

S9L3

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

Ho utilizzato il documento in allegato per aprire la cattura effettuata su WireShark. Una volta aperta la cattura sono riuscito a riordinare le richieste fatte, ciò che balza subito all’occhio è l’insistenza di un determinato IP nell’inoltrare pacchetti su ogni porta (Vedi Figura 2). Ciò ci fa pensare ad un attaccante intenzionato a scannerizzare le porte aperte sulla nostra rete così da impacchettare un attacco su misura.

Conversation Settings		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	Bits/s A → B	Bits/s B → A
Name resolution		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		
	Absolute start time	192.168.200.100	58938	192.168.200.150	3	2	134 bytes	966		1	74 bytes	1	60 bytes	36.873582	0.0003		
Limit to display filter		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		
Copy		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		
	Follow Stream...	192.168.200.100	41348	192.168.200.150	9	2	134 bytes	429		1	74 bytes	1	60 bytes	36.820242	0.0002		
Graph...		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		
Protocol		192.168.200.100	58814	192.168.200.150	13	2	134 bytes	235		1	74 bytes	1	60 bytes	36.801464	0.0002		
	Bluetooth	192.168.200.100	53648	192.168.200.150	14	2	134 bytes	382		1	74 bytes	1	60 bytes	36.815493	0.0003		
	DCCP	192.168.200.100	42454	192.168.200.150	15	2	134 bytes	233		1	74 bytes	1	60 bytes	36.801319	0.0002		
Ethernet		192.168.200.100	36316	192.168.200.150	16	2	134 bytes	748		1	74 bytes	1	60 bytes	36.849675	0.0003		
	FC	192.168.200.100	39712	192.168.200.150	17	2	134 bytes	943		1	74 bytes	1	60 bytes	36.871253	0.0002		
	FDDI	192.168.200.100	57066	192.168.200.150	18	2	134 bytes	743		1	74 bytes	1	60 bytes	36.849341	0.0002		
IEEE 802.11		192.168.200.100	49988	192.168.200.150	19	2	134 bytes	102		1	74 bytes	1	60 bytes	36.787346	0.0002		
	IEEE 802.15.4	192.168.200.100	48812	192.168.200.150	20	2	134 bytes	285		1	74 bytes	1	60 bytes	36.806188	0.0003		
	IPv4	192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	3	206 bytes	1	74 bytes	36.774615	0.0012			
IPv6		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			
	IPX	192.168.200.100	37888	192.168.200.150	24	2	134 bytes	800		1	74 bytes	1	60 bytes	36.854687	0.0002		
JXTA		192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	3	206 bytes	1	74 bytes	36.776512	0.0015			
	MPTCP	192.168.200.100	34782	192.168.200.150	26	2	134 bytes	159		1	74 bytes	1	60 bytes	36.792890	0.0002		
	NCP	192.168.200.100	52294	192.168.200.150	27	2	134 bytes	407		1	74 bytes	1	60 bytes	36.817415	0.0002		
Filter list for specific type		192.168.200.100	40542	192.168.200.150	28	2	134 bytes	489		1	74 bytes	1	60 bytes	36.826423	0.0002		
		192.168.200.100	57177	192.168.200.150	29	2	134 bytes	686		1	74 bytes	1	60 bytes	36.844944	0.0002		

