

Nell'esercizio di oggi dobbiamo individuare gli indicatori di compromissione (IOC) in un file di wireshark. Gli indicatori di compromissione sono delle prove, osservabili all'interno di una rete o sistema, che possono indicare un'intrusione. Indicatori tipici possono essere firme antivirali, connessioni TCP/UDP elevate o provenienti dallo stesso mittente e diretti su porte diverse, indirizzi IP o URL sospetti, ecc.

Nel file si possono identificare connessioni TCP multiple:

12	36	774143445	192.168.200.100	192.168.200.150	TCP	74	41304	→ 23	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535437	TSecr=0	WS=128	
13	36	774218116	192.168.200.100	192.168.200.150	TCP	74	56120	→ 111	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535437	TSecr=0	WS=128	
14	36	774257841	192.168.200.100	192.168.200.150	TCP	74	33878	→ 443	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535437	TSecr=0	WS=128	
15	36	774306395	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	774409627	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	192.168.200.150	TCP	74	23	→ 41304	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	TSval=4294952466	TSecr=810535437	WS=64
20	36	774685652	192.168.200.100	192.168.200.150	TCP	74	111	→ 56120	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460	SACK_PERM	TSval=4294952466	TSecr=810535437	WS=64

Come possiamo osservare nella figura sopra ci sono molte richieste TCP che partono dallo stesso mittente e vanno ognuna su una porta diversa. Stessa cosa per l'immagine sotto:

133	36	780325837	192.168.200.100	192.168.200.150	TCP	74	37252	→ 11	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535444	TSecr=0	WS=128
134	36	780346429	192.168.200.100	192.168.200.150	TCP	74	40648	→ 235	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535444	TSecr=0	WS=128
135	36	780409818	192.168.200.100	192.168.200.150	TCP	74	36548	→ 739	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535444	TSecr=0	WS=128
136	36	780427899	192.168.200.100	192.168.200.150	TCP	74	38866	→ 55	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535444	TSecr=0	WS=128
137	36	780472830	192.168.200.100	192.168.200.150	TCP	74	52136	→ 999	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535444	TSecr=0	WS=128
138	36	780490897	192.168.200.100	192.168.200.150	TCP	74	38022	→ 317	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM	TSval=810535444	TSecr=0	WS=128
139	36	780577880	192.168.200.100	192.168.200.100	TCP	60	266	→ 40822	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
140	36	780577981	192.168.200.100	192.168.200.100	TCP	60	11	→ 37252	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
141	36	780578026	192.168.200.100	192.168.200.100	TCP	60	235	→ 40648	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
142	36	780578074	192.168.200.100	192.168.200.100	TCP	60	739	→ 36548	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
143	36	780578119	192.168.200.100	192.168.200.100	TCP	60	55	→ 38866	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
144	36	780578158	192.168.200.100	192.168.200.100	TCP	60	999	→ 52136	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				
145	36	780578198	192.168.200.100	192.168.200.100	TCP	60	317	→ 38022	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0				

Questi sono IOC che possono indicare che qualcuno sta eseguendo una scansione dei servizi sull'indirizzo 192.168.200.150 usando la modalità SYN scan che non completa il three way handshake. Infatti le porte chiuse rispondono con un pacchetto reset (RST), mentre quelle aperte che rispondono con un SYN/ACK non ricevono in risposta il pacchetto ACK che completa il three way handshake.

Ci sono diverse azioni che si possono implementare per mitigare il rischio, come impostare una regola su un firewall per bloccare l'indirizzo IP sospetto, oppure implementare un IPS.

L'identificazione degli IOC è fondamentale per poter valutare le proporzioni dell'incidente e per poter attivare le procedure di incident response.