

# CONSEGNA S9/L3

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

Si inizia l'esercizio spostando su Kali il **file** della scansione **Wireshark**.

Una volta fatto lo si può aprire con Wireshark e si può iniziare ad **osservare** la **situazione** che ci troviamo davanti.

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 B...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53600 -> 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 -> 53600 [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	53600 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764819091	192.168.200.150	192.168.200.100	TCP	60	33876 -> 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=810522428 TSecr=4294951165
8	28.761029461	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761044619	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	28.775230899	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	41384 -> 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774210116	192.168.200.100	192.168.200.150	TCP	74	56129 -> 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257941	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	36.774366395	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	36.774495627	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	192.168.200.100	TCP	74	23 -> 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685592	192.168.200.150	192.168.200.100	TCP	74	111 -> 56129 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685996	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	554 -> 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774695776	192.168.200.150	192.168.200.100	TCP	60	105 -> 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774709404	192.168.200.100	192.168.200.150	TCP	60	41384 -> 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	56129 -> 111 [ACK] Seq=1 Ack=1 Win=0 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	36.775141121	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	60	41182 -> 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466

Frame 41: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth1, id 0  
Ethernet II, Src: PcsCompu\_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu\_39:7d:fe (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: 53602, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Packets: 2083 · Displayed: 2083 (100.0%) Profile: Default

Ad una rapida occhiata vediamo tantissimi **protocolli TCP**, ma andiamo ad indagare più a fondo.

Andando su **Statistics>Protocol Hierarchy** possiamo vedere la gerarchia di tutti i protocolli presenti nella cattura.

Fondamentalmente questa sezione ci mostra i **protocolli catturati** con la relativa **quantità** a fianco.

In questo caso per quanto riguarda il protocollo TCP (*Transmission Control Process*) sono stati trovati ben **2078 pacchetti**, esattamente il **99,8%** di tutti i pacchetti catturati.

Wireshark - Protocol Hierarchy Statistics - Cattura\_U3\_W1\_L3.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
Frame	100.0	2083	100.0	139872	30 k	0	0	0	2083
Ethernet	100.0	2083	25.2	35276	7652	0	0	0	2083
Internet Protocol Version 4	99.8	2079	29.7	41580	9019	0	0	0	2079
User Datagram Protocol	0.0	1	0.0	8	1	0	0	0	1
NetBIOS Datagram Service	0.0	1	0.2	244	52	0	0	0	1
SMB (Server Message Block Protocol)	0.0	1	0.1	162	35	0	0	0	1
SMB MailSlot Protocol	0.0	1	0.0	25	5	0	0	0	1
Microsoft Windows Browser Protocol	0.0	1	0.1	76	16	1	76	16	1
Transmission Control Protocol	99.8	2078	44.8	62652	13 k	2078	62652	13 k	2078
Address Resolution Protocol	0.2	4	0.1	148	32	4	148	32	4

Andando su **Statistics>Conversations** possiamo ottenere più il **MAC Address** sia dell'**host attaccante** che dell'**host attaccato**, rispettivamente *Address A* e *Address B*, come in figura.

Wireshark - Conversations - Cattura\_U3\_W1\_L3.pcapng

Conversation Settings	Ethernet - 2	IPv4 - 2	IPv6	TCP - 1026	UDP - 1
Name resolution	Address A	Address B			
Absolute start time	08:00:27.39:7dfe	08:00:27.4d:87:1e			
Limit to display filter					
	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
	2082	136.314 KiB	1054	75.902 KiB	1028
	1	286 bytes	1	286 bytes	0
	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
	0 bytes	0.000000	0.00000	47 kbps	37 kbps

Rimanendo sempre in questa voce e recandoci nella sezione **IPv4** possiamo ottenere gli **indirizzi IP** sia dell'**host attaccante** che dell'**host attaccato**, rispettivamente *Address A* e *Address B*, come in figura.

