Threat intelligence & IOC

S9 - L3

8	2022/221 09:59:28.655446952	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	2022/221 09:59:28.655462110	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	2022/221 09:59:28.668669748	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	2022/221 09:59:28.669047590	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
1	2022/221 09:58:59.893817491	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT
2	2022/221 09:59:23.658032486	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	2022/221 09:59:23.658105280	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	2022/221 09:59:23.658594814	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=
5	2022/221 09:59:23.658594918	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	2022/221 09:59:23.658632780	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
7	2022/221 09:59:23.658716582	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
12	2022/221 09:59:36.667960936	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	2022/221 09:59:36.668035607	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	2022/221 09:59:36.668075332	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	2022/221 09:59:36.668183796	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	2022/221 09:59:36.668223118	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	2022/221 09:59:36.668353025	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	2022/221 09:59:36.668432267	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	2022/221 09:59:36.668502996	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=

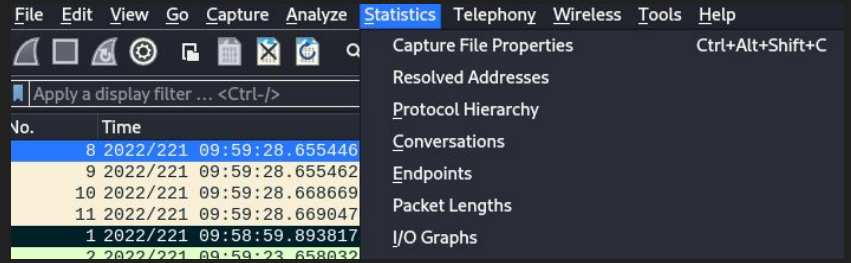
Questo è l'inizio della cattura, filtrata dai protocolli. I primi protocolli sono ARP, che fanno parte del processo di creazione delle comunicazioni su una rete. Possiamo vedere che ci sono 2 host rilevanti in questo screenshot, 192.168.200.100 e 192.168.200.150. Possiamo anche vedere i loro indirizzi MAC.

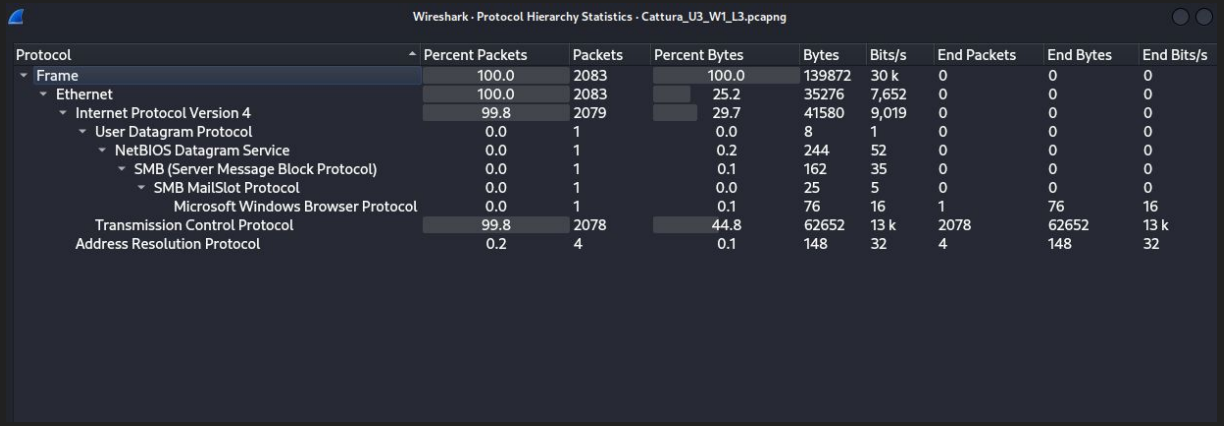
Dopo possiamo vedere che 192.168.200.150 ha inviato un pacchetto per essere broadcastato nella rete. Questo pacchetto ci dice che il host di nome METASPLOITABLE ha iniziato a fornire il servizio SMB, per stampare

