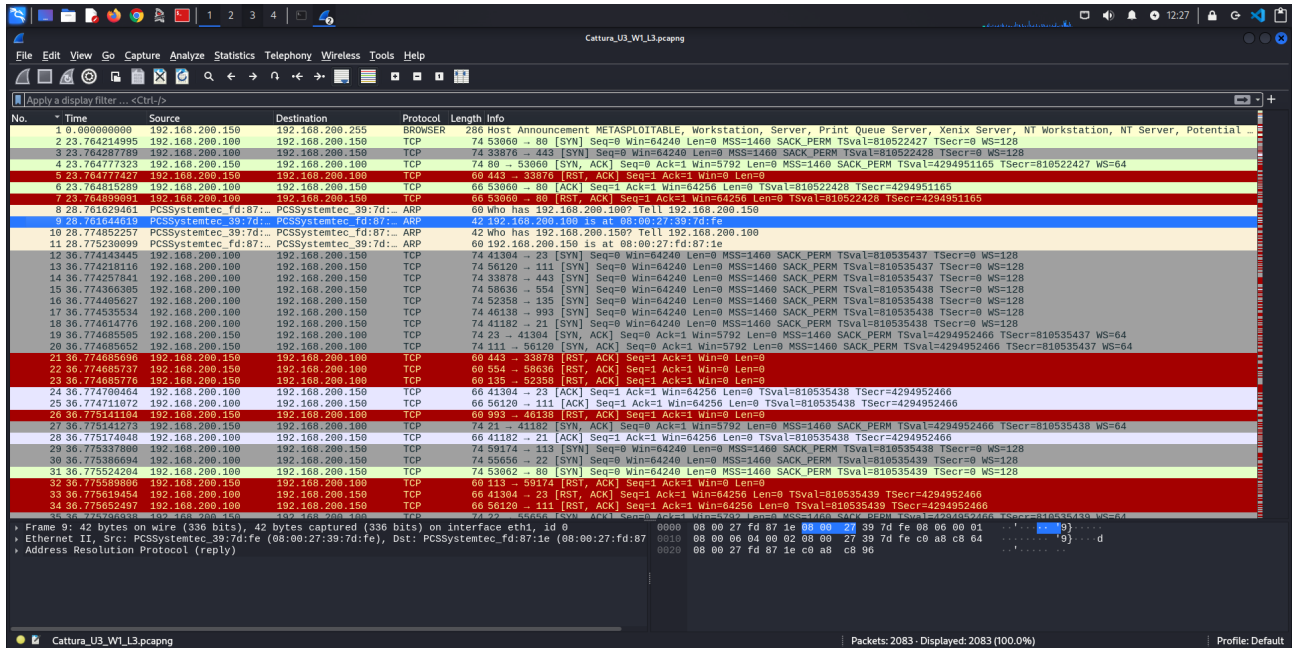
Azioni immediate per mitigare l'attacco:

1. **Monitorare il traffico di rete:** Usare strumenti per rilevare traffico anomalo, soprattutto per picchi di richieste SYN.
2. **Bloccare l'IP dell'attaccante:** Inserire regole nel firewall per bloccare l'indirizzo IP identificato.
3. **Aumentare il timeout delle richieste SYN:** Questo rallenta le scansioni rapide.
4. **Aggiornare e configurare i firewall:** Implementare protezioni contro le scansioni e limitare la velocità delle richieste.
- 5.

Azioni a lungo termine per prevenire attacchi futuri:

1. **Segmentare la rete:** Limitare l'accesso a risorse specifiche per ridurre l'efficacia delle scansioni.
2. **Implementare IDS/IPS:** Sistemi di rilevamento e prevenzione possono identificare e rispondere a scansioni in tempo reale.
3. **Formare il personale:** Educare i team IT sulle tecniche di scansione e sulle migliori pratiche di sicurezza.
4. **Applicare il rate limiting:** Limitare il numero di richieste SYN da un singolo IP in un intervallo di tempo.

