# Progetto S9 – L5

**Analisi di Threat Intelligence su Cattura di Traffico di Rete tramite Wireshark**

---

# Executive Summary:

Nel presente elaborato **ho analizzato una cattura di traffico di rete in formato `.pcapng` al fine di identificare eventuali Indicatori di Compromissione (IoC)**, ipotizzare possibili **vettori di attacco e** proporre **misure di contenimento e prevenzione.**

Dall'analisi è emersa un'attività riconducibile a un **port scanning sistematico**, effettuato dall'host **`192.168.200.100`** nei confronti del sistema **`192.168.200.150`**.

Il comportamento osservato **rappresenta una tipica fase di ricognizione preliminare a un potenziale attacco informatico.** Sono state quindi individuate **azioni correttive** immediate e s**trategie preventive per mitigare rischi futuri**.

---

# Introduzione:

L'obiettivo dell'esercizio è **applicare i principi di Threat Intelligence analizzando una cattura di rete tramite Wireshark**.

Ho seguito un approccio metodologico strutturato basato sulle fasi:

- Raccolta delle evidenze
- Elaborazione dei dati
- Analisi degli Indicatori di Compromissione
- Valutazione del rischio
- Definizione delle contromisure

**L'attività è stata svolta in ambiente Kali Linux, dopo aver trasferito la cattura tramite cartella condivisa da host Windows**.

