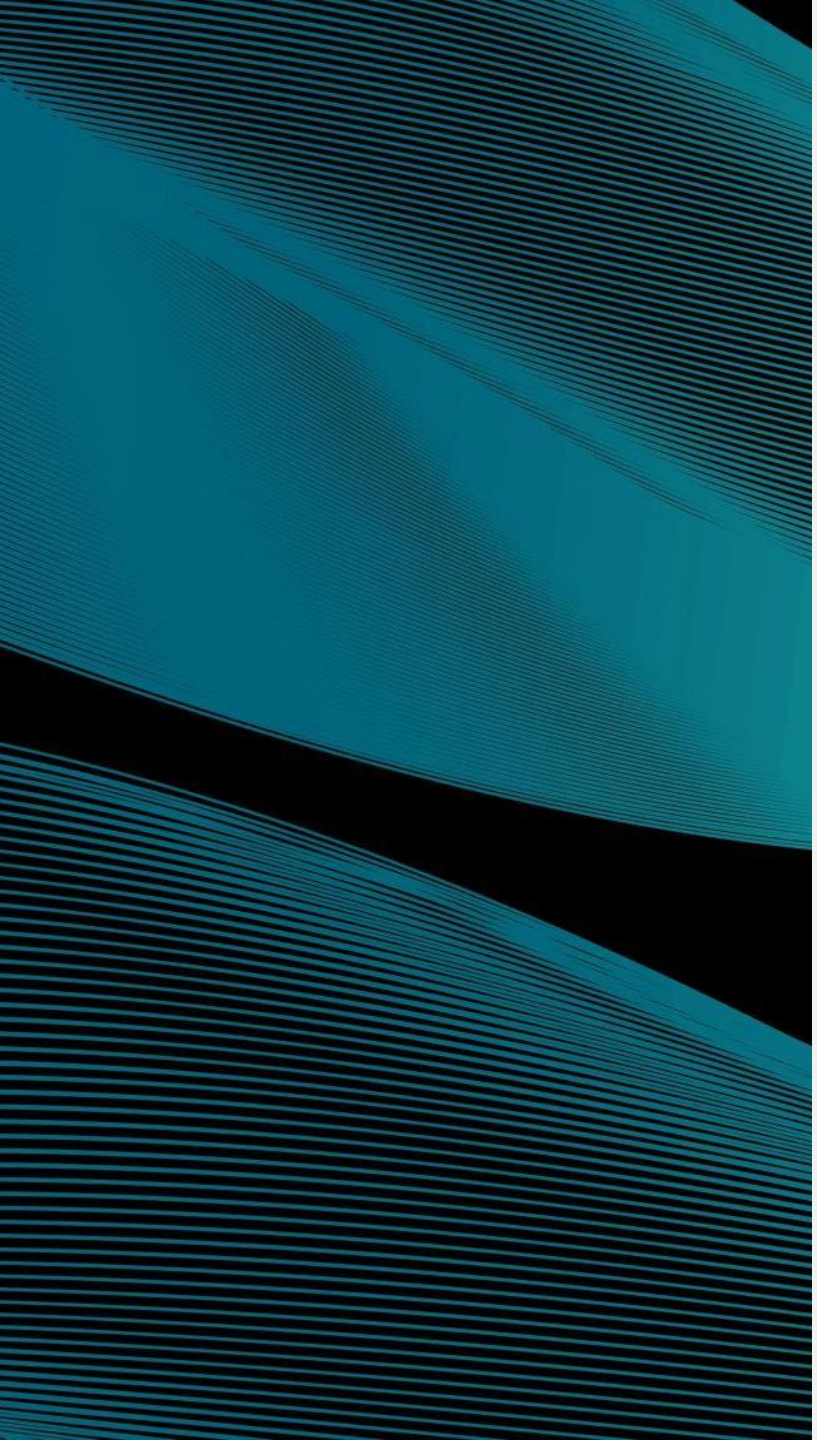

Threat Intelligence & IOC

Pablo Andres Balbuena Rios

Esercizio 3 Settimana 9

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

Identificare eventuali IOC

Come possiamo osservare in questo flusso di rete che ci fornisce Wireshark, notiamo che un dispositivo"192.168.200.100" sta mandando multiple richieste TCP ad un altro dispositivo "192.168.200.150" in ampi intervalli di porte.

Wireshark

74	36.777430632	192.168.200.150	192.168.200.100	TCP	60 707 → 56990 [RST, ACK] Se
75	36.777430741	192.168.200.150	192.168.200.100	TCP	60 436 → 35638 [RST, ACK] Se
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74 36138 → 580 [SYN] Seq=0 W
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74 52428 → 962 [SYN] Seq=0 W
78	36.777623082	192.168.200.150	192.168.200.100	TCP	60 98 → 34120 [RST, ACK] Seq
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60 78 → 49780 [RST, ACK] Seq
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74 41874 → 764 [SYN] Seq=0 W
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74 51506 → 435 [SYN] Seq=0 W
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60 580 → 36138 [RST, ACK] Se
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60 962 → 52428 [RST, ACK] Se
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60 764 → 41874 [RST, ACK] Se
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60 435 → 51506 [RST, ACK] Se
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66 33042 → 445 [RST, ACK] Se
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [RST, ACK] Se
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66 60632 → 25 [RST, ACK] Seq
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66 37282 → 53 [RST, ACK] Seq
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74 51450 → 148 [SYN] Seq=0 W
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74 48448 → 806 [SYN] Seq=0 W
92	36.778307830	192.168.200.100	192.168.200.150	TCP	74 54566 → 221 [SYN] Seq=0 W
93	36.778385846	192.168.200.150	192.168.200.100	TCP	60 148 → 51450 [RST, ACK] Se
94	36.778385948	192.168.200.150	192.168.200.100	TCP	60 806 → 48448 [RST, ACK] Se
95	36.778449494	192.168.200.150	192.168.200.100	TCP	60 221 → 54566 [RST, ACK] Se
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74 42420 → 1007 [SYN] Seq=0
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74 34646 → 206 [SYN] Seq=0 W
98	36.778614095	192.168.200.100	192.168.200.150	TCP	74 54202 → 131 [SYN] Seq=0 W
99	36.778663064	192.168.200.150	192.168.200.100	TCP	60 1007 → 42420 [RST, ACK] S
100	36.778721080	192.168.200.150	192.168.200.100	TCP	60 206 → 34646 [RST, ACK] Se

Ipotesi sui potenziali vettori di attacco

Dopo aver identificato ed evidenziato l'attacco. Possiamo constatare che l'attacco che sta avvenendo, è una scansione rumorosa in corso delle porte del dispositivo "192.168.200.150". Questo comporterebbe che l'attaccante vuole sapere se ci sono vulnerabilità in quel dispositivo.

Consigli d’azione per ridurre gli impatti dell’attacco

Per ridurre l'attacco consigliere di installare un buon Firewall sul Host, che non permetta ad un dispositivo di poter pingare e stabilire una connessione con Host stesso, e di minimizzare gli Host che possono stabilire la connessione.