Close

Help

Figura 1

Ethernet · 2	IPv4 · 2	IPv6	TCP · 1026	UDP · 1	
Address A		Port A Address B		Port B ▾	Pac
192.168.200.100	37396	192.168.200.150		1	
192.168.200.100	34748	192.168.200.150		2	
192.168.200.100	58938	192.168.200.150		3	
192.168.200.100	43056	192.168.200.150		4	
192.168.200.100	54282	192.168.200.150		5	
192.168.200.100	40874	192.168.200.150		6	
192.168.200.100	52702	192.168.200.150		7	
192.168.200.100	47720	192.168.200.150		8	
192.168.200.100	41348	192.168.200.150		9	
192.168.200.100	46014	192.168.200.150		10	
192.168.200.100	37252	192.168.200.150		11	
192.168.200.100	41700	192.168.200.150		12	
192.168.200.100	58814	192.168.200.150		13	
192.168.200.100	53648	192.168.200.150		14	
192.168.200.100	42454	192.168.200.150		15	
192.168.200.100	36316	192.168.200.150		16	
192.168.200.100	39712	192.168.200.150		17	
192.168.200.100	57066	192.168.200.150		18	
192.168.200.100	49988	192.168.200.150		19	
192.168.200.100	48812	192.168.200.150		20	
192.168.200.100	41182	192.168.200.150		21	
192.168.200.100	55656	192.168.200.150		22	
192.168.200.100	41304	192.168.200.150		23	
192.168.200.100	37888	192.168.200.150		24	
192.168.200.100	60632	192.168.200.150		25	
192.168.200.100	34782	192.168.200.150		26	
192.168.200.100	52294	192.168.200.150		27	
192.168.200.100	40542	192.168.200.150		28	

Figura 2

Nella Figura 3 possiamo notare quali porte sono state rilevate “aperte” da parte dell’attaccante. E’ possibile notare in fondo alla figura le porte aperte tramite l’osservazione delle risposte ottenute.

//Nota: Le porte aperte sono quelle che hanno ottenuto lo scambio di 4 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	Bits/s A → B	Bits/s B → A
192.168.200.100	47100	192.168.200.150	1010	2	134 bytes	579	1	74 bytes	1	60 bytes	36.834310	0.0002		
192.168.200.100	48408	192.168.200.150	1011	2	134 bytes	860	1	74 bytes	1	60 bytes	36.862758	0.0008		
192.168.200.100	53308	192.168.200.150	1012	2	134 bytes	895	1	74 bytes	1	60 bytes	36.866735	0.0003		
192.168.200.100	43698	192.168.200.150	1013	2	134 bytes	615	1	74 bytes	1	60 bytes	36.836725	0.0014		
192.168.200.100	42700	192.168.200.150	1014	2	134 bytes	66	1	74 bytes	1	60 bytes	36.781160	0.0001		
192.168.200.100	44580	192.168.200.150	1015	2	134 bytes	260	1	74 bytes	1	60 bytes	36.800393	0.0001		
192.168.200.100	39078	192.168.200.150	1016	2	134 bytes	273	1	74 bytes	1	60 bytes	36.805289	0.0001		
192.168.200.100	36474	192.168.200.150	1017	2	134 bytes	1017	1	74 bytes	1	60 bytes	36.878092	0.0002		
192.168.200.100	57032	192.168.200.150	1018	2	134 bytes	751	1	74 bytes	1	60 bytes	36.849909	0.0001		
192.168.200.100	40832	192.168.200.150	1019	2	134 bytes	195	1	74 bytes	1	60 bytes	36.796479	0.0001		
192.168.200.100	33384	192.168.200.150	1020	2	134 bytes	640	1	74 bytes	1	60 bytes	36.839439	0.0002		
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	38352	192.168.200.150	1022	2	134 bytes	594	1	74 bytes	1	60 bytes	36.835363	0.0026		
192.168.200.100	59292	192.168.200.150	1023	2	134 bytes	463	1	74 bytes	1	60 bytes	36.823536	0.0003		
192.168.200.100	37738	192.168.200.150	1024	2	134 bytes	404	1	74 bytes	1	60 bytes	36.817332	0.0003		
192.168.200.100	41182	192.168.200.150	21	4	280 bytes	9	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	53060	192.168.200.150	80	4	280 bytes	0	3	206 bytes	1	74 bytes	23.764215	0.0007		
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	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	42046	192.168.200.150	513	4	280 bytes	480	3	206 bytes	1	74 bytes	36.835398	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		

Figura 3

No.	Time	Source	Destination	Protocol	Length	Info
15	36.774366305	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	36.774405627	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	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=64
20	36.774685652	192.168.200.100	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774693696	192.168.200.150	192.168.200.100	TCP	60	443 → 53062 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774709464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711872	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775378880	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
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
32	36.775593080	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796388	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797984	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
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
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
39	36.775931654	192.168.200.100	192.168.200.150	TCP	60	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Figura 4