

# S9L5

## Threat Intelligence e IoC

L'obiettivo dell'analisi odierna è esaminare una cattura di rete effettuata con Wireshark, al fine di identificare e analizzare eventuali **Indicatori di Compromissione (IoC)**.

Questi indicatori potrebbero segnalare la presenza di attacchi in corso o attività sospette nella rete. Una volta individuati gli IoC, sarà necessario formulare ipotesi sui **potenziali vettori di attacco** utilizzati dai malintenzionati per compromettere la rete o i dispositivi connessi.

Infine, si proporranno azioni concrete per mitigare gli impatti dell'attacco attuale e implementare misure preventive che possano ridurre il rischio di attacchi simili in futuro.

Di seguito troviamo due schermate che mostrano una parte del traffico di rete a disposizione.

No.	Time	Source	Destination	Protocol	Length Info
1	8:09:00:00:00:00	192.168.200.159	192.168.200.159	TCP	264 New Announcement METASPOLOITABLE Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential...
2	23.784214995	192.168.200.109	192.168.200.159	TCP	74 53069 - 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810522427 Tscr=0 WS=128
3	23.784287789	192.168.200.109	192.168.200.159	TCP	74 53876 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810522428 Tscr=0 WS=128
4	23.784777323	192.168.200.159	192.168.200.109	TCP	74 89 - 53066 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810522428 Tscr=0 WS=128
5	23.784777447	192.168.200.159	192.168.200.109	TCP	69 443 - 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.784815289	192.168.200.109	192.168.200.159	TCP	66 53069 - 88 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810522428 Tscr=4294951165
7	23.784899991	192.168.200.109	192.168.200.159	TCP	66 53069 - 88 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810522428 Tscr=4294951165
8	23.784900001	192.168.200.109	192.168.200.159	TCP	66 53069 - 88 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810522428 Tscr=4294951165
9	28.71644619	PcsCompu_fd:37:1e	PcsCompu_fd:37:1e	ARP	42 192.168.200.109 Is at 00:00:27:39:7d:fe
10	28.77485257	PcsCompu_fd:37:1e	PcsCompu_fd:37:1e	ARP	42 who has 192.168.200.159 Tell 192.168.200.109
11	28.77485299	PcsCompu_fd:37:1e	PcsCompu_fd:37:1e	ARP	60 192.168.200.159 Is at 00:00:27:fd:87:1e
12	36.774143445	192.168.200.109	192.168.200.159	TCP	74 41394 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tscr=0 WS=128
13	36.774218110	192.168.200.109	192.168.200.159	TCP	74 56126 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tscr=0 WS=128
14	36.774257841	192.168.200.109	192.168.200.159	TCP	74 33876 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tscr=0 WS=128
15	36.774257853	192.168.200.109	192.168.200.159	TCP	74 56126 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535437 Tscr=0 WS=128
16	36.774409827	192.168.200.109	192.168.200.159	TCP	74 52359 - 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128
17	36.774535534	192.168.200.109	192.168.200.159	TCP	74 46138 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128
18	36.774614776	192.168.200.109	192.168.200.159	TCP	74 41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128
19	36.774685585	192.168.200.109	192.168.200.159	TCP	74 23 - 41394 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tscr=810535437 WS=64
20	36.774685652	192.168.200.159	192.168.200.109	TCP	74 111 - 56129 [SYN, ACK] Seq=0 Ack=1 Win=64256 Len=0 Tsvl=810535438 Tscr=4294952466
21	36.774685696	192.168.200.159	192.168.200.109	TCP	69 443 - 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685731	192.168.200.159	192.168.200.109	TCP	69 554 - 56833 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685739	192.168.200.159	192.168.200.109	TCP	69 556 - 52389 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774710454	192.168.200.109	192.168.200.159	TCP	68 41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535438 Tscr=4294952466
25	36.774711972	192.168.200.109	192.168.200.159	TCP	66 56129 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535438 Tscr=4294952466
26	36.775141194	192.168.200.159	192.168.200.109	TCP	69 993 - 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141237	192.168.200.159	192.168.200.109	TCP	74 21 - 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tscr=810535438 WS=64
28	36.775140448	192.168.200.109	192.168.200.159	TCP	66 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535438 Tscr=4294952466
29	36.775337889	192.168.200.109	192.168.200.159	TCP	74 59174 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128
30	36.775386694	192.168.200.109	192.168.200.159	TCP	74 56556 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535438 Tscr=0 WS=128
31	36.775386749	192.168.200.109	192.168.200.159	TCP	74 55962 - 86 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535439 Tscr=0 WS=128
32	36.775568939	192.168.200.109	192.168.200.159	TCP	69 41304 - 23 [SYN, ACK] Seq=0 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466
33	36.775619454	192.168.200.109	192.168.200.159	TCP	68 41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466
34	36.775652497	192.168.200.109	192.168.200.159	TCP	66 56129 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466
35	36.775796939	192.168.200.109	192.168.200.159	TCP	74 22 - 55956 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tscr=810535439 WS=64