---

# 1) Preparazione dell'ambiente

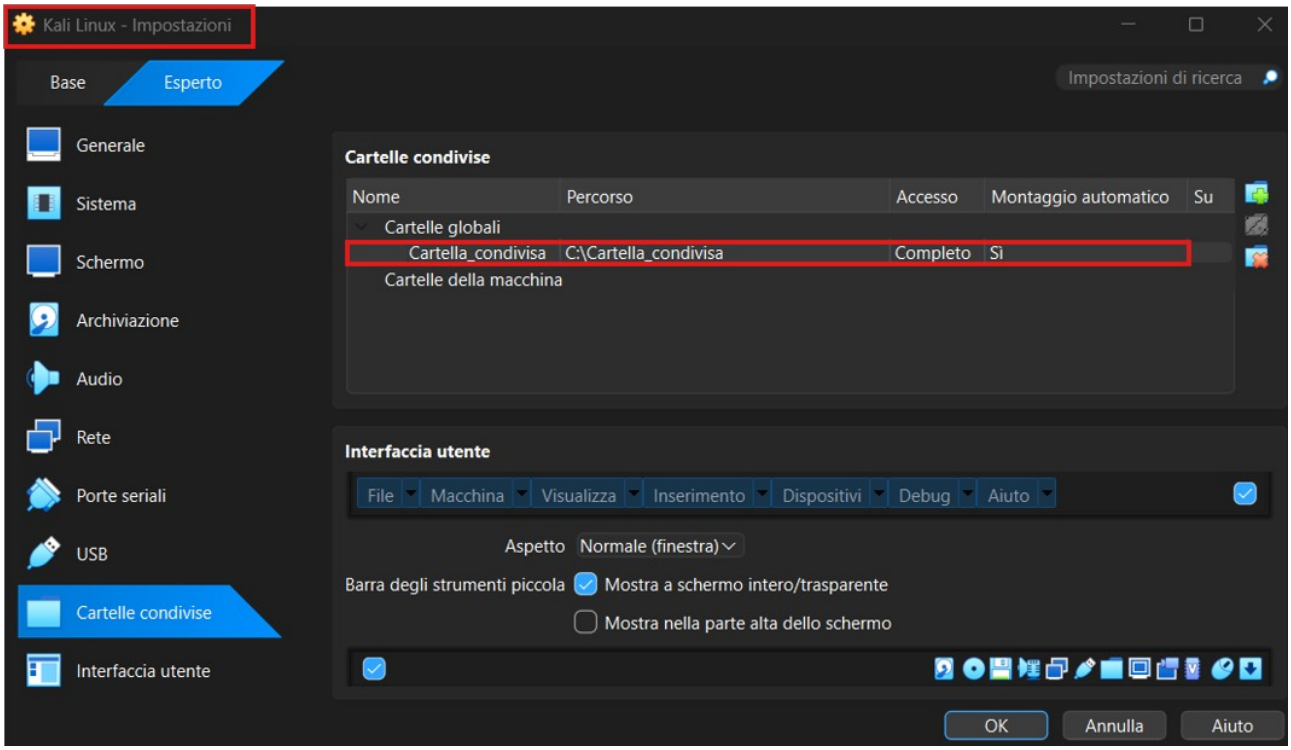
## Configurazione cartella condivisa

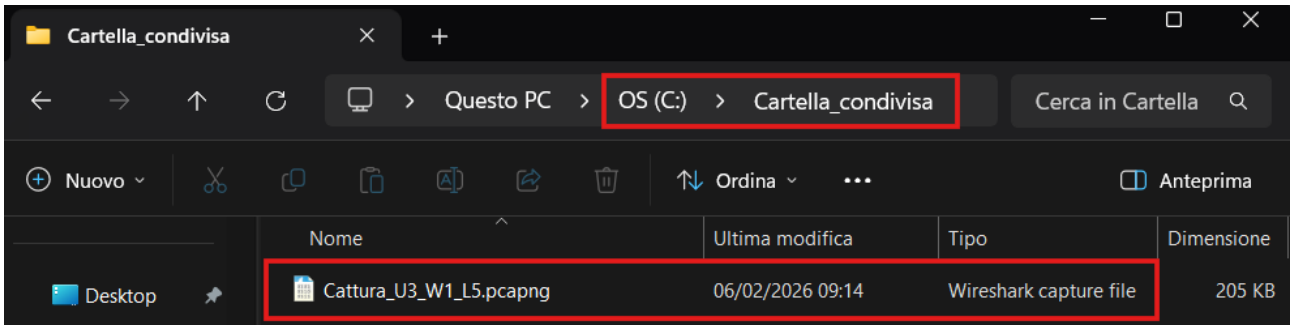
Ho creato sul sistema host la cartella:

**`C:\Cartella_condivisa`**

All’interno ho inserito il file:

**`Cattura_U3_W1_L5.pcapng`**




**In VirtualBox ho configurato la cartella condivisa con**:

- Montaggio automatico attivo
- Accesso completo
- Configurazione permanente

---

# Trasferimento su Kali Linux

Una volta avviata Kali, ho verificato la presenza della cartella in:

**`ls /media`**

Ho individuato la directory:

