

# Threat Intelligence

&

IOC

**Amin El Kassimi**

CyberSecurity EN  
Paolo Rampino  
Feb 6, 2026

## Executive Summary

Mission.....	1
Analisi tecnica "Top-Down" (Statistiche) .....	2
Risultati Analisi Tecnica Top Down.....	3
Prossimi passi: Filtri per ridurre il "rumore" .....	8
Scansione / tentativi di connessione.....	9
🛡️ Strategia di Mitigazione e Difesa (Post-Analisi).....	11

## Mission

Viene fornita una cattura di rete effettuata con Wireshark. Analizzare la cattura attentamente e rispondere ai seguenti quesiti:

1. Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
2. In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati.
3. Alla Fine consigliare un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

Pipeline ideale:

1. **Triage** (statistiche)
2. **Riduzione** (filtri)
3. **Selezione evidenze** (stream / conversazioni)
4. **Correlazione** (timeline: chi parla con chi, quando, con che protocollo)
5. **Hypothesis testing** (es: "scan SMB?" → cerco SMB/445, NTLM, tentativi)
6. **Azioni** (containment + hardening + detection)

## Analisi tecnica "Top-Down" (Statistiche)

Prima di guardare i singoli pacchetti, bisogna guardare la foresta, non gli alberi.

2083 pacchetti *non sono troppi* (Wireshark ride), ma sono **troppi da leggere a occhio** uno per uno.

In questi casi si procede come in incident response:

**triage → riduzione → evidenze → ipotesi → contromisure.** L'IA può aiutare molto, ma solo se le sida **un sottoinsieme informativo**, non la "Divina Commedia dei pacchetti".

### Triage in Wireshark (10 minuti, massima resa)

#### 1) Statistics → Protocol Hierarchy

Indica dove sta il volume: DNS? HTTP? TLS? SMB? RDP? ICMP?

→ Questo già restringe il campo.

#### 2) Statistics → Conversations (Tab: Ethernet / IPv4 / TCP / UDP)

Ordina per:

- **Bytes**
- **Packets**
- **Duration**

Cerca:

- IP "chiacchieroni" (molti pacchetti)
- connessioni brevissime ripetute (beaconing / scanning)
- una macchina che parla con *tantissimi* IP (scan) o con *uno strano* IP esterno (C2)

#### 3) Statistics → DNS (se presente)

Guarda domini richiesti, NXDOMAIN ripetuti, query strane.

#### 4) Statistics → Endpoints

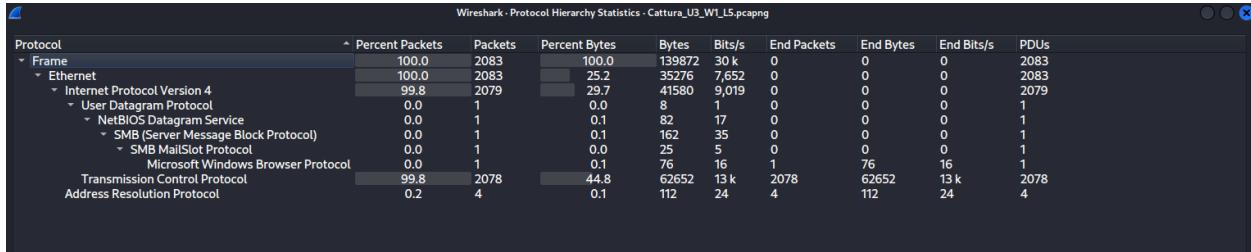
Individua host interni "anomali".

**5) Statistics > I/O Graph:** Permette di vedere i picchi di traffico nel tempo. Un picco improvviso di pacchetti può indicare l'inizio di un exploit o di un brute force.

Queste 4 viste trasformano 2083 pacchetti in **5-20 candidati**.