In questo caso:

- **192.168.200.150** è l'**attaccante**
- **192.168.200.100** è la **macchina host**

Wireshark - Conversations - Cattura\_U3\_W1\_L3.pcapng

Conversation Settings	Ethernet - 2	IPv4 - 2	IPv6	TCP - 1026	UDP - 1
Name resolution	Address A	Address B			
Absolute start time	192.168.200.100	192.168.200.150			
Limit to display filter					
	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
	2078	136.314 KiB	1054	75.902 KiB	1028
	1	286 bytes	1	286 bytes	0
	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
	0 bytes	0.000000	0.00000	47 kbps	37 kbps

Rechiamoci anche nella sezione **TCP** per visionare tutti i pacchetti TCP che sono stati catturati.

Se clicchiamo una volta sulla voce **“Port B”** possiamo **ordinare** tutti i pacchetti inviati dalla macchina attaccante, come in figura sotto.

Wireshark - Conversations - Cattura\_U3\_W1\_L3.pcapng

Conversation Settings	Ethernet - 2	IPv4 - 2	IPv6	TCP - 1026	UDP - 1														
Name resolution	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				
Absolute start time	192.168.200.100	37396	192.168.200.150	Port B	1	2 134 bytes	874	1	74 bytes	1	60 bytes	36.864770	0.0002						
Limit to display filter	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	49888	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	54782	192.168.200.150	26	2 134 bytes	150	1	74 bytes	1	60 bytes	36.792880	0.0002							

Transmission Control Protocol, Src Port: 53062, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

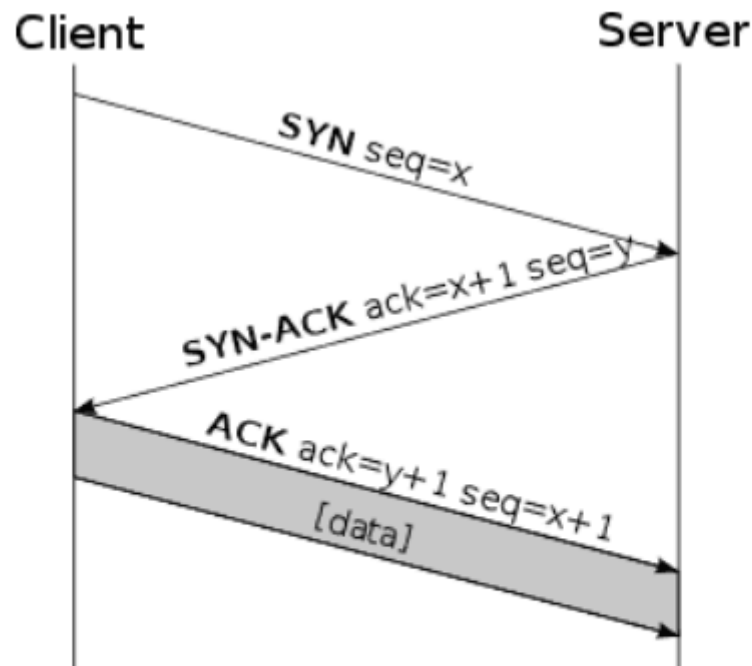
Possiamo ottenere anche l'elenco delle **porte aperte** cliccando una volta su **“Packets”**. Il programma ci ordinerà i pacchetti per **grandezza** e quelli più grandi (da **4 pacchetti**) sono le nostre **porte aperte**, perché completano il **Three-Way-Handshake**, un metodo utilizzato in una rete **TCP/IP** per creare una connessione tra un host/client locale e un server scambiando i pacchetti **SYN** e **ACK**.

- Le **porte aperte** che sono state individuate sono: **21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514**.

Wireshark - Conversations - Cattura\_U3\_W1\_L3.pcapng

Conversation Settings	Ethernet - 1	IPv4 - 1	IPv6	TCP - 1026	UDP														
Name resolution	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			
Absolute start time	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					
Limit to display filter	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	50120	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	36.778478	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	36.823398	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					

Il **Three-Way-Handshake** è raffigurato nella figura sotto.