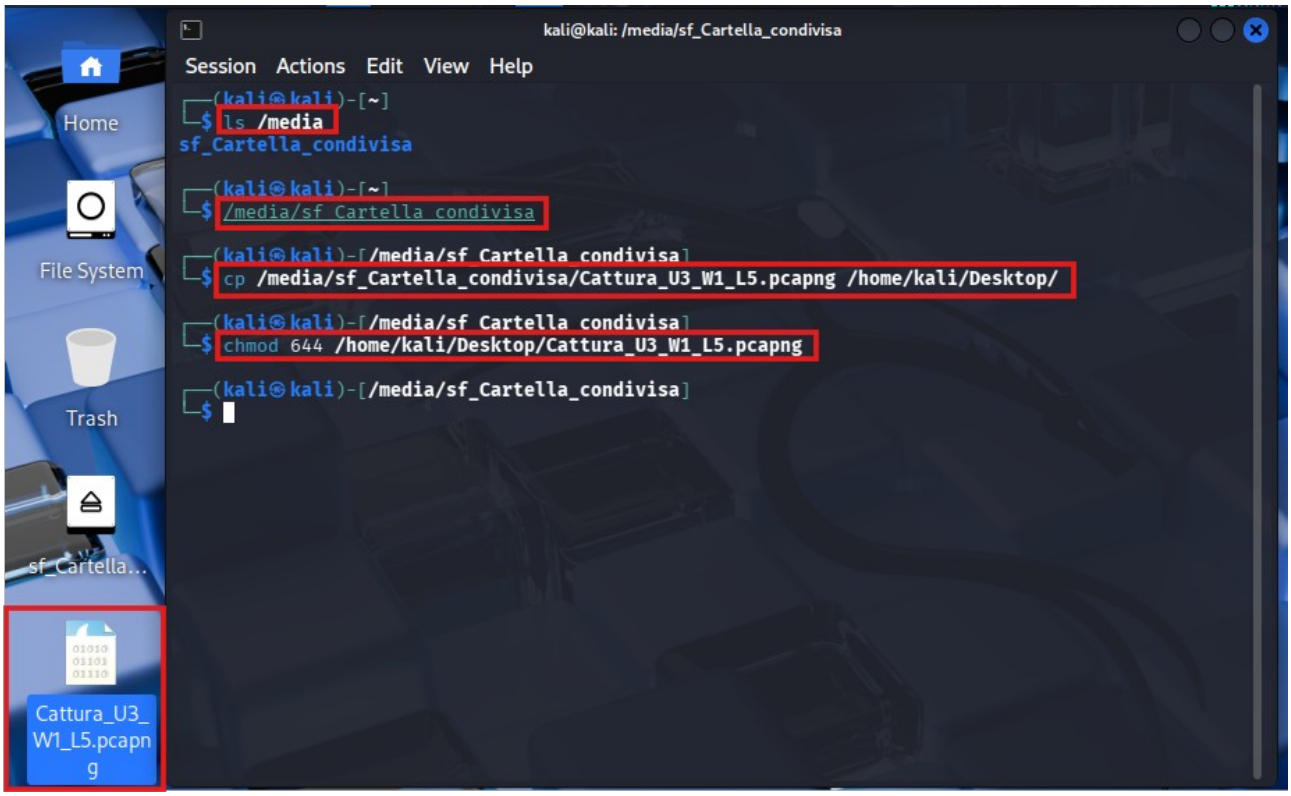
**`/media/sf_Cartella_condivisa`**

Ho copiato il file sul Desktop:

**`cp /media/sf_Cartella_condivisa/Cattura_U3_W1_L5.pcapng /home/kali/Desktop/`**

Ho impostato i permessi:

**`chmod 644 /home/kali/Desktop/Cattura_U3_W1_L5.pcapng`**




**Successivamente ho aperto il file con Wireshark.**

Quindi ho verificato la corretta presenza della cartella condivisa in `/media`, ho copiato il file sul Desktop di Kali e ho impostato i permessi di lettura per consentire l'apertura con Wireshark.

---

# 2) Analisi della Cattura

## Raccolta informazioni preliminare

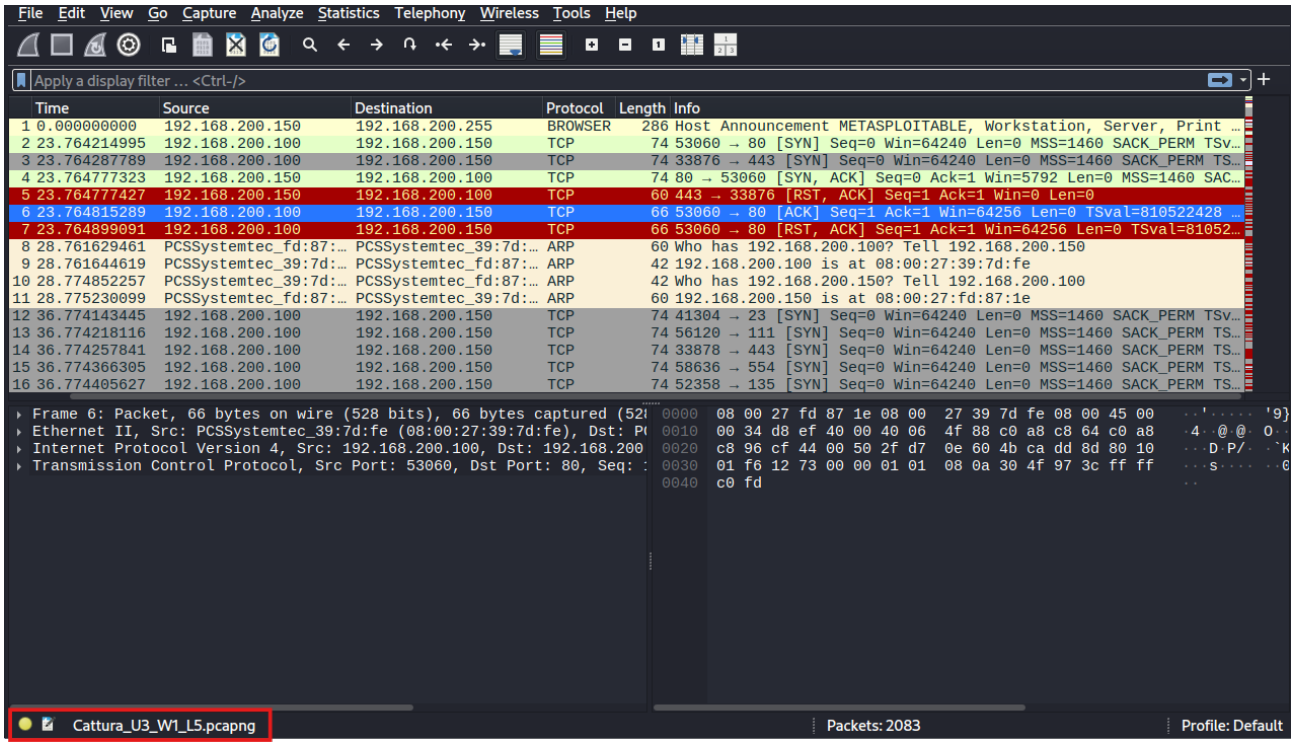
Ho consultato:

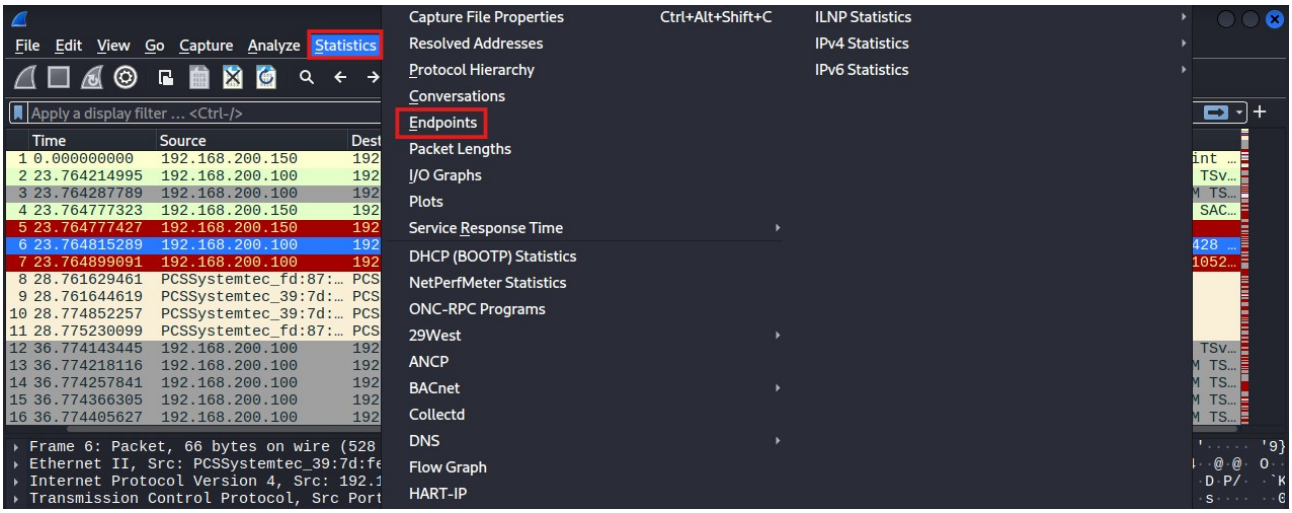
**`Statistics → Endpoints → IPv4`**

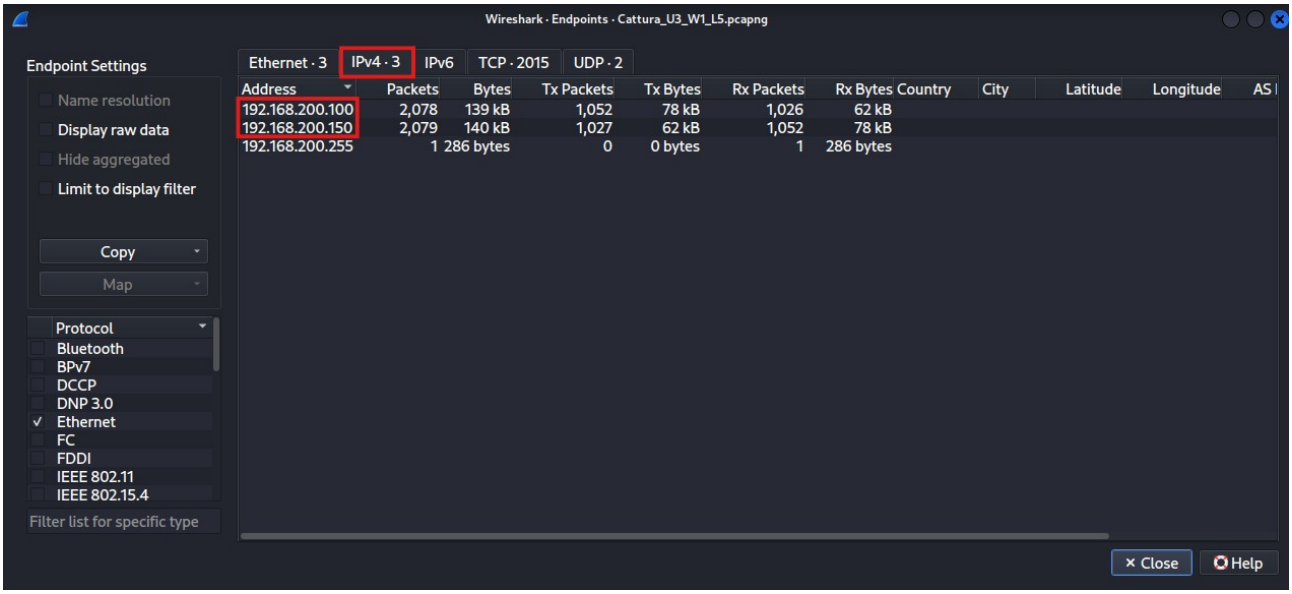
Sono emersi due host principali:

- **192.168.200.100**
- **192.168.200.150**

---

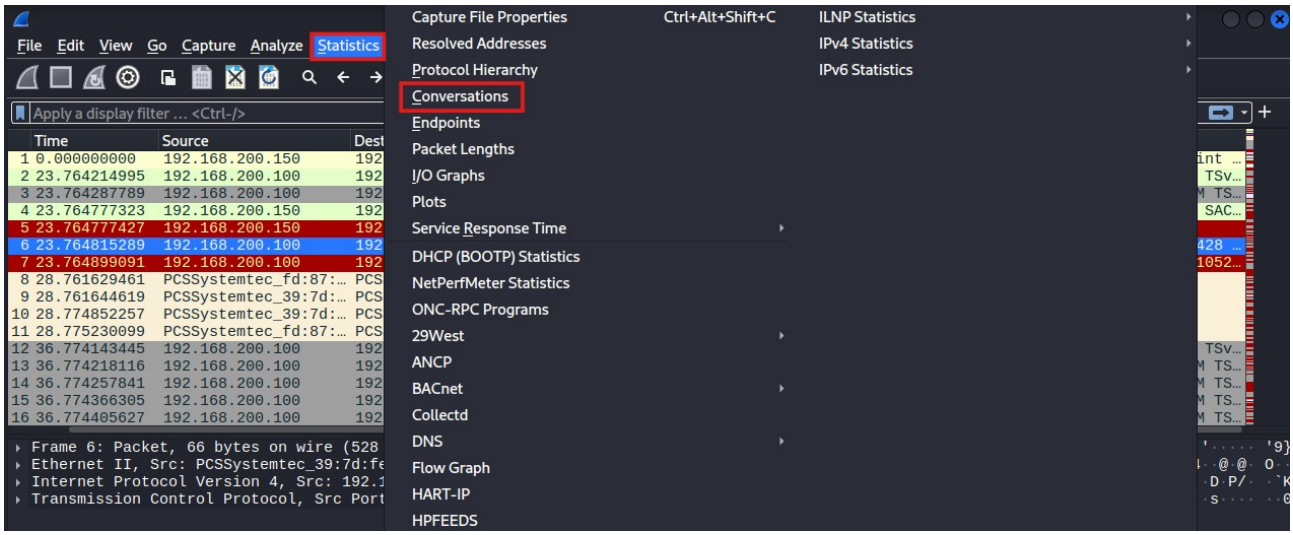

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Time Source Destination Protocol Length Info
1 0.000000000 192.168.200.150 192.168.200.255 BROWSER 286 Host Announcement METASPLOITABLE, Workstation, Server, Print ...
2 23.764214995 192.168.200.100 192.168.200.150 TCP 74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv...
3 23.764287789 192.168.200.100 192.168.200.150 TCP 74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS...
4 23.764777323 192.168.200.150 192.168.200.100 TCP 74 80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC...
5 23.764777427 192.168.200.150 192.168.200.100 TCP 60 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6 23.764815289 192.168.200.100 192.168.200.150 TCP 66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 ...
7 23.764899091 192.168.200.100 192.168.200.150 TCP 66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81052...
8 28.761629461 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP 60 Who has 192.168.200.100? Tell 192.168.200.150
9 28.761644619 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP 42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP 42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP 60 192.168.200.150 is at 08:00:27:fd:87:1e
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 TSv...
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 TS...
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 TS...