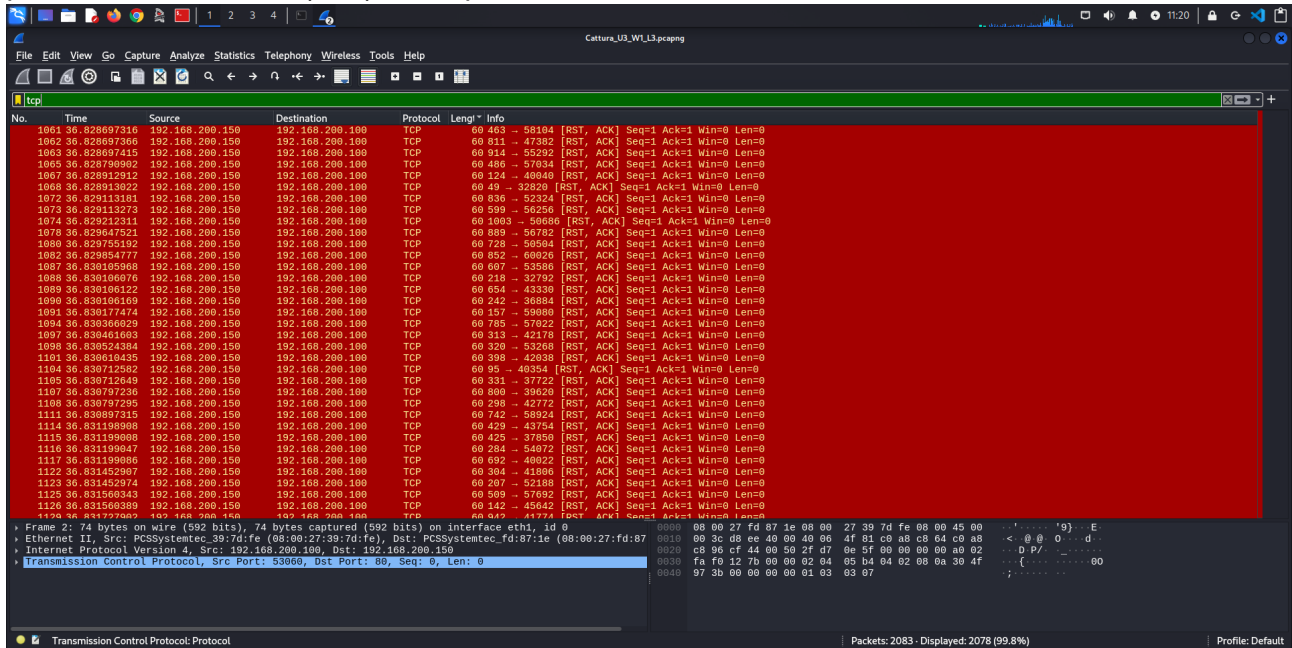
Questo è il primo risultato che esce fuori una volta che apro il file. Dopo averlo ordinato dalla colonna No. 1, noto che la prima riga restituisce l'IP source 192.168.200.150 che corrisponde a una macchina Metasploitable, la vittima di questo potenziale attacco. Le altre righe mostrano i vari pacchetti TCP in vari stati come SYN, ACK e RST, ogni stato rappresenta una fase diversa della comunicazione TCP.