## Risultati Analisi Tecnica Top Down

### 1) Statistics → Protocol Hierarchy



### Evidenze

- 2083 pacchetti totali
- ~99.8% **IPv4**
- ~99.8% **TCP** (2078 pacchetti)
- **UDP praticamente assente**
- **DNS assente**
- Presenza **marginale** di:
  - NetBIOS Datagram Service
  - SMB Mailslot
  - Microsoft Windows Browser Protocol (1 pacchetto)

### Indicazioni

- Traffico **quasi esclusivamente TCP**
- Assenza di DNS → **nessuna risoluzione di nomi**
- SMB/NetBIOS trascurabile → **non file sharing attivo**

## 2) Statistics → Conversations → IPv4 (ordinato per Bytes)

DCCP	Ethernet - 2	<b>IPv4 - 2</b>	IPv6	TCP - 1026	UDP - 1								
Address A	Address 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	192.168.200.150		2,078	139 kB	1	1,052	78 kB	1,026	62 kB	23.764215	13.1147	47 kbps	37 kbps
192.168.200.150	192.168.200.255		0	1 286 bytes	0	1	286 bytes	0	0 bytes	0.000000	0.0000		

### Conversazione dominante

- 192.168.200.100 ↔ 192.168.200.150
  - **2078 pacchetti**
  - **139 KB**
  - Comunicazione **bidirezionale**
  - Durata ~13 s
  - Bitrate costante (~ 47 kbps / 37 kbps)

### Altra voce

- 192.168.200.150 → 192.168.200.255
  - 1 pacchetto (broadcast)

### Indicazioni

- **Un solo flusso rilevante**
  - Nessun traffico esterno
  - Pattern **point-to-point interno**
-