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 TS...
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 TS...
Frame 6: Packet, 66 bytes on wire (528 bits), 66 bytes captured (52
Ethernet II, Src: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe), Dst: P
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200
Transmission Control Protocol, Src Port: 53060, Dst Port: 80, Seq:
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 34 d8 ef 40 00 40 06 4f 88 c0 a8 c8 64 c0 a8
0020 c8 96 cf 44 00 50 2f d7 0e 60 4b ca dd 8d 80 10
0030 01 f6 12 73 00 00 01 01 08 0a 30 4f 97 3c ff ff
0040 c0 fd
Cattura_U3_W1_L5.pcapng
Packets: 2083
Profile: Default

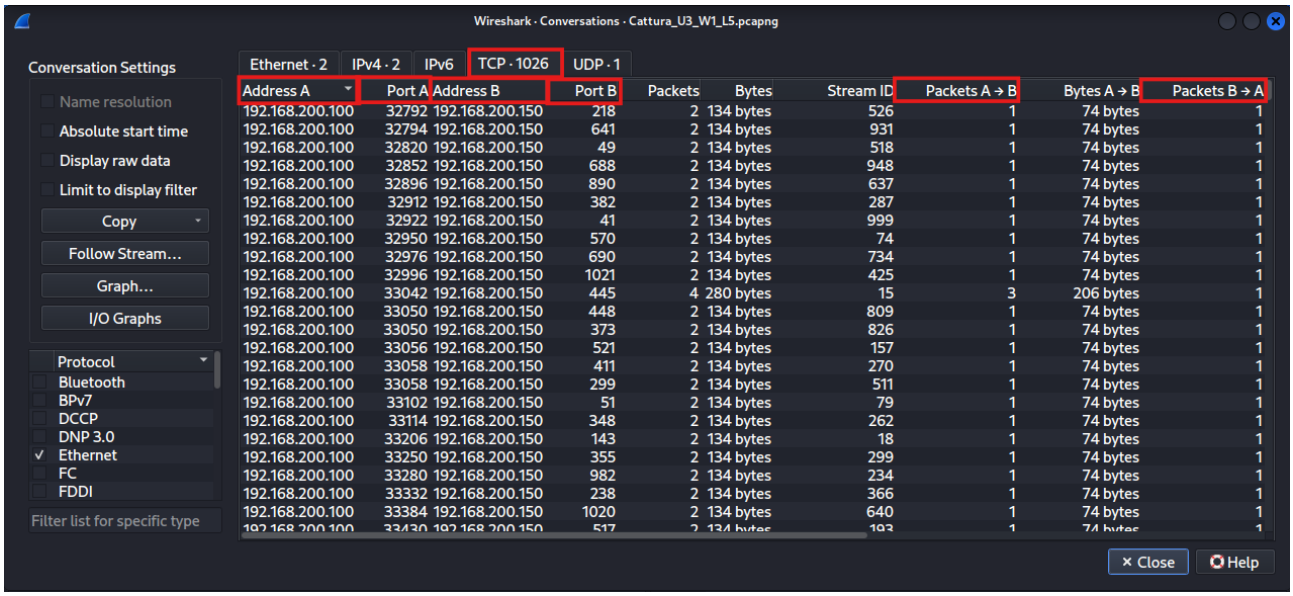

File Edit View Go Capture Analyze Statistics
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Plots
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
ILNP Statistics
IPv4 Statistics
IPv6 Statistics


Wireshark · Endpoints · Cattura_U3_W1_L5.pcapng
Endpoint Settings
Name resolution
Display raw data
Hide aggregated
Limit to display filter
Copy
Map
Protocol
Bluetooth
BPv7
DCCP
DNP 3.0
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
Filter list for specific type
Ethernet · 3
IPv4 · 3
IPv6
TCP · 2015
UDP · 2
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City Latitude Longitude AS
192.168.200.100 2,078 139 kB 1,052 78 kB 1,026 62 kB
192.168.200.150 2,079 140 kB 1,027 62 kB 1,052 78 kB
192.168.200.255 1 286 bytes 0 0 bytes 1 286 bytes
Close
Help