36	36.775797094	192.168.200.159	192.168.200.109	TCP	74 88 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tscr=810535439 WS=64
37	36.775803786	192.168.200.109	192.168.200.159	TCP	66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466
38	36.775813239	192.168.200.109	192.168.200.159	TCP	66 53062 - 86 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466
39	36.775861964	192.168.200.109	192.168.200.159	TCP	66 41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466
40	36.775957870	192.168.200.109	192.168.200.159	TCP	66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466
41	36.776058533	192.168.200.159	192.168.200.109	TCP	66 53062 - 88 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466
42	36.776175338	192.168.200.109	192.168.200.159	TCP	74 50584 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535439 Tscr=0 WS=128
43	36.776233388	192.168.200.109	192.168.200.159	TCP	74 54226 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535439 Tscr=0 WS=128
44	36.776333661	192.168.200.109	192.168.200.159	TCP	74 34548 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
45	36.776385694	192.168.200.109	192.168.200.159	TCP	74 33402 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
46	36.776402594	192.168.200.109	192.168.200.159	TCP	74 49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
47	36.776451284	192.168.200.159	192.168.200.109	TCP	69 199 - 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.159	192.168.200.109	TCP	69 895 - 54228 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776496101	192.168.200.109	192.168.200.159	TCP	74 144 - 50900 [SYN] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
50	36.776496366	192.168.200.109	192.168.200.159	TCP	74 33209 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
51	36.776512221	192.168.200.109	192.168.200.159	TCP	74 60632 - 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
52	36.776568669	192.168.200.109	192.168.200.159	TCP	74 49654 - 116 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
53	36.776671272	192.168.200.109	192.168.200.159	TCP	74 37282 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
54	36.776728175	192.168.200.109	192.168.200.159	TCP	74 54898 - 37289 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
55	36.776813123	192.168.200.159	192.168.200.109	TCP	69 687 - 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776813124	192.168.200.109	192.168.200.159	TCP	74 34548 - 34648 [SYN] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
57	36.776849828	192.168.200.109	192.168.200.159	TCP	74 44452 - 33042 [RST, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tscr=810535440 WS=64
58	36.776904922	192.168.200.159	192.168.200.109	TCP	69 256 - 40814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776984961	192.168.200.109	192.168.200.159	TCP	74 139 - 46998 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tscr=810535440 WS=64
60	36.776985001	192.168.200.159	192.168.200.109	TCP	69 143 - 43206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776985044	192.168.200.109	192.168.200.159	TCP	74 25 - 66634 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tscr=810535440 WS=64
62	36.776985082	192.168.200.109	192.168.200.159	TCP	69 110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776985120	192.168.200.109	192.168.200.159	TCP	74 53 - 37289 [SYN] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsvl=4294952466 Tscr=810535440 WS=64
64	36.776988002	192.168.200.109	192.168.200.159	TCP	69 609 - 54860 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.777143014	192.168.200.109	192.168.200.159	TCP	74 55998 - 767 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
66	36.777644192	192.168.200.109	192.168.200.159	TCP	66 46996 - 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=4294952466
67	36.776983232	192.168.200.109	192.168.200.159	TCP	66 60632 - 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=4294952466
68	36.776983878	192.168.200.109	192.168.200.159	TCP	66 37282 - 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535440 Tscr=4294952466
69	36.777118481	192.168.200.159	192.168.200.109	TCP	66 487 - 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36.777143016	192.168.200.109	192.168.200.159	TCP	74 56598 - 767 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
71	36.777186931	192.168.200.109	192.168.200.159	TCP	74 35538 - 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
72	36.777233994	192.168.200.109	192.168.200.159	TCP	74 49128 - 99 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
73	36.777233934	192.168.200.109	192.168.200.159	TCP	74 49128 - 99 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535440 Tscr=0 WS=128
74	36.777343632	192.168.200.109	192.168.200.159	TCP	69 607 - 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777343741	192.168.200.109	192.168.200.159	TCP	69 636 - 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777437918	192.168.200.109	192.168.200.159	TCP	74 36138 - 588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128
77	36.777522494	192.168.200.109	192.168.200.159	TCP	74 52428 - 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsvl=810535441 Tscr=0 WS=128
78	36.777623082	192.168.200.109	192.168.200.159	TCP	69 98 - 34120 [RST, ACK] Seq=1 Ack=1 Win=