## 2.1) Statistics → Conversations → TCP (estratti)

DCCP	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	Flows
192.168.200.100	32792	192.168.200.150	218	2	134 bytes	526	1	74 bytes	1	60 bytes	36.829887	0.0002			0
192.168.200.100	32794	192.168.200.150	641	2	134 bytes	931	1	74 bytes	1	60 bytes	36.870238	0.0002			0
192.168.200.100	32820	192.168.200.150	49	2	134 bytes	518	1	74 bytes	1	60 bytes	36.828836	0.0001			0
192.168.200.100	32852	192.168.200.150	688	2	134 bytes	948	1	74 bytes	1	60 bytes	36.871590	0.0002			0
192.168.200.100	32894	192.168.200.150	890	2	134 bytes	637	1	74 bytes	1	60 bytes	36.838788	0.0006			0
192.168.200.100	32922	192.168.200.150	382	2	134 bytes	287	1	74 bytes	1	60 bytes	36.806271	0.0003			0
192.168.200.100	32950	192.168.200.150	41	2	134 bytes	999	1	74 bytes	1	60 bytes	36.875958	0.0002			0
192.168.200.100	32976	192.168.200.150	570	2	134 bytes	74	1	74 bytes	1	60 bytes	36.782215	0.0002			0
192.168.200.100	32996	192.168.200.150	1021	2	134 bytes	425	1	74 bytes	1	60 bytes	36.848545	0.0003			0
192.168.200.100	33002	192.168.200.150	445	4	286 bytes	15	3	206 bytes	1	74 bytes	36.870205	0.0002			0
192.168.200.100	33050	192.168.200.150	448	2	134 bytes	809	1	74 bytes	1	60 bytes	36.855520	0.0002			0
192.168.200.100	33050	192.168.200.150	373	2	134 bytes	826	1	74 bytes	1	60 bytes	36.857281	0.0002			0
192.168.200.100	33056	192.168.200.150	521	2	134 bytes	157	1	74 bytes	1	60 bytes	36.792679	0.0002			0
192.168.200.100	33058	192.168.200.150	411	2	134 bytes	270	1	74 bytes	1	60 bytes	36.804717	0.0002			0
192.168.200.100	33058	192.168.200.150	299	2	134 bytes	511	1	74 bytes	1	60 bytes	36.828373	0.0003			0
192.168.200.100	33102	192.168.200.150	51	2	134 bytes	79	1	74 bytes	1	60 bytes	36.782582	0.0003			0
192.168.200.100	33114	192.168.200.150	348	2	134 bytes	262	1	74 bytes	1	60 bytes	36.803843	0.0002			0
192.168.200.100	33206	192.168.200.150	143	2	134 bytes	18	1	74 bytes	1	60 bytes	36.776496	0.0004			0
192.168.200.100	33250	192.168.200.150	355	2	134 bytes	299	1	74 bytes	1	60 bytes	36.807513	0.0002			0
192.168.200.100	33280	192.168.200.150	982	2	134 bytes	234	1	74 bytes	1	60 bytes	36.801427	0.0002			0
192.168.200.100	33332	192.168.200.150	238	2	134 bytes	366	1	74 bytes	1	60 bytes	36.813553	0.0003			0
192.168.200.100	33384	192.168.200.150	1020	2	134 bytes	640	1	74 bytes	1	60 bytes	36.839439	0.0002			0
192.168.200.100	33430	192.168.200.150	517	2	134 bytes	193	1	74 bytes	1	60 bytes	36.796309	0.0003			0
192.168.200.100	33452	192.168.200.150	77	2	134 bytes	744	1	74 bytes	1	60 bytes	36.849410	0.0001			0
192.168.200.100	33460	192.168.200.150	112	2	134 bytes	673	1	74 bytes	1	60 bytes	36.842749	0.0002			0
192.168.200.100	33566	192.168.200.150	63	2	134 bytes	305	1	74 bytes	1	60 bytes	36.808437	0.0002			0
192.168.200.100	33618	192.168.200.150	91	2	134 bytes	960	1	74 bytes	1	60 bytes	36.872641	0.0003			0
192.168.200.100	33698	192.168.200.150	615	2	134 bytes	558	1	74 bytes	1	60 bytes	36.832322	0.0002			0
192.168.200.100	33718	192.168.200.150	359	2	134 bytes	93	1	74 bytes	1	60 bytes	36.785943	0.0003			0
192.168.200.100	33782	192.168.200.150	172	2	134 bytes	272	1	74 bytes	1	60 bytes	36.805267	0.0001			0
192.168.200.100	33876	192.168.200.150	443	2	134 bytes	1	1	74 bytes	1	60 bytes	23.764288	0.0005			0
192.168.200.100	33878	192.168.200.150	443	2	134 bytes	4	1	74 bytes	1	60 bytes	36.774258	0.0004			0
192.168.200.100	33884	192.168.200.150	408	2	134 bytes	620	1	74 bytes	1	60 bytes	36.837045	0.0011			0
192.168.200.100	33896	192.168.200.150	763	2	134 bytes	149	1	74 bytes	1	60 bytes	36.791956	0.0002			0
192.168.200.100	33900	192.168.200.150	764	2	134 bytes	777	1	74 bytes	1	60 bytes	36.800007	0.0007			0
192.168.200.100	33910	192.168.200.150	511	2	134 bytes	222	1	74 bytes	1	60 bytes	36.800059	0.0003			0
192.168.200.100	33948	192.168.200.150	300	2	134 bytes	957	1	74 bytes	1	60 bytes	36.877281	0.0002			0
192.168.200.100	33950	192.168.200.150	720	2	134 bytes	937	1	74 bytes	1	60 bytes	36.870868	0.0001			0
192.168.200.100	33994	192.168.200.150	620	2	134 bytes	961	1	74 bytes	1	60 bytes	36.872660	0.0003			0
192.168.200.100	34004	192.168.200.150	528	2	134 bytes	203	1	74 bytes	1	60 bytes	36.797483	0.0003			0
192.168.200.100	34072	192.168.200.150	843	2	134 bytes	718	1	74 bytes	1	60 bytes	36.847269	0.0002			0
192.168.200.100	34024	192.168.200.150	833	2	134 bytes	395	1	74 bytes	1	60 bytes	36.816349	0.0002			0
192.168.200.100	34030	192.168.200.150	1005	2	134 bytes	843	1	74 bytes	1	60 bytes	36.861458	0.0004			0
192.168.200.100	34064	192.168.200.150	96	2	134 bytes	421	1	74 bytes	1	60 bytes	36.819024	0.0006			0
192.168.200.100	34094	192.168.200.150	645	2	134 bytes	662	1	74 bytes	1	60 bytes	36.841512	0.0003			0
192.168.200.100	34120	192.168.200.150	98	2	134 bytes	26	1	74 bytes	1	60 bytes	36.777303	0.0003			0
192.168.200.100	34130	192.168.200.150	230	2	134 bytes	979	1	74 bytes	1	60 bytes	36.874531	0.0002			0
192.168.200.100	34180	192.168.200.150	666	2	134 bytes	934	1	74 bytes	1	60 bytes	36.870574	0.0002			0
192.168.200.100	34182	192.168.200.150	177	2	134 bytes	326	1	74 bytes	1	60 bytes	36.810645	0.0002			0

## Pattern osservato

- **1026 stream TCP**
- Tutti:
  - 192.168.200.100 → 192.168.200.150
  - porte di destinazione diverse
  - 2 pacchetti per stream
  - ~134 bytes totali
  - Durata ~0.0002–0.0008 s
  - Nessun flusso persistente

## Indicazioni

- Tentativi di connessione **ripetuti e brevissimi**
- **Una porta diversa per ogni tentativo**
- Nessun trasferimento applicativo

