ESERCIZIO: Per lʼesercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

● Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso

● In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

● Consigliate unʼazione per ridurre gli impatti dellʼattacco attuale ed eventualmente un simile attacco futuro

***GLI IOC***

*Gli Indicatori di Compromissione IoC) sono segnali specifici che suggeriscono che un sistema o una rete è stata compromessa da un attacco informatico.*

*Tipi di IoC:*

*● Indirizzi IP Malevoli: IP noti per essere utilizzati in attività dannose.*

*● Hash di File: Impronte digitali uniche di file malevoli.*

*● URL e Domini Malevoli: Siti web utilizzati per phishing o distribuzione di malware.*

*● Processi Anomali: Programmi o attività in esecuzione non autorizzati o sospetti.*

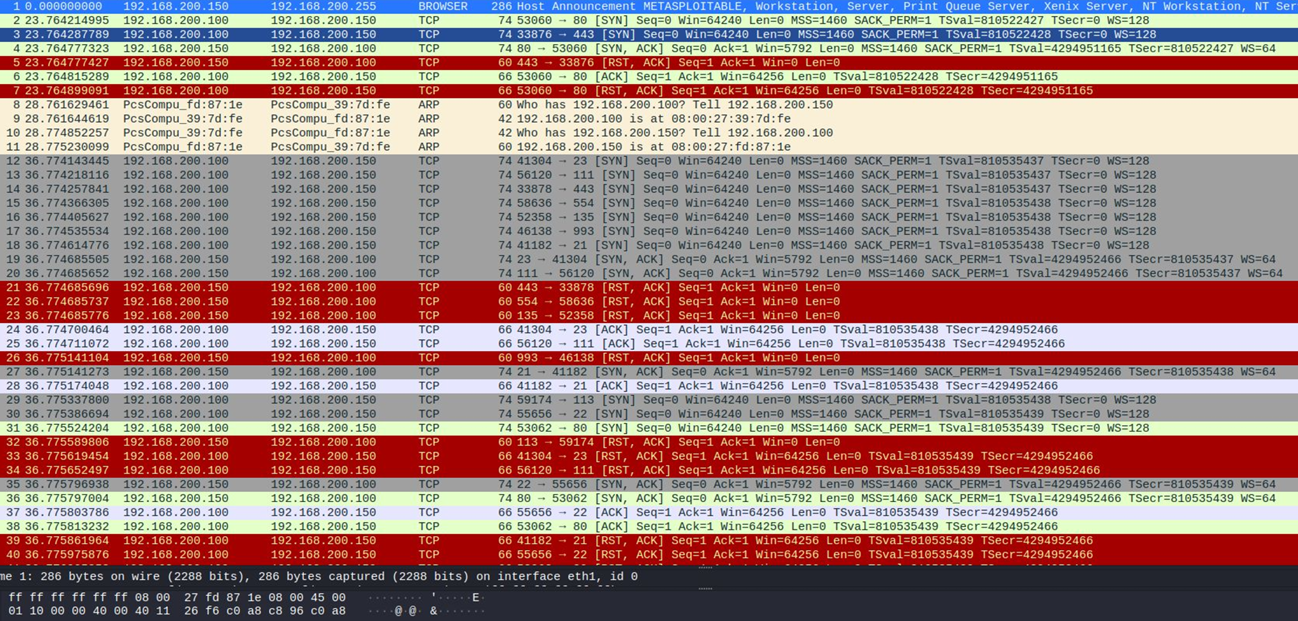
*● Modifiche ai File: Alterazioni non autorizzate a file di sistema o applicazioni.*

*Uso degli IoC:*

*● Rilevamento: Identificare e monitorare attività sospette.*

*● Risposta agli Incidenti: Informare le azioni correttive durante un'indagine su un incidente.*

*● Prevenzione: Bloccare attacchi futuri utilizzando liste di controllo aggiornate.*



**IOC identificati**

**Indirizzi IP**

L’indirizzo IP 192.168.200.150 appare come bersaglio in molte sessioni *TCP* che terminano con pacchetti *RST.*

**Motivo**: Le connessioni interrotte frequentemente tramite **RST** possono indicare: scansioni di porta e tentativi di attacco falliti.

L’indirizzo 192.168.200.100 agisce come mittente, ma in alcuni casi riceve risposte che sembrano essere tentativi di handshake TCP.