8	2022/221 09:59:28.655446952	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	2022/221 09:59:28.655462110	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	2022/221 09:59:28.668669748	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	2022/221 09:59:28.669047590	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
1	2022/221 09:58:59.893817491	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT
2	2022/221 09:59:23.658032486	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	2022/221 09:59:23.658105280	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	2022/221 09:59:23.658594814	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=
5	2022/221 09:59:23.658594918	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	2022/221 09:59:23.658632780	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
7	2022/221 09:59:23.658716582	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
12	2022/221 09:59:36.667960936	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	2022/221 09:59:36.668035607	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	2022/221 09:59:36.668075332	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	2022/221 09:59:36.668183796	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	2022/221 09:59:36.668223118	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	2022/221 09:59:36.668353025	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	2022/221 09:59:36.668432267	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	2022/221 09:59:36.668502996	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=

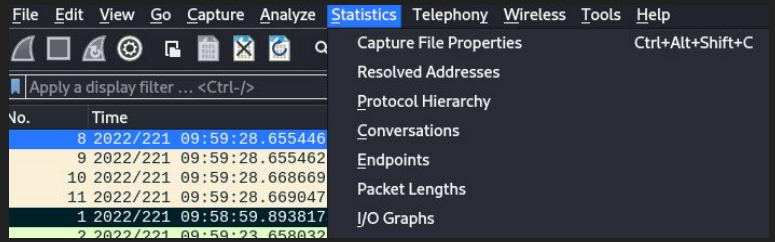
In questo screenshot possiamo vedere la prima di molte conversazioni TCP sospette. 192.168.200.100 invia un pacchetto SYN a 192.168.200.150, risponde con un ACK, 192.168.200.100 risponde con un SYN-ACK, quindi chiude la conversazione con REST-ACK.

Andando nella parte superiore dell'interfaccia utente, possiamo selezionare "Statistics" e quindi selezionare "Protocol Hierarchy". Una volta qui, puoi vedere che in questa acquisizione WireShark, il 99,8% dei pacchetti inviati sono TCP, il che indica che quanto visto in precedenza la conversazione è stata probabilmente ripetuta molte più volte.





Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	2083	100.0	139872	30 k	0	0	0
Ethernet	100.0	2083	25.2	35276	7,652	0	0	0
Internet Protocol Version 4	99.8	2079	29.7	41580	9,019	0	0	0
User Datagram Protocol	0.0	1	0.0	8	1	0	0	0
NetBIOS Datagram Service	0.0	1	0.2	244	52	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.1	162	35	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	5	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.1	76	16	1	76	16
Transmission Control Protocol	99.8	2078	44.8	62652	13 k	2078	62652	13 k
Address Resolution Protocol	0.2	4	0.1	148	32	4	148	32



Selezioniamo nuovamente "Statistics" e andiamo su "Conversations". Andiamo alle conversazioni TCP-1026 e clicchiamo per filtrare per porta.

Ci mette ogni conversazione fatta su ogni porta, e come vediamo ci ha stato una conversazione per ogni porta una per una. Questa è una prova inconfutabile che 192.168.200.100 è l'host di scansione delle porte 192.168.200.150 (Metasploitable).

Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 1026 | UDP · 1

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	37396	192.168.200.150	1	2	134 bytes	874	1	74 bytes	1	60 bytes	36.864770	0.0002		
192.168.200.100	34748	192.168.200.150	2	2	134 bytes	292	1	74 bytes	1	60 bytes	36.806880	0.0002		
192.168.200.100	58938	192.168.200.150	3	2	134 bytes	966	1	74 bytes	1	60 bytes	36.873582	0.0003		
192.168.200.100	43056	192.168.200.150	4	2	134 bytes	557	1	74 bytes	1	60 bytes	36.832248	0.0003		
192.168.200.100	54282	192.168.200.150	5	2	134 bytes	661	1	74 bytes	1	60 bytes	36.841442	0.0003		
192.168.200.100	40874	192.168.200.150	6	2	134 bytes	212	1	74 bytes	1	60 bytes	36.798733	0.0003		
192.168.200.100	52702	192.168.200.150	7	2	134 bytes	505	1	74 bytes	1	60 bytes	36.827912	0.0002		
192.168.200.100	47720	192.168.200.150	8	2	134 bytes	124	1	74 bytes	1	60 bytes	36.790063	0.0001		
192.168.200.100	41348	192.168.200.150	9	2	134 bytes	429	1	74 bytes	1	60 bytes	36.820242	0.0002		
192.168.200.100	46014	192.168.200.150	10	2	134 bytes	216	1	74 bytes	1	60 bytes	36.799061	0.0002		
192.168.200.100	37252	192.168.200.150	11	2	134 bytes	54	1	74 bytes	1	60 bytes	36.780326	0.0003		
192.168.200.100	41700	192.168.200.150	12	2	134 bytes	793	1	74 bytes	1	60 bytes	36.854291	0.0002		
192.168.200.100	58814	192.168.200.150	13	2	134 bytes	235	1	74 bytes	1	60 bytes	36.801464	0.0002		
192.168.200.100	53648	192.168.200.150	14	2	134 bytes	382	1	74 bytes	1	60 bytes	36.815493	0.0003		
192.168.200.100	42454	192.168.200.150	15	2	134 bytes	233	1	74 bytes	1	60 bytes	36.801319	0.0002		
192.168.200.100	36316	192.168.200.150	16	2	134 bytes	748	1	74 bytes	1	60 bytes	36.849675	0.0003		
192.168.200.100	39712	192.168.200.150	17	2	134 bytes	943	1	74 bytes	1	60 bytes	36.871253	0.0002		
192.168.200.100	57066	192.168.200.150	18	2	134 bytes	743	1	74 bytes	1	60 bytes	36.849341	0.0002		
192.168.200.100	49988	192.168.200.150	19	2	134 bytes	102	1	74 bytes	1	60 bytes	36.787346	0.0002		
192.168.200.100	48812	192.168.200.150	20	2	134 bytes	285	1	74 bytes	1	60 bytes	36.806168	0.0003		
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	41304	192.168.200.150	23	4	280 bytes	2	3	206 bytes	1	74 bytes	36.774143	0.0015		
192.168.200.100	37888	192.168.200.150	24	2	134 bytes	800	1	74 bytes	1	60 bytes	36.854687	0.0002		
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	34782	192.168.200.150	26	2	134 bytes	159	1	74 bytes	1	60 bytes	36.792890	0.0002		
192.168.200.100	52294	192.168.200.150	27	2	134 bytes	407	1	74 bytes	1	60 bytes	36.817415	0.0002		
192.168.200.100	40542	192.168.200.150	28	2	134 bytes	489	1	74 bytes	1	60 bytes	36.826423	0.0002		
192.168.200.100	57172	192.168.200.150	29	2	134 bytes	686	1	74 bytes	1	60 bytes	36.844094	0.0002		
192.168.200.100	50624	192.168.200.150	30	2	134 bytes	647	1	74 bytes	1	60 bytes	36.840149	0.0004		
192.168.200.100	42462	192.168.200.150	31	2	134 bytes	623	1	74 bytes	1	60 bytes	36.837395	0.0008		
192.168.200.100	58262	192.168.200.150	32	2	134 bytes	173	1	74 bytes	1	60 bytes	36.794491	0.0003		
192.168.200.100	40194	192.168.200.150	33	2	134 bytes	981	1	74 bytes	1	60 bytes	36.874668	0.0002		
192.168.200.100	41062	192.168.200.150	34	2	134 bytes	841	1	74 bytes	1	60 bytes	36.861335	0.0002		
192.168.200.100	37230	192.168.200.150	35	2	134 bytes	278	1	74 bytes	1	60 bytes	36.805714	0.0002		
192.168.200.100	47180	192.168.200.150	36	2	134 bytes	309	1	74 bytes	1	60 bytes	36.808661	0.0007		
192.168.200.100	42742	192.168.200.150	37	2	134 bytes	597	1	74 bytes	1	60 bytes	36.835560	0.0025		
192.168.200.100	47896	192.168.200.150	38	2	134 bytes	845	1	74 bytes	1	60 bytes	36.861585	0.0002		