### 3) Statistics → DNS

Packet Type	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total Packets	0					100%	-	-
rcode	0					100%	-	-
pcodes	0					100%	-	-
Service Stats	0					100%	-	-
request-response time (msec)	0					-	-	-
no. of unsolicited responses	0					-	-	-
no. of retransmissions	0					-	-	-
Response Stats	0					100%	-	-
no. of questions	0					-	-	-
no. of authorities	0					-	-	-
no. of answers	0					-	-	-
no. of additionals	0					-	-	-
Response	0					100%	-	-
Query Type	0					100%	-	-
Query Stats	0					100%	-	-
Qname Len	0					-	-	-
Label Stats	0					-	-	-
4th Level or more	0					-	-	-
3rd Level	0					-	-	-
2nd Level	0					-	-	-
1st Level	0					-	-	-
Query Name	0					100%	-	-
Payload size	0					100%	-	-
Class	0					100%	-	-
Answer Type	0					100%	-	-

## Risultato

- **DNS completamente assente**
- 0 query
- 0 risposte

## Indicazioni

- Nessuna comunicazione basata su nomi
- Attività **non dipendente da infrastruttura DNS**

**→ Sintesi IOC (impliciti dai dati)**

1. Alta cardinalità di connessioni TCP
2. Poche decine di byte per connessione
3. Porte di destinazione variabili
4. Un solo host sorgente
5. Assenza di handshake completi applicativi

**→ Pattern coerente con:**

- TCP port scanning interno
- Service discovery aggressivo
- Scan automatizzato (non umano)

**→ Nessuna evidenza di:**

- esfiltrazione dati
- C2
- malware beaconing
- brute force applicativo

## Prossimi passi: Filtri per ridurre il “rumore”

Applicare filtri che pescano eventi tipici da IOC, per "affettare" la cattura:

### 1.Scansione / tentativi di connessione

- SYN senza ACK (molti tentativi):

```
tcp.flags.syn==1 && tcp.flags.ack==0
```

### 2.Error/Reset

- Reset frequenti:

```
tcp.flags.reset==1
```

### 3.Ritrasmissioni (instabilità o evasione)

```
tcp.analysis.retransmission || tcp.analysis.fast_retransmission
```

### DNS “sospetto”

- tante query senza risposta/errore:

```
dns.flags.rcode != 0 || dns.flags.response == 0
```

### 4.HTTP in chiaro

```
http
```

### 5.Guarda solo l'inizio delle sessioni applicative.

- Sessioni Attive:

```
http.request o tls.handshake.type == 1
```

### 6.Nascondere il traffico di "sottofondo" che spesso sporca la cattura.

- Pulisce richiese arp:

```
!(arp or icmp or dns)
```

## Scansione / tentativi di connessione

- SYN senza ACK (molti tentativi):
   