## Analisi della rete

Dall'analisi del traffico catturato tramite Wireshark, emergono chiari segnali di un'attività di scansione delle porte TCP condotta tramite uno strumento automatizzato, probabilmente utilizzando **Nmap** con i comandi `-sT` o `-T5 -Pn`. Questa modalità, che rappresenta una **scansione TCP completa (TCP Connect Scan)**, prevede il completamento del 3-way handshake per ogni porta analizzata, rendendola meno furtiva rispetto ad altre tecniche, ma estremamente efficace per identificare i servizi attivi su un host.

L'host sorgente coinvolto nella scansione è **192.168.200.100**, mentre l'host di destinazione è **192.168.200.150**. Il traffico analizzato evidenzia un comportamento sistematico: una sequenza di pacchetti SYN viene inviata verso un'ampia gamma di porte dell'host target. In risposta, l'host di destinazione mostra tre comportamenti distinti:

1. **SYN**, che indica la richiesta di connessione ad una porta.
2. **SYN/ACK**, che indica la presenza di porte aperte e quindi servizi attivi.
3. **RST**, che segnala che alcune porte sono chiuse o una chiusura di connessione.

L'uso della modalità `-sT` comporta il completamento delle connessioni TCP, confermato dalla presenza di pacchetti ACK nei flussi di traffico osservati. Questo tipo di scansione, pur essendo meno stealth rispetto alla scansione SYN (che si limita alla fase iniziale del 3-way handshake), permette di raccogliere informazioni più dettagliate sull'host di destinazione. Inoltre, l'opzione `-T4` o `-T5` indica una configurazione pensata per eseguire la scansione a velocità aumentata, generando un numero elevato di pacchetti in un intervallo di tempo ridotto. Questo spiega l'alta densità di traffico catturato durante l'analisi.

Il comportamento osservato risulta coerente con un'attività di ricognizione mirata, probabilmente volta a identificare i servizi attivi e lo stato delle porte sull'host di destinazione. Il completamento delle connessioni TCP lascia tracce evidenti nei log del sistema target, aumentando le probabilità di rilevamento da parte di firewall o sistemi di intrusion detection (IDS). Tuttavia, l'analisi mostra che nessun payload applicativo è stato scambiato, confermando che l'obiettivo principale era esclusivamente quello di sondare lo stato delle porte senza instaurare connessioni operative.