Close | Help

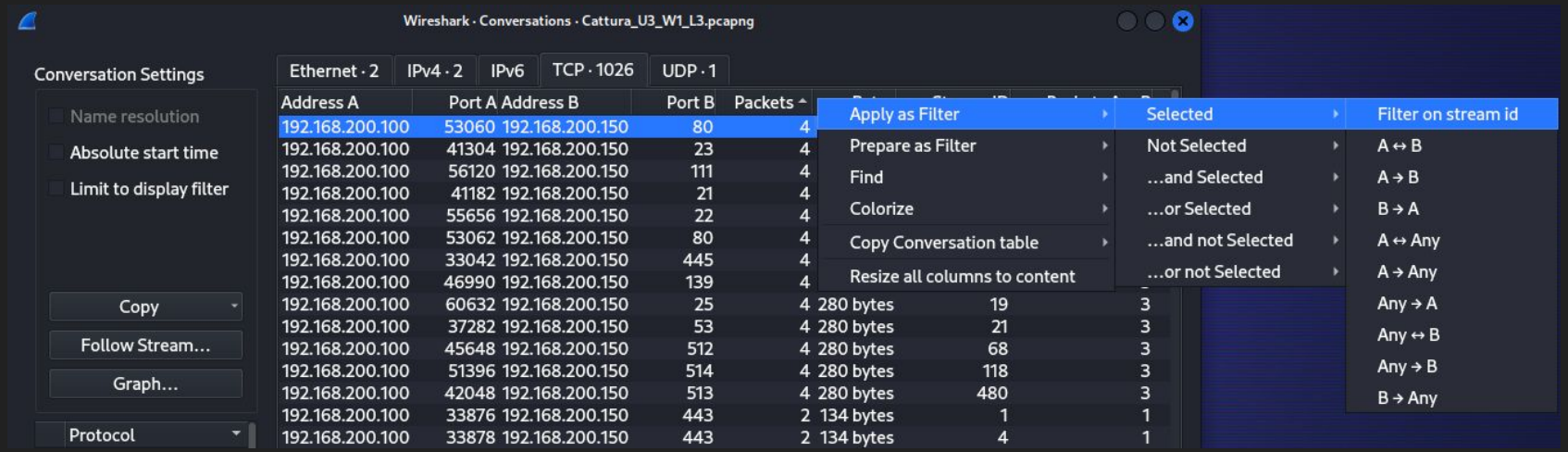
Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 1026 | UDP · 1

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
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	41304	192.168.200.150	23	4	280 bytes	2	3	206 bytes	1	74 bytes	36.774143	0.0015
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	53060	192.168.200.150	80	4	280 bytes	0	3	206 bytes	1	74 bytes	23.764215	0.0007
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	56120	192.168.200.150	111	4	280 bytes	3	3	206 bytes	1	74 bytes	36.774218	0.0014
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	33042	192.168.200.150	445	4	280 bytes	15	3	206 bytes	1	74 bytes	36.776386	0.0015
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	42048	192.168.200.150	513	4	280 bytes	480	3	206 bytes	1	74 bytes	36.825398	0.0039
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	37396	192.168.200.150	1	2	134 bytes	874	1	74 bytes	1	60 bytes	36.864770	0.0002
192.168.200.100	34748	192.168.200.150	2	2	134 bytes	292	1	74 bytes	1	60 bytes	36.806880	0.0002

