S9L3

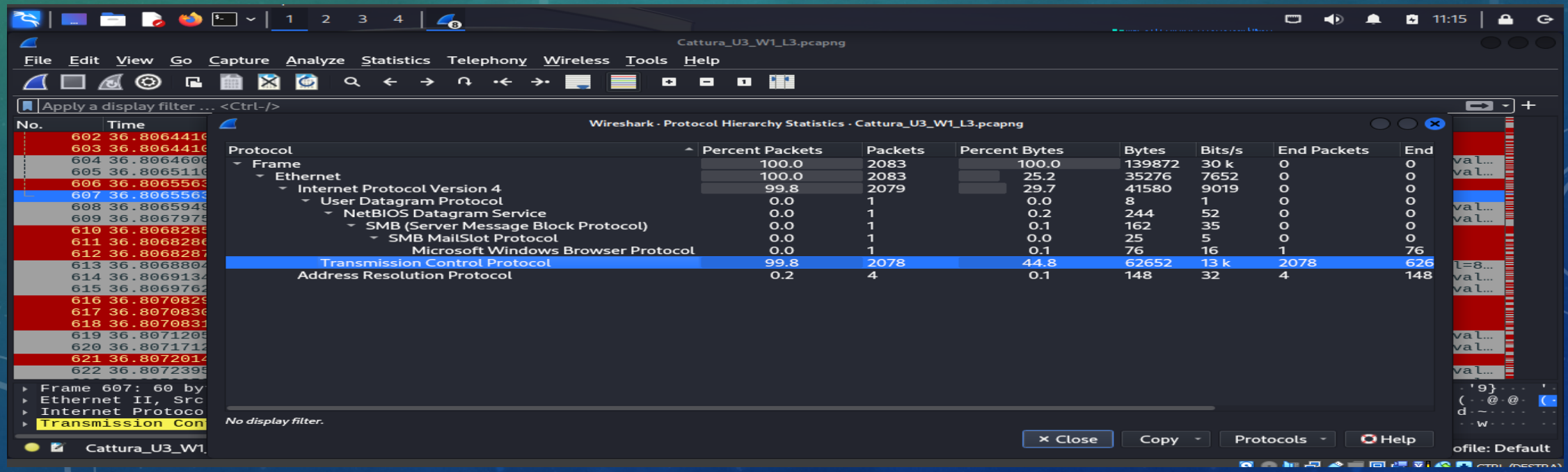
TRACCIA:

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

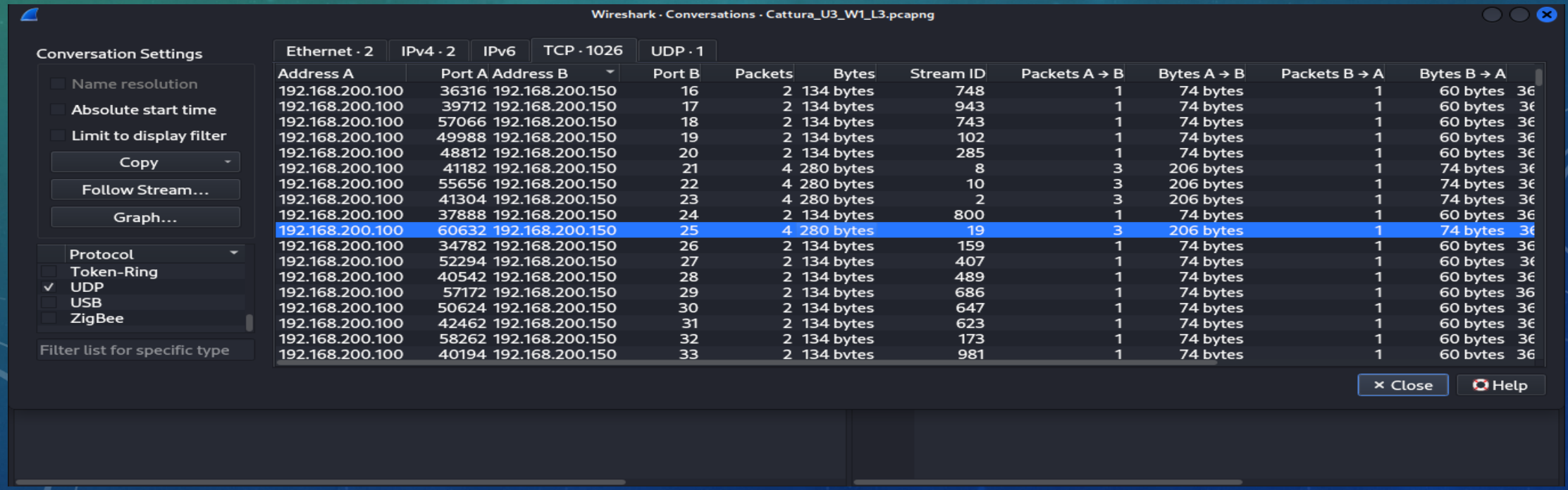
UN'AZIONE PER RIDURRE GLI IMPATTI DELL'ATTACCO