Tcp-handshake : Client = A : Server = B

Three-way handshake

Con il filtro “**tcp.stream eq 2**” da applicare nella **barra dei filtri** in alto (oppure semplicemente facendo **tasto destro** su un pacchetto **TCP**, “**Follow**” e poi “**TCP Stream**”) si può ottenere nel dettaglio il flusso del pacchetto TCP.

Nella figura sotto il pacchetto TCP selezionato completa il *Three-Way-Handshake*.

The following table represents the data shown in the Wireshark packet capture, filtered by 'tcp.stream eq 2'. It details the three packets of the TCP handshake.

No.	Time	Source	Destination	Protocol	Length	Info
12	36.774543445	192.168.200.100	192.168.200.150	TCP	74	41384 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
19	36.774695505	192.168.200.150	192.168.200.100	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
24	36.774708464	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466

Below the packet list, the details pane for the selected packet (No. 24) shows the following information:

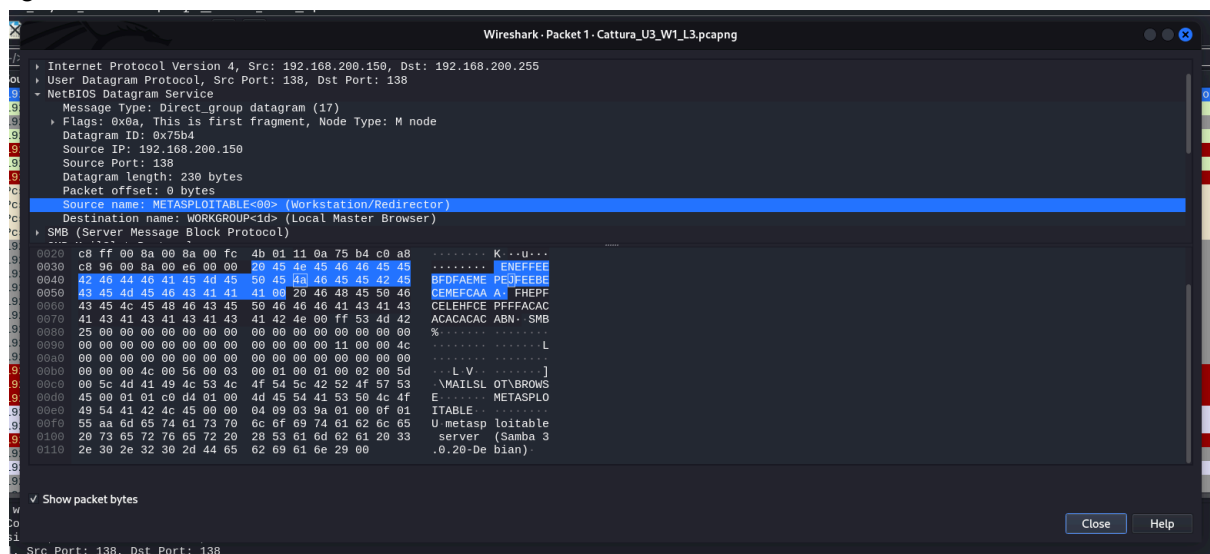
- Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
- Ethernet II, Src: PcsCompu\_39:7d:fe (08:00:27:38:7d:fe), Dst: PcsCompu\_fd:87:1e (08:00:27:fd:87:1e)
- Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
- Transmission Control Protocol, Src Port: 41384, Dst Port: 23, Seq: 0, Len: 0