tcp.flags.syn==1 && tcp.flags.ack==0

tcp.flags.syn==1 && tcp.flags.ack==0						
No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53069 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810522427 Tsecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	41305 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810522428 Tsecr=0 WS=128
12	36.77414345	192.168.200.100	192.168.200.150	TCP	74	41304 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810523437 Tsecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=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 Tsvl=810535437 Tsecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58638 - 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tsecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52356 - 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tsecr=0 WS=128
17	36.774455354	192.168.200.100	192.168.200.150	TCP	74	46130 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tsecr=0 WS=128
18	36.774485209	192.168.200.100	192.168.200.150	TCP	74	46130 - 1000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tsecr=0 WS=128
29	36.775376800	192.168.200.100	192.168.200.150	TCP	74	50174 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tsecr=0 WS=128
30	36.775388694	192.168.200.100	192.168.200.150	TCP	74	55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tsecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 - 89 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tsecr=0 WS=128
42	36.776178338	192.168.200.100	192.168.200.150	TCP	74	56684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tsecr=0 WS=128
43	36.776233898	192.168.200.100	192.168.200.150	TCP	74	54220 - 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tsecr=0 WS=128
44	36.776339618	192.168.200.100	192.168.200.150	TCP	74	34644 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
46	36.776482589	192.168.200.100	192.168.200.150	TCP	74	49814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
47	36.776512089	192.168.200.100	192.168.200.150	TCP	74	49814 - 269 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
48	36.776549366	192.168.200.100	192.168.200.150	TCP	74	33206 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
51	36.776551222	192.168.200.100	192.168.200.150	TCP	74	60632 - 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
52	36.776588696	192.168.200.100	192.168.200.150	TCP	74	49654 - 116 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
54	36.776728715	192.168.200.100	192.168.200.150	TCP	74	54899 - 599 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 - 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74	56994 - 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35638 - 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
72	36.777309622	192.168.200.100	192.168.200.150	TCP	74	49814 - 36 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tsecr=0 WS=128
73	36.777379394	192.168.200.100	192.168.200.150	TCP	74	40789 - 79 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535441 Tsecr=0 WS=128
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74	36138 - 589 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535441 Tsecr=0 WS=128
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74	52428 - 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535441 Tsecr=0 WS=128
80	36.777645927	192.168.200.100	192.168.200.150	TCP	74	41874 - 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535441 Tsecr=0 WS=128
81	36.777688998	192.168.200.100	192.168.200.150	TCP	74	51568 - 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535441 Tsecr=0 WS=128
90	36.7778179978	192.168.200.100	192.168.200.150	TCP	74	51450 - 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535441 Tsecr=0 WS=128
91	36.7778268161	192.168.200.100	192.168.200.150	TCP	74	48444 - 896 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535441 Tsecr=0 WS=128
92	36.777852026	192.168.200.100	192.168.200.150	TCP	74	54810 - 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535441 Tsecr=0 WS=128
93	36.778420791	192.168.200.100	192.168.200.150	TCP	74	34229 - 297 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535442 Tsecr=0 WS=128
97	36.778501226	192.168.200.100	192.168.200.150	TCP	74	34646 - 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535442 Tsecr=0 WS=128
98	36.778614095	192.168.200.100	192.168.200.150	TCP	74	54262 - 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535442 Tsecr=0 WS=128
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	49318 - 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535442 Tsecr=0 WS=128
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74	51276 - 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535442 Tsecr=0 WS=128
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74	39565 - 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535442 Tsecr=0 WS=128
107	36.778983153	192.168.200.100	192.168.200.150	TCP	74	47238 - 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535442 Tsecr=0 WS=128
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	56542 - 897 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535442 Tsecr=0 WS=128
111	36.779145904	192.168.200.100	192.168.200.150	TCP	74	49130 - 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535442 Tsecr=0 WS=128
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 Tsvl=810535443 Tsecr=0 WS=128

Frame 113: 94 bytes on wire (592 bits) on interface eth1, id 0  
 Ethernet II, Src: PCSystemTec\_39:7d:fe (08:00:27:39:7d:fe), Dst: PCSystemTec\_fd:87:1e (08:00:27:fd:87:1e)  
 Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150  
 Transmission Control Protocol, Src Port: 43140, Dst Port: 214, Seq: 0, Len: 0

0s\* cannot be found among the possible values for tcp.flags.ack.

Packets: 2083 - Displayed: 1026 (49.3%) - Marked: 1 (0.0%)

## Elevato numero di pacchetti TCP SYN

Tutti con SYN=1 e senza ACK → tentativi di apertura connessione non completati.

**Sorgente unica:** 192.168.200.100

**Host target:** 192.168.200.150

## Porte di destinazione molteplici e variabili

Es.: 80, 443, 23, 111, 135, 139, 445, 993, ecc.

### Payload nullo (Len=0)

Nessuna comunicazione applicativa.

### Ritmo rapido e regolare

Pattern automatizzato, non umano.

### Conclusioni:

→ **TCP SYN port scanning attivo**

→ Fase di **ricognizione** per individuare servizi aperti sull'host target.

Sunto dei punti chiave:

Dal punto di vista tecnico, l'host **192.168.200.100** invia esclusivamente pacchetti **TCP con flag SYN impostato**, che rappresentano il primo passo del three-way handshake TCP. Tuttavia, questi tentativi **non vengono mai seguiti da una sessione completa**: non si osservano pacchetti di dati né l'avvio di un protocollo applicativo. In pratica, l'host sorgente si limita a "bussare" alle porte del sistema di destinazione senza mai stabilire una comunicazione reale.

Questo comportamento è indicativo di una scansione perché le **porte di destinazione cambiano continuamente** (ad esempio 80, 443, 23, 111, 135, 445, ecc.) e ciascuna viene testata **una sola volta**. Inoltre, tutti i pacchetti SYN presentano caratteristiche identiche: stessa dimensione, stesse opzioni TCP e un pattern temporale regolare. Questi elementi sono tipici di un processo automatizzato, progettato per individuare rapidamente quali servizi rispondono su un determinato host.