C’È UNA FINESTRA APERTA INTITOLATA “WIRESHARK: HIERARCHY STATISTICS - CATTURA_U3_WL3.PCAPNG” CHE MOSTRA LE STATISTICHE DEI PROTOCOLLI UTILIZZATI DOPODICHE’ SIAMO ANDATI ALLA VOCE STATISTICS E ABBIAMO SELEZIONATO PROTOCOL HIERARCHY STATICS. L’IMMAGINE MOSTRA UNA LISTA DI PACCHETTI DI RETE CON COLONNE PER IL NUMERO DEL PACCHETTO, IL TEMPO TRASCORSO, LA SORGENTE, LA DESTINAZIONE, IL

PROTOCOLLO UTILIZZATO E LE INFORMAZIONI SULLA LUNGHEZZA. POSSIAMO VEDERE CHE ABBIAMO EVIDENZIATO E’ IL TCP LA PERCENTUALE DEI PACCHETTI INVIATA È DEL 99,8%



WIRESHARK, UNO STRUMENTO UTILIZZATO PER L'ANALISI DEI PACCHETTI DI RETE. HAI EVIDENZIATO 4 PACCHETTI, E DALLA TUA DESCRIZIONE, SEMBRA CHE TU STIA INDICANDO UN COMPLETAMENTO SYN ACK. ECCO ALCUNI DETTAGLI:
LA FINESTRA VISUALIZZATA È LA "CONVERSATIONS", CHE MOSTRA LE CONVERSAZIONI TRA INDIRIZZI IP DIVERSI.
CI SONO COLONNE PER GLI INDIRIZZI IP A E B, LE PORTE A E B, I PACCHETTI TOS, I PACCHETTI UDP E TCP.
QUATTRO RIGHE SONO EVIDENZIATE IN BLU; QUESTE RIGHE MOSTRANO LA COMUNICAZIONE TRA L'INDIRIZZO IP 192.168.200.100 E 192.168.200.150 ATTRAVERSO DIVERSE PORTE. OGNI RIGA EVIDENZIATA MOSTRA UN NUMERO DIVERSO DI BYTE INVIATI DA A 192.168.200.100 E B 192.168.200.150 (74 BYTES, 206 BYTES) E DA B AD A (60 BYTES). NEL CONTESTO DI UNA CONNESSIONE TCP, UN PACCHETTO SYN ACK È INVIATO COME RISPOSTA A UN PACCHETTO SYN PER STABILIRE UNA CONNESSIONE. SE VEDI UN PACCHETTO SYN SEGUITO DA UN PACCHETTO SYN ACK, SIGNIFICA CHE LA CONNESSIONE È STATA STABILITA CON SUCCESSO.



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.200.100	36316	192.168.200.150	16	2	134 bytes	748	1	74 bytes	1	60 bytes
192.168.200.100	39712	192.168.200.150	17	2	134 bytes	943	1	74 bytes	1	60 bytes
192.168.200.100	57066	192.168.200.150	18	2	134 bytes	743	1	74 bytes	1	60 bytes
192.168.200.100	49988	192.168.200.150	19	2	134 bytes	102	1	74 bytes	1	60 bytes
192.168.200.100	48812	192.168.200.150	20	2	134 bytes	285	1	74 bytes	1	60 bytes
192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	3	206 bytes	1	74 bytes
192.168.200.100	55656	192.168.200.150	22	4	280 bytes	10	3	206 bytes	1	74 bytes
192.168.200.100	41304	192.168.200.150	23	4	280 bytes	2	3	206 bytes	1	74 bytes
192.168.200.100	37888	192.168.200.150	24	2	134 bytes	800	1	74 bytes	1	60 bytes
192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	3	206 bytes	1	74 bytes
192.168.200.100	34782	192.168.200.150	26	2	134 bytes	159	1	74 bytes	1	60 bytes
192.168.200.100	52294	192.168.200.150	27	2	134 bytes	407	1	74 bytes	1	60 bytes
192.168.200.100	40542	192.168.200.150	28	2	134 bytes	489	1	74 bytes	1	60 bytes
192.168.200.100	57172	192.168.200.150	29	2	134 bytes	686	1	74 bytes	1	60 bytes
192.168.200.100	50624	192.168.200.150	30	2	134 bytes	647	1	74 bytes	1	60 bytes
192.168.200.100	42462	192.168.200.150	31	2	134 bytes	623	1	74 bytes	1	60 bytes
192.168.200.100	58262	192.168.200.150	32	2	134 bytes	173	1	74 bytes	1	60 bytes
192.168.200.100	40194	192.168.200.150	33	2	134 bytes	981	1	74 bytes	1	60 bytes