Dall’analisi degli Endpoint IPv4 emergono tre indirizzi. **L’indirizzo 192.168.200.255 rappresenta un broadcast di rete e non è rilevante ai fini dell’analisi**. **Gli host coinvolti nell’attività sospetta sono 192.168.200.100 e 192.168.200.150.**

Ho consultato:
**`Statistics → Conversations → TCP`**




Dall’analisi delle conversazioni TCP **emerge un elevato numero di tentativi di connessione tra 192.168.200.100 e 192.168.200.150.**
Ogni conversazione è composta da **un solo pacchetto in direzione A → B (SYN) e uno in direzione B → A (RST/ACK), per un totale di due pacchetti, senza completamento dell’handshake** TCP.
In assenza della sequenza completa **SYN – SYN/ACK – ACK,** non viene stabilita alcuna sessione TCP effettiva.
**Qui invece ogni stream ha solo 2 pacchetti.** La presenza di **numerose porte di destinazione differenti conferma un comportamento coerente con un’attività di port scanning.**

---

# Analisi tecnica del traffico

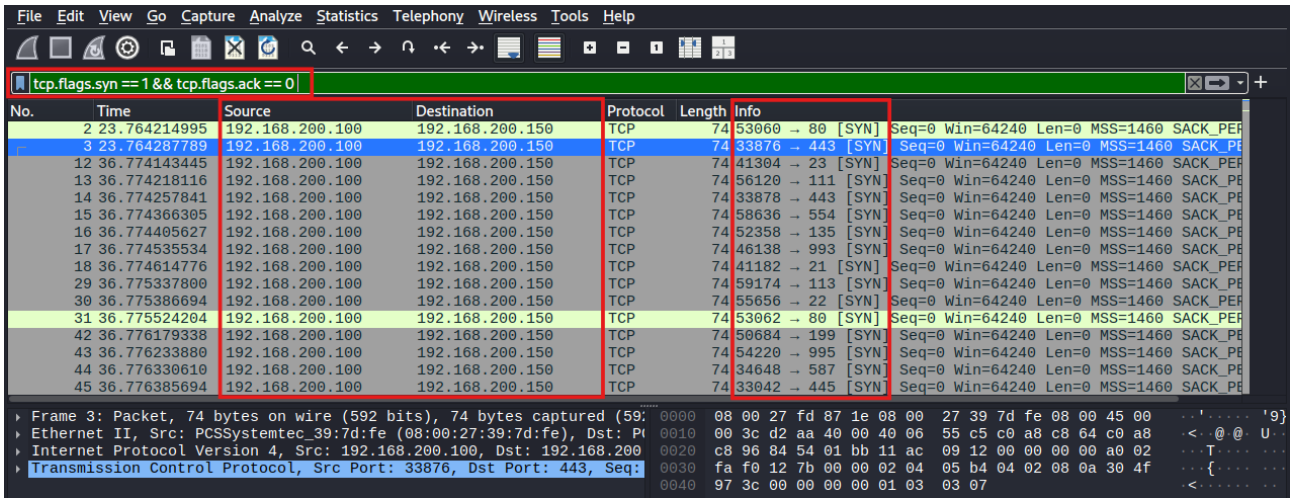
Ho applicato il filtro:

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

Ho osservato numerosi tentativi di connessione (**pacchetti SYN**) provenienti da:

`192.168.200.100 → 192.168.200.150`

verso porte multiple.