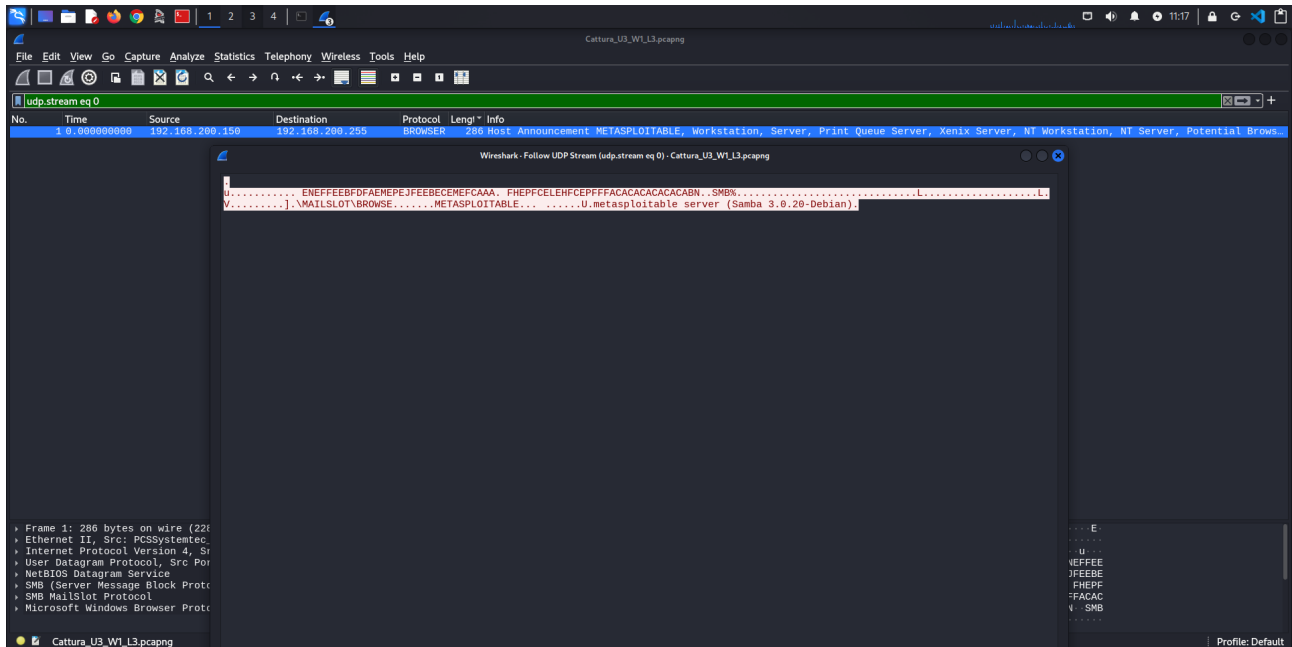
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential ...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=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 -> 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764777323	192.168.200.150	192.168.200.100	TCP	60	443 -> 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815298	192.168.200.100	192.168.200.150	TCP	60	53060 -> 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	53060 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PCSSystemtec.fid:87::	PCSSystemtec.39:7d::	ARP	60	who has 192.168.200.100? Tell 192.168.200.150
9	28.761641019	PCSSystemtec.39:7d::	PCSSystemtec.fid:87::	ARP	60	192.168.200.100 is at 08:00:27:fd:87:1e
10	28.774852257	PCSSystemtec.39:7d::	PCSSystemtec.fid:87::	ARP	42	who has 192.168.200.150? Tell 192.168.200.100
11	28.775230999	PCSSystemtec.fid:87::	PCSSystemtec.39:7d::	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774243445	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=128
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=128
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=128
15	36.774366395	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	36.774465027	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	46138 -> 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	36.774635595	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	36.774656552	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	36.774686990	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	36.774708464	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	36.774711872	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	36.775111104	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	36.775174848	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	36.775378989	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	59666 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524294	192.168.200.100	192.168.200.150	TCP	74	53662 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775599880	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

Frame 0: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth1, id 0 ...
Ethernet II, Src: PCSSystemtec.39:7d:fe (08:00:27:39:7d:fe), Dst: PCSSystemtec.fid:87:1e (08:00:27:fd:87:1e) ...
Address Resolution Protocol (reply) ...

Questo secondo screen mostra l'interfaccia di Wireshark con i pacchetti filtrati tramite tcp. Ho mostrato le righe in rosso con la Length 60 e la info in cui viene indicato che sono pacchetti di rete TCP (RST), usati per terminare bruscamente una connessione.



Poi ho filtrato per la porta UDP, trovando questo singolo risultato.



Poi sono andato su Statistics → Conversation, mi è uscita questa schermata, e dopo varie ricerche ho avuto modo di notare che i Packets numero 4 corrispondono alle porte aperte, quindi la 80,23,111,21,22...