**Motivo**: Potrebbe essere un dispositivo compromesso o usato per eseguire attività non autorizzate, come scansioni SYN.

**PORTE**

**Porta 80 (HTTP):** Molti pacchetti iniziano un tentativo di comunicazione verso questa porta, ma le connessioni vengono chiuse con RST.

**Motivo:** Questa porta è spesso utilizzata per scansioni o tentativi di exploit.

**Porta 443 (HTTPS):** Il tentativo di connessione a questa porta si conclude con RST.

**Motivo:** Tentativo di vulnerabilità

**Porte non standard (59174, 55346):** Sono in sessioni TCP ma interrompono la sessione in modo non corretto

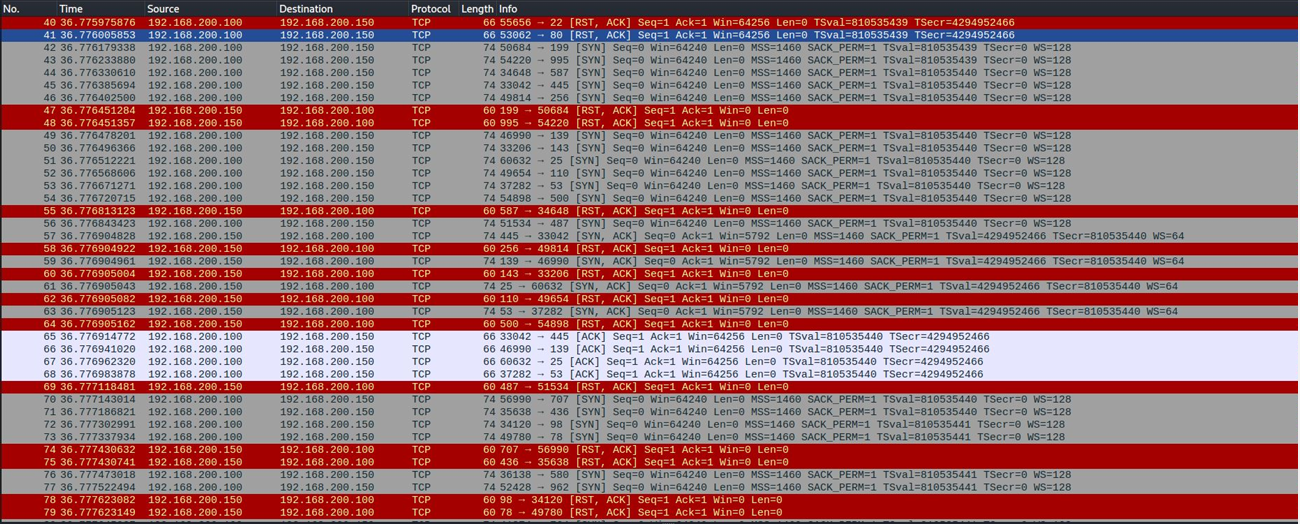
**Motivo:** L’uso di porte alte indica attività scorrette e protocolli utilizzati per attacchi.