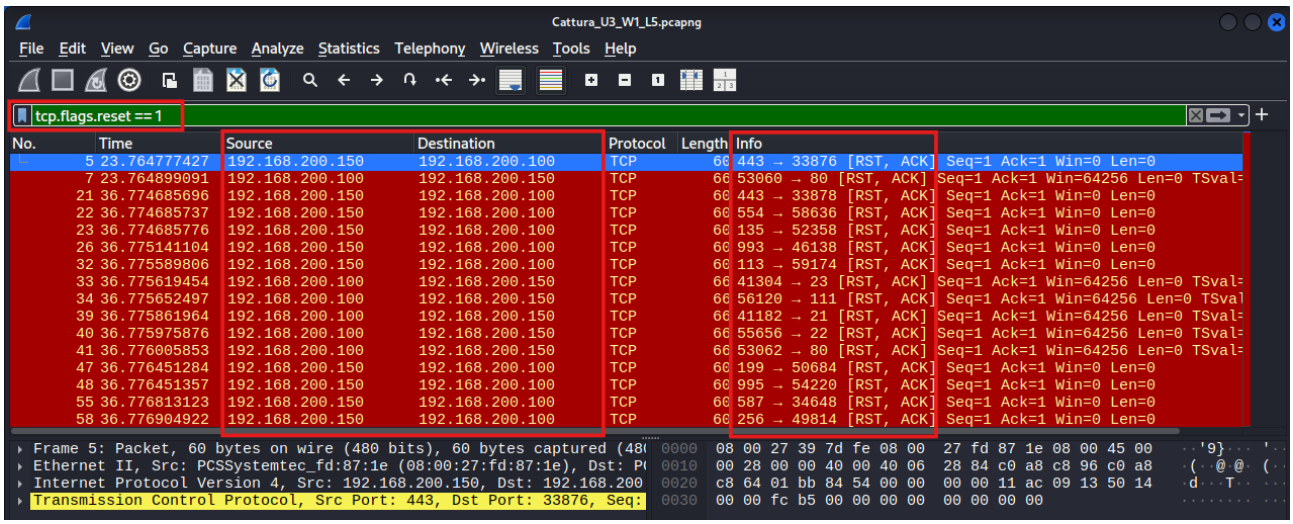

Come si evidenzia, **ho applicato il filtro `tcp.flags.syn == 1 && tcp.flags.ack == 0`** al fine di individuare i tentativi iniziali di apertura delle connessioni TCP.
L'analisi **mostra numerosi pacchetti SYN provenienti dall'host 192.168.200.100 verso l'host 192.168.200.150 su porte di destinazione differenti.**
L'assenza del completamento dell'handshake TCP e la varietà delle porte coinvolte indicano **un comportamento coerente con un'attività di port scanning.**

Successivamente ho utilizzato il filtro:

`tcp.flags.reset == 1`

Il sistema target ha risposto con pacchetti **RST/ACK**, indicando porte chiuse.

---




Dopo aver applicato il **filtro `tcp.flags.reset == 1` per individuare le risposte di reset**.
L'host **192.168.200.150 risponde ai tentativi di connessione con pacchetti RST/ACK verso 192.168.200.100.**
La presenza del flag **RST indica il rifiuto della connessione TCP, confermando che le porte contattate risultano chiuse.**
Questo comportamento **è coerente con una fase di port scanning in cui il sistema target non espone i servizi sondati.**

---

# 3) Indicatori di Compromissione (IoC)

Dall'analisi ho identificato:

- IP sorgente sospetto: **192.168.200.100**
- IP target: **192.168.200.150**
- Elevato numero di tentativi **SYN** verso porte differenti
- Risposte **RST/ACK** dal target
- Pattern coerente con **attività di port scanning**

Porte coinvolte:

**22, 80, 443, 445, 25, 110, 53, 587, 995.**

**Gli IoC rilevati sono di natura tecnica (network-based).**

---

# 4) Ipotesi sul Vettore di Attacco

Il comportamento osservato è compatibile con una fase di **ricognizione attiva**.

L'host **192.168.200.100** sembra eseguire uno scanning per identificare:

- Servizi SSH esposti
- Servizi SMB vulnerabili
- Applicazioni web
- Servizi di posta

Questa fase precede tipicamente:

- **Tentativi di brute force**
- **Exploit di vulnerabilità note**
- **Attacchi ai servizi esposti**

---

# 5) Azioni Raccomandate

## Contenimento immediato

- **Bloccare o limitare l'IP 192.168.200.100 tramite firewall**
- Applicare rate limiting sui tentativi di connessione

## Prevenzione futura

- **Chiudere porte non necessarie**
- **Implementare IDS/IPS** con regole anti-scan
- **Attivare monitoraggio SIEM** su pattern anomali
- **Segmentare la rete** per ridurre superficie di attacco

---

# Conclusione

L'analisi della cattura ha evidenziato un'**attività di port scanning sistematico verso l'host 192.168.200.150. Gli Indicatori di Compromissione individuati (IoC) suggeriscono una fase preliminare di attacco**, potenzialmente **finalizzata all'identificazione di servizi vulnerabili**. **Qualora fossero stati individuati servizi attivi, l'attaccante avrebbe potuto procedere con tecniche di exploitation o brute force**, determinando un'escalation dell'attacco. **L'adozione delle misure suggerite riduce significativamente la probabilità di compromissione futura**.