Il traffico osservato non è compatibile con un utilizzo normale della rete. Un browser o un'applicazione legittima tende a contattare **un numero limitato di porte ben definite** e, soprattutto, completa il three-way handshake prima di iniziare lo scambio di dati. In questo caso, invece, **non è presente alcun payload** né traccia di protocolli applicativi, rafforzando l'ipotesi di un'attività di ricognizione.

Il pattern complessivo è coerente con una **TCP SYN scan (half-open scan)**, una tecnica classica di reconnaissance utilizzata per mappare i servizi esposti su un host senza stabilire connessioni complete. Questo tipo di scansione è comunemente implementato da strumenti come **nmap** o moduli di **Metasploit**.

Analizzando le porte sondate, è possibile intuire l'obiettivo dell'attaccante: la presenza di tentativi verso porte come **23 (Telnet)**, **111 (RPC)**, **135/139/445 (servizi Windows/Samba)** e **80/443 (servizi Web)** indica una fase di **enumerazione dei servizi attivi**, probabilmente finalizzata a individuare punti di ingresso vulnerabili e preparare successivi attacchi, come exploit mirati o tentativi di brute force.

Gli IOC indicano **un attacco in fase di ricognizione attiva**, con:

- **port scanning automatizzato**
- **enumerazione dei servizi**
- **ricerca di superfici di attacco note (Telnet, SMB vulnerabile)**

Non si osserva ancora exploit riuscito, ma **l'attacco è chiaramente in corso** e in una fase preliminare.

Convalidata la nostra ipotesi trovando relazioni con la Analisi **tecnica "Top-Down"** si procede con la messa in sicurezza di queste criticità per poi passare alle altre analisi meno critiche.

## 1) Strategia di Mitigazione e Difesa (Post-Analisi)

### 1. Azioni Immediate (Contenimento dell'attacco attuale)

Dato che è stata identificata un'attività di **TCP SYN Scan** automatizzata da parte dell'host 192.168.200.100:

- **Isolamento della Sorgente:** Configurare una regola ACL sul firewall o utilizzare iptables/nftables per droppare tutto il traffico proveniente dall'IP incriminato.
- **Chiusura dei Servizi non necessari:** Poiché l'attaccante ha enumerato servizi critici (Samba 3.0.20, Telnet port 23, RPC port 111), è prioritario spegnere i servizi identificati che non sono strettamente necessari all'operatività del laboratorio.
- **Interruzione dell'Enumerazione:** Disabilitare l'invio di pacchetti "Host Announcement" (protocollo BROWSER) per evitare che la versione esatta del software (Samba) venga esposta passivamente sulla rete.

### 2. Riduzione degli Impatti Futuri (Hardening)

Per evitare che un simile tentativo di ricognizione evolva in un'intrusione riuscita:

- **Patch Management (Focus Samba):** La versione 3.0.20 rilevata è estremamente vulnerabile. L'impatto si riduce drasticamente aggiornando il pacchetto o applicando le patch per le vulnerabilità RCE (Remote Code Execution) note.
- **Sostituzione Protocolli Insicuri:** Sostituire servizi in chiaro come **Telnet (23)** con protocolli criptati come SSH, limitando l'accesso solo tramite chiavi SSH e non password.
- **Network Segmentation:** Inserire la macchina "Metasploitable" in una VLAN isolata con regole di ingresso restrittive, affinché un eventuale compromissione non permetta il movimento laterale verso altri host della rete.

### 3. Monitoraggio e Detection (Prevenzione Attiva)

Per rilevare "bussate" automatizzate prima che l'attaccante trovi una falla:

- **Implementazione IDS/IPS:** Configurare **Snort** o **Suricata** con regole specifiche per il *Thresholding*. Esempio: "Se un IP invia più di 20 pacchetti SYN in 1 secondo verso porte diverse, genera un alert e blocca l'IP".
- **Analisi dei Log:** Non limitarsi a Wireshark; integrare i log di sistema (Syslog) per correlare i pacchetti RST/ACK visti in rete con i tentativi di accesso falliti lato server.
- **Port Knocking:** Per i servizi che devono restare aperti, implementare il *Port Knocking*: la porta rimane "chiusa" al SYN scan e si apre solo dopo che l'utente autorizzato ha inviato una sequenza specifica di pacchetti su porte predefinite.