Wireshark - Conversations - Cattura_U3_W1_L3.pcapng

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.200.100	53660	192.168.200.150	80	4	280 bytes	0	3	206 bytes	1	74 bytes	22.764215	0.0007		
192.168.200.100	41304	192.168.200.150	23	4	280 bytes	2	3	206 bytes	1	74 bytes	36.774143	0.0015		
192.168.200.100	56120	192.168.200.150	111	4	280 bytes	3	3	206 bytes	1	74 bytes	36.774218	0.0014		
192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	3	206 bytes	1	74 bytes	36.774615	0.0012		
192.168.200.100	55656	192.168.200.150	22	4	280 bytes	10	3	206 bytes	1	74 bytes	36.775387	0.0006		
192.168.200.100	53062	192.168.200.150	80	4	280 bytes	11	3	206 bytes	1	74 bytes	36.775524	0.0005		
192.168.200.100	33042	192.168.200.150	445	4	280 bytes	15	3	206 bytes	1	74 bytes	36.776386	0.0015		
192.168.200.100	46990	192.168.200.150	139	4	280 bytes	17	3	206 bytes	1	74 bytes	36.776478	0.0014		
192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	3	206 bytes	1	74 bytes	36.776512	0.0015		
192.168.200.100	37282	192.168.200.150	53	4	280 bytes	21	3	206 bytes	1	74 bytes	36.776671	0.0014		
192.168.200.100	45648	192.168.200.150	512	4	280 bytes	68	3	206 bytes	1	74 bytes	36.781357	0.0006		
192.168.200.100	51396	192.168.200.150	514	4	280 bytes	118	3	206 bytes	1	74 bytes	36.788600	0.0011		
192.168.200.100	42048	192.168.200.150	513	4	280 bytes	480	3	206 bytes	1	74 bytes	36.825398	0.0039		
192.168.200.100	33876	192.168.200.150	443	2	134 bytes	1	1	74 bytes	1	60 bytes	23.764288	0.0005		
192.168.200.100	33878	192.168.200.150	443	2	134 bytes	4	1	74 bytes	1	60 bytes	36.774258	0.0004		
192.168.200.100	58636	192.168.200.150	554	2	134 bytes	5	1	74 bytes	1	60 bytes	36.774366	0.0003		
192.168.200.100	52358	192.168.200.150	135	2	134 bytes	6	1	74 bytes	1	60 bytes	36.774406	0.0003		
192.168.200.100	40158	192.168.200.150	993	2	134 bytes	7	1	74 bytes	1	60 bytes	36.774536	0.0006		
192.168.200.100	59174	192.168.200.150	113	2	134 bytes	9	1	74 bytes	1	60 bytes	36.775338	0.0003		
192.168.200.100	50684	192.168.200.150	199	2	134 bytes	12	1	74 bytes	1	60 bytes	36.776179	0.0003		
192.168.200.100	54220	192.168.200.150	995	2	134 bytes	13	1	74 bytes	1	60 bytes	36.776234	0.0002		
192.168.200.100	34640	192.168.200.150	587	2	134 bytes	14	1	74 bytes	1	60 bytes	36.776331	0.0005		
192.168.200.100	49814	192.168.200.150	256	2	134 bytes	16	1	74 bytes	1	60 bytes	36.776403	0.0005		
192.168.200.100	33206	192.168.200.150	143	2	134 bytes	18	1	74 bytes	1	60 bytes	36.776496	0.0004		
192.168.200.100	49654	192.168.200.150	110	2	134 bytes	20	1	74 bytes	1	60 bytes	36.776569	0.0003		
192.168.200.100	54698	192.168.200.150	500	2	134 bytes	22	1	74 bytes	1	60 bytes	36.776721	0.0002		
192.168.200.100	51534	192.168.200.150	487	2	134 bytes	23	1	74 bytes	1	60 bytes	36.776843	0.0003		
192.168.200.100	56990	192.168.200.150	707	2	134 bytes	24	1	74 bytes	1	60 bytes	36.777143	0.0003		
192.168.200.100	35636	192.168.200.150	436	2	134 bytes	25	1	74 bytes	1	60 bytes	36.777187	0.0002		
192.168.200.100	34120	192.168.200.150	98	2	134 bytes	26	1	74 bytes	1	60 bytes	36.777203	0.0003		
192.168.200.100	49780	192.168.200.150	78	2	134 bytes	27	1	74 bytes	1	60 bytes	36.777338	0.0003		

Filter list for specific type

Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 53660, Dst Port: 80, Seq: 0, Len: 0

Transmission Control Protocol: Protocol

Packets: 2083 - Displayed: 2078 (99.8%)

Profile: Default

Qui ulteriori filtri TCP in cui sono mostrati i diversi pacchetti catturati. Vedendo più nel dettaglio, i rossi indicano TCP reset, i blu sono pacchetti di riconoscimento TCP (ACK) e quelli in verde sono pacchetti SYN.

Wireshark - Statistics - Packets - Cattura_U3_W1_L3.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
89	36.778831265	192.168.200.100	192.168.200.150	TCP	66	7282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 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
199	36.78199957	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
273	36.789861130	192.168.200.100	192.168.200.150	TCP	66	51396 → 514 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535453 Tsecr=4294952467
997	36.825733668	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
1079	36.829165224	192.168.200.100	192.168.200.150	TCP	66	42048 → 513 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535493 Tsecr=4294952471
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53660 → 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	192.168.200.100	192.168.200.150	TCP	74	80 → 53660 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 Tsecr=810522427 WS=64
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=810535487 Tsecr=0 WS=128
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=128
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=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	46138 → 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	36.774685595	192.168.200.100	192.168.200.150	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	192.168.200.100	192.168.200.150	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 Tsecr=810535437 WS=64
27	36.775141273	192.168.200.100	192.168.200.150	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 Tsecr=810535438 WS=64
29	36.775378689	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	36.775524264	192.168.200.100	192.168.200.150	TCP	74	53662 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 Tsecr=0 WS=128
38	36.775797098	192.168.200.100	192.168.200.150	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	36.775797094	192.168.200.100	192.168.200.150	TCP	74	80 → 53662 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 Tsecr=810535439 WS=64
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	98684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 Tsecr=0 WS=128
43	36.776233889	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	36.776338619	192.168.200.100	192.168.200.150	TCP	74	34648 → 597 [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	36.776492589	192.168.200.100	192.168.200.150	TCP	74	48914 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 Tsecr=0 WS=128
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	36.776586866	192.168.200.100	192.168.200.150	TCP	74	49654 → 118 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 Tsecr=0 WS=128
53	36.776619272	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