### Indicatori di compromissione (IoC):

Dall'analisi emergono diversi **Indicatori di Compromissione**, tra cui:

- **Sequenza di pacchetti SYN distribuiti su molte porte**: un segnale tipico di una scansione.
- **Completamento del 3-way handshake TCP**: caratteristico della scansione TCP Connect.
- **Presenza di risposte SYN/ACK**: evidenza di porte aperte e servizi attivi sull'host target.
- **Pacchetti RST**: indicano che molte porte sono chiuse.
- **Velocità elevata del traffico**: coerente con l'opzione `-T4` o `-T5` utilizzata per eseguire la scansione in tempi ridotti.

### Vettori di attacco:

Questa attività rappresenta una fase iniziale di un potenziale attacco informatico. Attraverso la scansione delle porte, l'host sorgente potrebbe:

- **Raccogliere informazioni sui servizi attivi**: come server web (porta 80/443), database o servizi di gestione remota.
- **Preparare attacchi successivi**: sfruttando eventuali vulnerabilità associate alle porte aperte o ai servizi individuati.

Un aspetto particolarmente preoccupante è che l'host sorgente **192.168.200.100** si trova all'interno della rete, il che suggerisce che l'attività di scansione sia stata avviata da una macchina interna. Questa situazione cambia radicalmente lo scenario, poiché l'attacco potrebbe provenire da un utente malintenzionato che ha già accesso alla rete aziendale o da un dispositivo compromesso. Di conseguenza, diventa estremamente importante approfondire le indagini per comprendere come l'attaccante abbia ottenuto accesso alla rete interna e per prevenire ulteriori compromissioni.

### Azioni consigliate:

Per ridurre l'impatto di attività simili e migliorare la sicurezza della rete, si raccomandano le seguenti azioni:

1. **Identificazione dell'host sorgente**: Condurre un'analisi approfondita sul dispositivo **192.168.200.100** per determinare se sia stato compromesso o se l'attività sia stata avviata intenzionalmente da un insider.

2. **Monitoraggio dei log di rete:** L'attività di scansione lascia tracce evidenti. Un'analisi regolare dei log può facilitare l'identificazione precoce di comportamenti anomali.
3. **Configurazione dei firewall:** Limitare temporaneamente il protocollo TCP in modo da bloccare temporaneamente la scansione ma non isolare totalmente l'indirizzo IP attaccante. In questo caso il dispositivo risulterà comunque operativo ma non potrà più effettuare una scansione dei dispositivi.
4. **Implementazione di sistemi IDS/IPS:** Utilizzare soluzioni di rilevamento delle intrusioni per identificare e bloccare automaticamente attività sospette, come scansioni a tappeto.
5. **Implementazione di politiche di rate limiting:** Configurare dispositivi di rete (come switch e router) per limitare il numero di richieste messe verso le porte o verso un singolo host. Questo può impedire scansioni a tappeto o attività automatizzate ad alta velocità, riducendo la probabilità di compromissioni e sovraccarichi.

## Conclusione

L'attività catturata rappresenta un chiaro esempio di una scansione TCP Connect eseguita con il comando nmap **-sT -T4 o -T5 -Pn**. Questo tipo di ricognizione è volto a identificare lo stato delle porte e dei servizi sull'host di destinazione. Tuttavia, il fatto che la scansione provenga da un host interno (192.168.200.150) indica un possibile compromesso di un dispositivo all'interno della rete o un'azione intenzionale da parte di un insider. Questo richiede un'indagine urgente e approfondita, poiché un attacco dall'interno potrebbe rappresentare una minaccia significativa per l'intera infrastruttura. È fondamentale adottare contromisure proattive per rilevare e mitigare tempestivamente tali attività e rafforzare la sicurezza della rete.