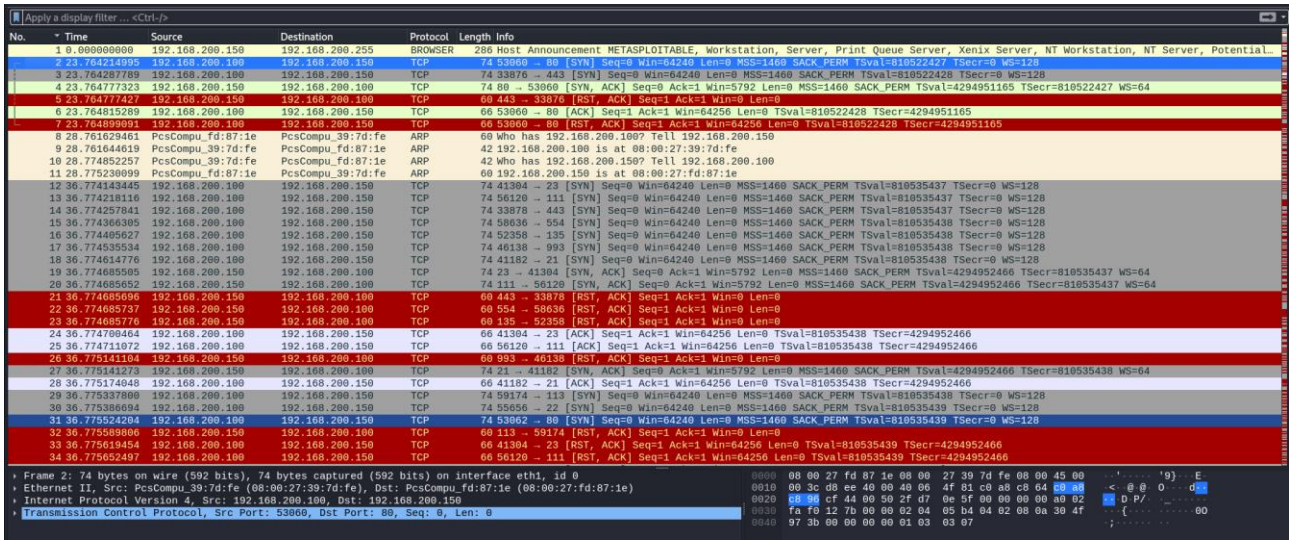
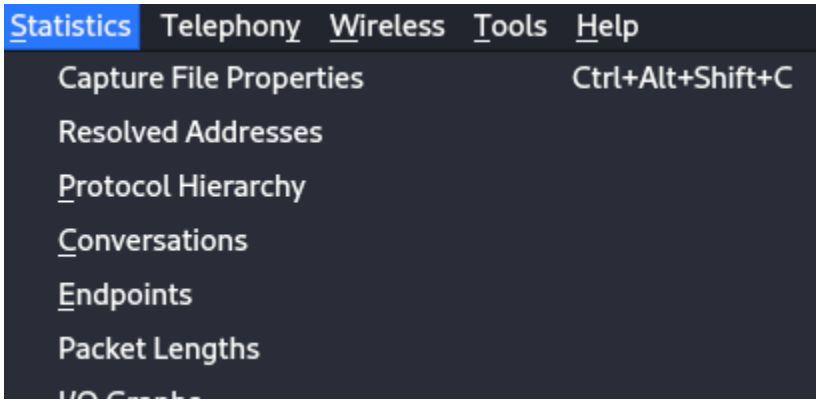
ESERCITAZIONE S9 L 3

Threat Intelligence & IOC

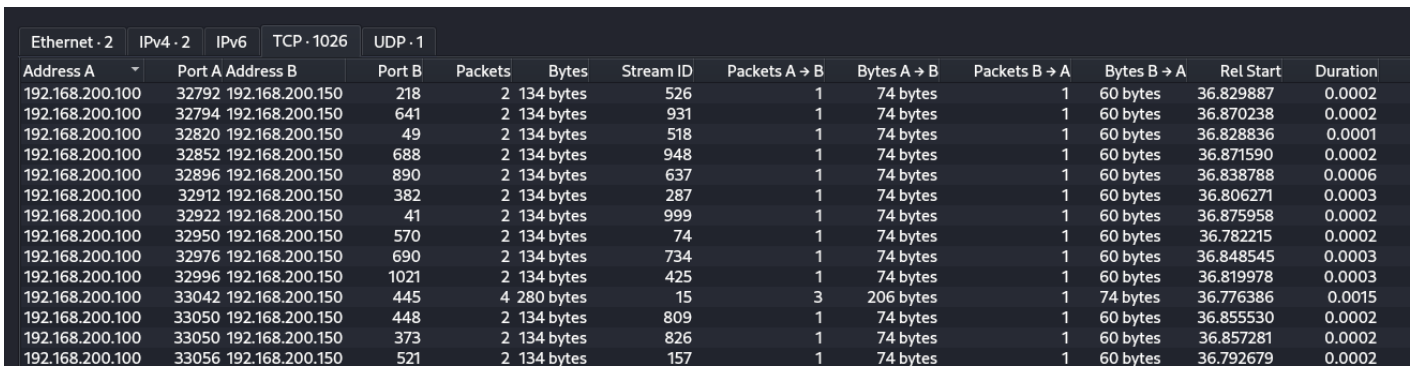
Una volta scaricato e spostato il file su Kali, possiamo aprilo con WireShark.