Filter list for specific type

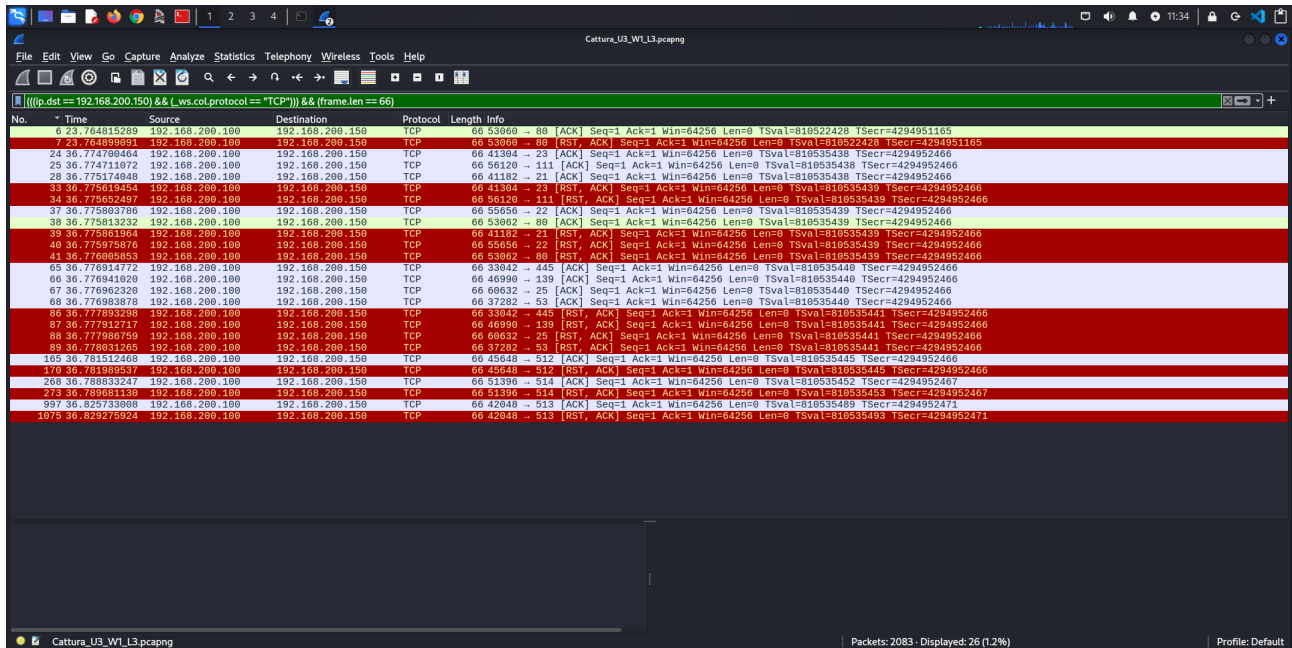
Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
Ethernet II, Src: PCSystemtec_38:7d:f6 (08:00:27:38:7d:f6), Dst: PCSystemtec_fd:87:1e (08:00:27:fd:87:1e)
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 53660, Dst Port: 80, Seq: 0, Len: 0

Cattura_U3_W1_L3.pcapng

Packets: 2083 - Displayed: 2078 (99.8%)

Profile: Default

Qui invece ho voluto filtrare solo per i protocolli TCP con destinazione 192.168.200.150 e con Length 66.



The image shows a Wireshark packet capture window titled "Cattura_U3_W1_L3.pcapng". The filter bar at the top contains the expression: `((ip.dst == 192.168.200.150) && (_ws.col.protocol == "TCP")) && (frame.len == 66)`. The packet list below shows 26 filtered packets, all of which are TCP segments with a length of 66 bytes. The packets are numbered 6 through 1075 in the list, with corresponding time, source, and destination IP addresses. The details pane for the selected packet (No. 6) shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53660 → 88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165

The status bar at the bottom indicates "Packets: 2083 - Displayed: 26 (1.2%)" and "Profile: Default".