

S9 L3

Davide Andreozzi

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.

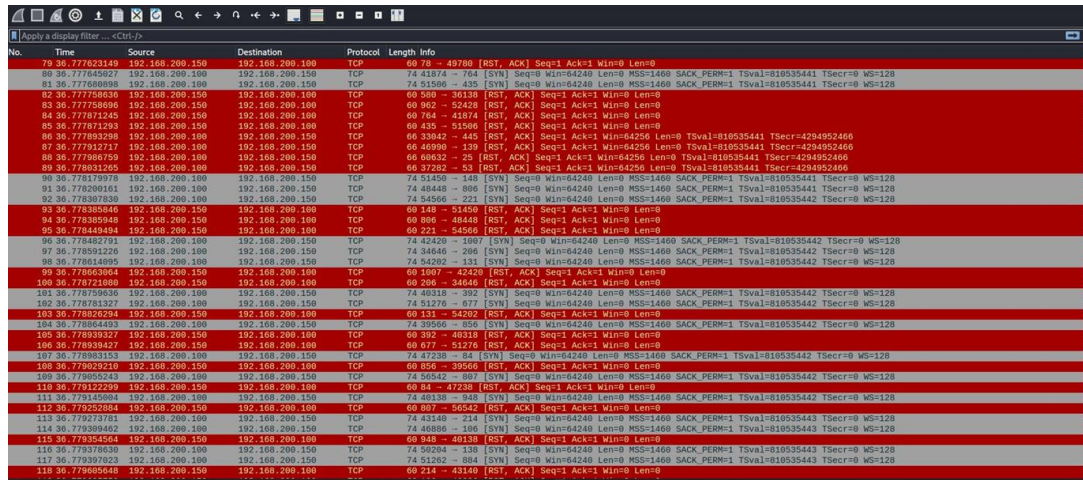
Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- 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

Risoluzione esercizio – IOC

Possiamo vedere come siano presenti molte richieste TCP (SYN) dall'Host 192.168.200.100.

Questo ci fa presumere che sia in atto una scansione di rete in quanto tra queste ci sono alcune risposte dal client 192.168.200.150 con la dicitura [RST, ACK] che indicano che la connessione è stata rifiutata quindi la porta è chiusa. Mentre in altre la risposta [SYN, ACK] indica che la porta è aperta.



No.	Time	Source	Destination	Protocol	Length	Info
70	36.777023149	192.168.200.150	192.168.200.100	TCP	60	70 → 48708 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
108	36.777045022	192.168.200.150	192.168.200.150	TCP	74	48708 → 7041 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
81	36.777080898	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
102	36.777758835	192.168.200.150	192.168.200.100	TCP	60	800 → 80138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758996	192.168.200.150	192.168.200.100	TCP	60	802 → 52420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.777871293	192.168.200.150	192.168.200.100	TCP	60	835 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64250 Len=0 TSval=810535441 TSecr=4284952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46980 → 139 [RST, ACK] Seq=1 Ack=1 Win=64250 Len=0 TSval=810535441 TSecr=4284952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632 → 26 [RST, ACK] Seq=1 Ack=1 Win=64250 Len=0 TSval=810535441 TSecr=4284952466
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64250 Len=0 TSval=810535441 TSecr=4284952466
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
91	36.778200101	192.168.200.100	192.168.200.150	TCP	74	48440 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
92	36.778307030	192.168.200.100	192.168.200.150	TCP	74	54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
93	36.778385846	192.168.200.150	192.168.200.100	TCP	60	148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778395948	192.168.200.150	192.168.200.100	TCP	60	806 → 48440 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449484	192.168.200.150	192.168.200.100	TCP	60	221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74	42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74	54566 → 208 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
98	36.778614895	192.168.200.100	192.168.200.150	TCP	74	54282 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
99	36.778653064	192.168.200.150	192.168.200.100	TCP	60	1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721080	192.168.200.150	192.168.200.100	TCP	60	208 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	48318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
102	36.778781527	192.168.200.100	192.168.200.150	TCP	74	51176 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
103	36.778815244	192.168.200.150	192.168.200.100	TCP	60	115 → 51176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778844493	192.168.200.100	192.168.200.150	TCP	74	39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
105	36.77883927	192.168.200.150	192.168.200.100	TCP	60	392 → 48318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778839427	192.168.200.150	192.168.200.100	TCP	60	877 → 51176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778883153	192.168.200.100	192.168.200.150	TCP	74	47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
108	36.778929210	192.168.200.150	192.168.200.100	TCP	60	656 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.778955242	192.168.200.150	192.168.200.100	TCP	74	50542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779215500	192.168.200.150	192.168.200.100	TCP	74	40130 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
112	36.779252084	192.168.200.150	192.168.200.100	TCP	60	807 → 50542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
114	36.779309462	192.168.200.100	192.168.200.150	TCP	74	48406 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
115	36.779354564	192.168.200.150	192.168.200.100	TCP	60	948 → 40130 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378030	192.168.200.100	192.168.200.150	TCP	74	50204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
117	36.779397023	192.168.200.100	192.168.200.150	TCP	74	51262 → 804 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
118	36.779605848	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Risoluzione esercizio – Soluzioni per ridurre l’impatto

- Impostare delle regole di Firewall per bloccare tutte le richieste da quel determinato indirizzo ip.

- Utilizzo di IDS/IPS

- Chiudere le porte e/o servizi non necessari per mitigare probabilità di intrusione da parte di un ipotetico attaccante

Apply a display filter ... (Ctrl-D)									
No.	Time	Source	Destination	Protocol	Length	Info			
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, 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	53602 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466			
42	36.776137330	192.168.200.100	192.168.200.150	TCP	74	59084 → 139 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128			
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
45	36.776386994	192.168.200.100	192.168.200.150	TCP	74	33942 → 445 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
47	36.776451284	192.168.200.150	192.168.200.150	TCP	60	199 → 56084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
48	36.776451367	192.168.200.150	192.168.200.150	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
50	36.776499306	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
51	36.776522221	192.168.200.100	192.168.200.150	TCP	74	60032 → 25 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
52	36.776560606	192.168.200.100	192.168.200.150	TCP	74	49054 → 110 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54008 → 500 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 487 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
57	36.776904826	192.168.200.150	192.168.200.100	TCP	74	445 → 33942 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64			
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
59	36.776964961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64			
60	36.776995004	192.168.200.150	192.168.200.100	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
61	36.776995043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64			
62	36.776995062	192.168.200.150	192.168.200.100	TCP	60	110 → 49054 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
63	36.776995121	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64			
64	36.776995162	192.168.200.150	192.168.200.100	TCP	60	500 → 54008 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
65	36.777024172	192.168.200.100	192.168.200.150	TCP	66	33942 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466			
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466			
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466			
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466			
69	36.777119481	192.168.200.150	192.168.200.100	TCP	60	487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
70	36.777143814	192.168.200.100	192.168.200.150	TCP	74	56990 → 787 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
71	36.777180821	192.168.200.100	192.168.200.150	TCP	74	36638 → 408 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128			
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120 → 98 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128			
73	36.777337834	192.168.200.100	192.168.200.150	TCP	74	49780 → 78 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128			
74	36.777431632	192.168.200.150	192.168.200.100	TCP	60	10 → 56000 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
75	36.777430741	192.168.200.150	192.168.200.100	TCP	60	436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74	36138 → 580 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128			
77	36.777521484	192.168.200.100	192.168.200.150	TCP	74	52428 → 862 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128			
78	36.777623082	192.168.200.150	192.168.200.100	TCP	60	98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			