Andiamo in *Statics > Conversations*



Così da avere una visione riepilogativa delle trasmissioni *TCP*



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	32792	192.168.200.150	218	2	134 bytes	526	1	74 bytes	1	60 bytes	36.829887	0.0002
192.168.200.100	32794	192.168.200.150	641	2	134 bytes	931	1	74 bytes	1	60 bytes	36.870238	0.0002
192.168.200.100	32820	192.168.200.150	49	2	134 bytes	518	1	74 bytes	1	60 bytes	36.828836	0.0001
192.168.200.100	32852	192.168.200.150	688	2	134 bytes	948	1	74 bytes	1	60 bytes	36.871590	0.0002
192.168.200.100	32896	192.168.200.150	890	2	134 bytes	637	1	74 bytes	1	60 bytes	36.838788	0.0006
192.168.200.100	32912	192.168.200.150	382	2	134 bytes	287	1	74 bytes	1	60 bytes	36.806271	0.0003
192.168.200.100	32922	192.168.200.150	41	2	134 bytes	999	1	74 bytes	1	60 bytes	36.875958	0.0002
192.168.200.100	32950	192.168.200.150	570	2	134 bytes	74	1	74 bytes	1	60 bytes	36.782215	0.0002
192.168.200.100	32976	192.168.200.150	690	2	134 bytes	734	1	74 bytes	1	60 bytes	36.848545	0.0003
192.168.200.100	32996	192.168.200.150	1021	2	134 bytes	425	1	74 bytes	1	60 bytes	36.819978	0.0003
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	33050	192.168.200.150	448	2	134 bytes	809	1	74 bytes	1	60 bytes	36.855530	0.0002
192.168.200.100	33050	192.168.200.150	373	2	134 bytes	826	1	74 bytes	1	60 bytes	36.857281	0.0002
192.168.200.100	33056	192.168.200.150	521	2	134 bytes	157	1	74 bytes	1	60 bytes	36.792679	0.0002

Come prima analisi possiamo riordinare gli ip, così da evidenziare se ci sono state enumerazioni delle porte tra gli host.

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/
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	

Come si può ben vedere, l' host 192.168.200.100 ha effettuato un'enumerazione delle porte sul host 192.168.200.150, evidenziato quindi un primo evento critico, in quanto l'enumerazione viene eseguita in una prima fase di attacco.

Un ulteriore analisi è quello di capire se l'host attaccante è riuscito a effettuare l'enumerazione delle porte, motivo per cui si ordinano in modo decrescente il numero dei pacchetti.

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	Bi
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	53062	192.168.200.150	80	4	280 bytes	11	3	206 bytes	1	74 bytes	36.775524	0.0005	
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	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	

Possiamo notare che l'host 192.168.200.100 è venuto a conoscenza delle porte aperte, in quanto nelle comunicazioni ha ricevuto/inviato 4 pacchetti, sintomo della corretta comunicazione *TCP* (SYN – SYN/ACK – ACK – RST/ACK)

tcp.stream eq 11

No.	Time	Source	Destination	Protocol	Length	Info
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
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
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
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

Esempio di corretta comunicazione dello stato della porta 80 su ip 192.168.200.150

Il vettore di questo attacco è un host interno, probabilmente infetto, attaccato anche esso, oppure uno stesso dipendente.

Sicuramente una soluzione efficace ed immediata è quello di inibire la connessione dell'attaccante con il resto della rete aziendale, così da non generare altro traffico sospetto e interrompere qualsiasi tipo di attacco. Successivamente bisognerebbe analizzare l'host, controllando che non ci siano backdoor e vulnerabilità sfruttabili dall'esterno, tali da far risultare che l'attacco sia interno. Nel caso di esito positivo, bisognerebbe

- Riparare le eventuali vulnerabilità riscontrare, con applicazioni di patch;
- Aumentare nell'immediato la sicurezza dei servizi esposti dalle porte ormai conosciute, in quanto è molto probabile che possa avvenire un attacco proprio da quelle porte e servizi;
- Implementare policy più stringenti al firewall interno, così che non avvenga in futuro un'enumerazione completa delle porte

Se i controlli precedenti risultano negativi, in questo caso abbiamo la certezza che l'attacco fosse perpetrato dall'interno, bisognerebbe quindi:

- Indagare da chi e con quali intenzioni
- Aumentare la protezione degli spazi fisici