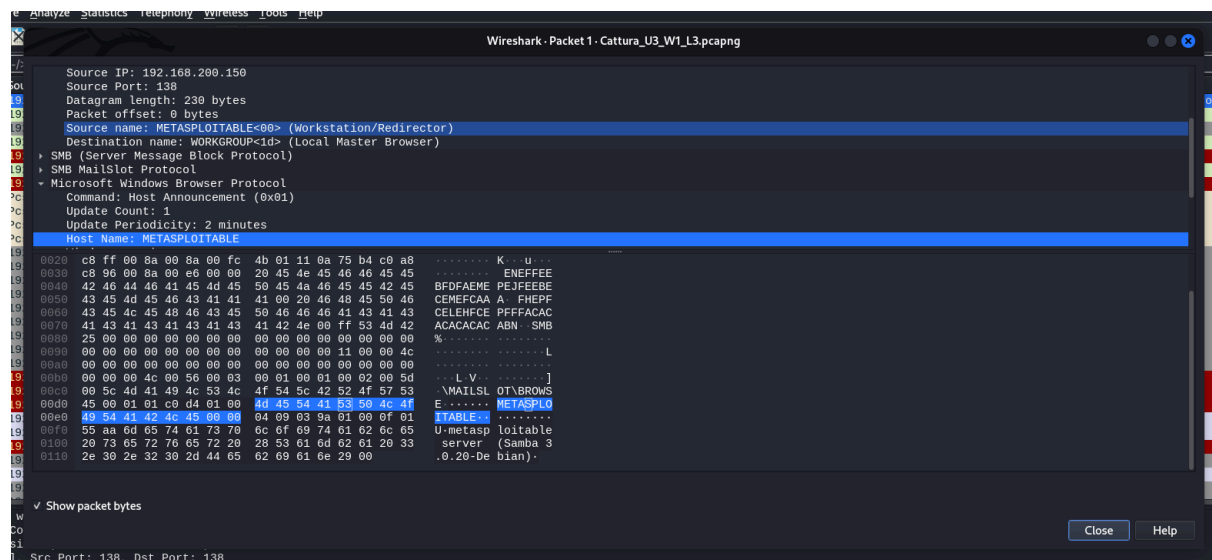
Nel dettaglio in figura sotto il **protocollo ARP** dell'attaccante.



Possiamo notare anche la presenza del **pacchetto BROWSER**, il primo che troviamo nella scansione.

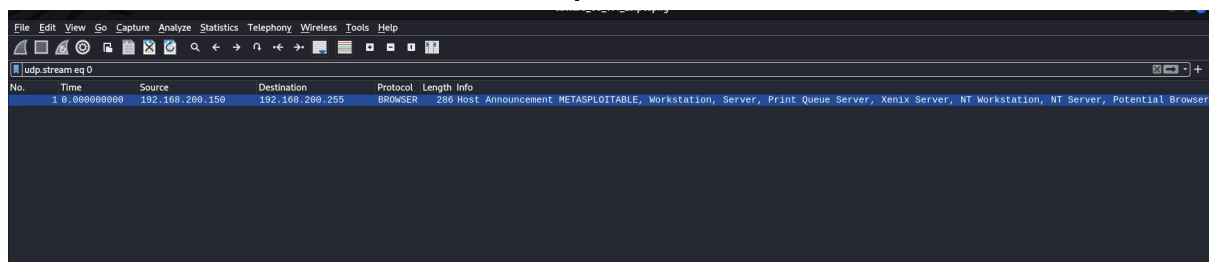
Se facciamo doppio click su tale pacchetto possiamo scoprire che la macchina attaccante è **Metasploitable**.ed è presente sia nella dicitura “**Source name**” che in “**Host**”, come da figure.





Possiamo fare anche la controprova seguendo il traffico del pacchetto, facendo **tasto destro** sul pacchetto **BROWSER**, “Follow” e poi “UDP Stream”.

Così facendo possiamo vedere molto meglio le informazioni che ci servono: abbiamo trovato un attaccante che usa una macchina **Metasploitable basata su Samba 3.0.20-Debian**.



- Giunti a questo punto si può tranquillamente affermare che l'attaccante stava eseguendo un **port scanning** sul nostro host.  
Come **azione** per **ridurre** gli **impatti dell'attacco** si può (e si deve) utilizzare un **firewall**.