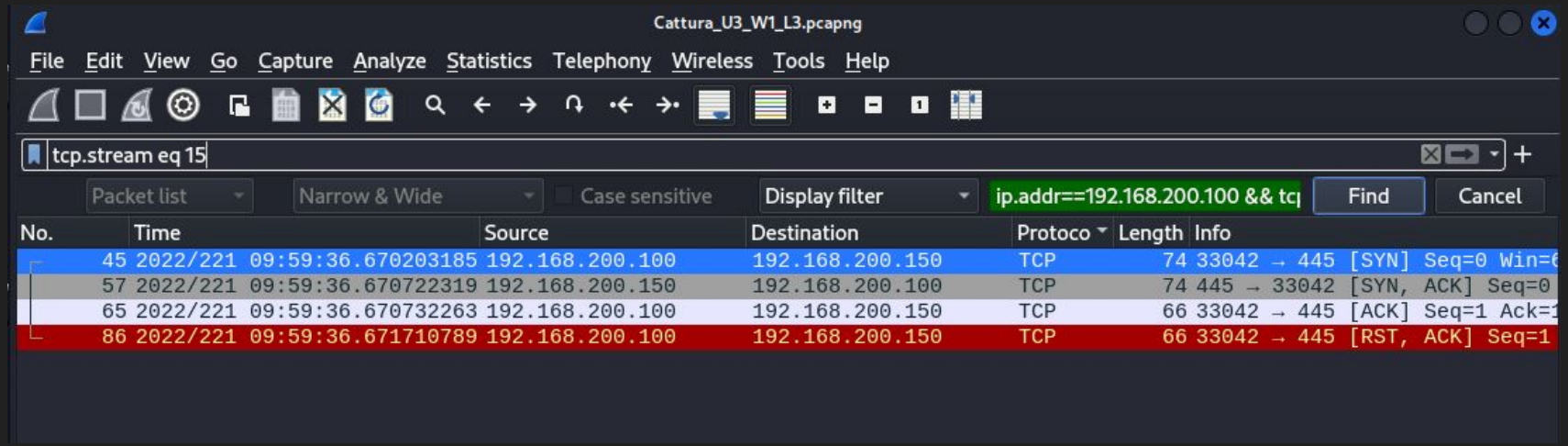
Ma non è tutto, potremo vedere anche quali porti attivi sono stati scoperti!

Se ricordiamo lo screenshot della slide 2, possiamo vedere un 3-way-handshake + il pacchetto per chiudere la comunicazione, ovvero un totale di 4 pacchetti. Se la porta scansionata risponde con un ACK ad un messaggio SYN, questa è una conferma che è una porta attiva, in caso contrario, la "conversazione" che l'attaccante tenterà sarà di soli 2 pacchetti, il SYN e l'RST-ACK.

Filtrando poi le conversazioni con 4 pacchetti, possiamo vedere che 13 porte hanno risposto con ACK, cioè sono state scoperte 13 porte attive e potenzialmente vulnerabili.



Seguiremo una delle conversazioni del pacchetto da 4, facendo clic con il pulsante destro del mouse e filtrando come mostrato nell'immagine.



Come visto in precedenza, un 3-way-handshake, più RST-ACK.

VETTORI DI ATTACCO

REMEDIATION ACTIONS

Il modo più efficace per proteggere l'host Metasploitable da un potenziale attacco sarebbe negare l'ip 192.168.200.100 nella ACL del firewall, ma questo non garantisce che lo stesso soggetto malintenzionato non tenti di sfruttare le porte già scoperte.

Possiamo ridurre al minimo la superficie di attacco disattivando tutti i servizi che non sono importanti. Alcuni di questi servizi che dovremmo disattivare sarebbero quelli presenti sulle porte 21 e 23 (FTP e Telnet), poiché sono servizi altamente vulnerabili, sia allo sniffing dei pacchetti che all'iniezione di una reverse shell remota