**ARP anomali:** Ripetuti pacchetti ARP con lo stesso destinatario e mittente (**PcsCompu\_fd:87:1e**).

**Motivo:** Potenziale attacco di spoofing ARP per intercettare il traffico della rete locale.

**Connessioni SYN senza risposta (SYN Flooding):** Alcuni tentativi di handshake non ricevono mai un ACK.

**Motivo:** Tipico comportamento da scansioni SYN o attacchi SYN per esaurire le risorse della vittima.

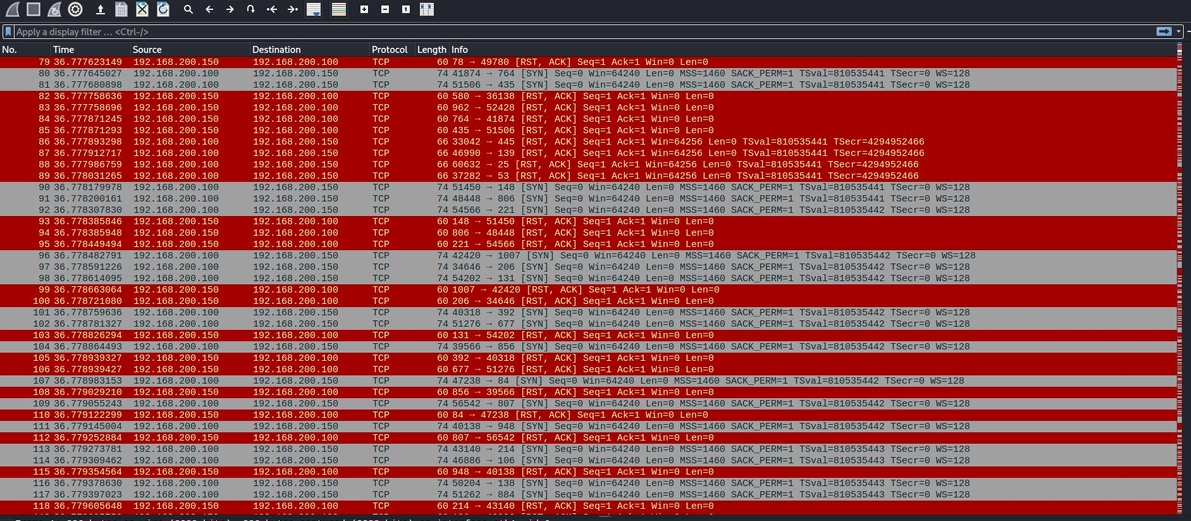


**IOC Identificati**

Numerosi pacchetti con flag (RST, ACK), indicano una chiusura forzata delle connessioni TCP. **Motivo:** può indicare scansioni di porta, tentativi di exploit falliti e dispositivi compromessi.

I pacchetti RST indicano traffico non autorizzato o respinto.

Per quanto riguarda IP, Porte e comportamenti anomali, i motivi sono gli stessi indicati precedentemente.



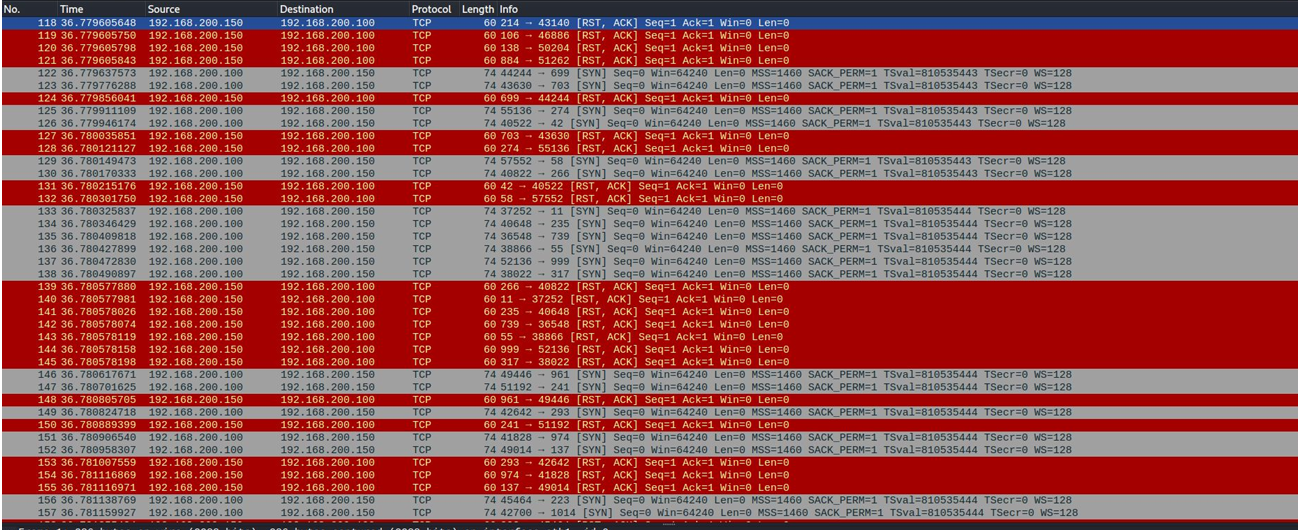
**IOC Identificati**

*(Siccome IP e alcune Porte sono le stesse, le loro caratteristiche e possibili anomalie sono state già descritte)*

Il traffico, essendo dominato da RST e ACK, si presenta come anomalia perché chiudono le connessione TCP e potrebbe essere associato ad *attacchi SYN* e alla *scansione di porte.*

Porte non standard troppo alte come 49780, 51418, 52848 l’uso di porte alte non standard è comune per attività malevoli, come: attività anomale e protocolli sfruttati per attacchi.

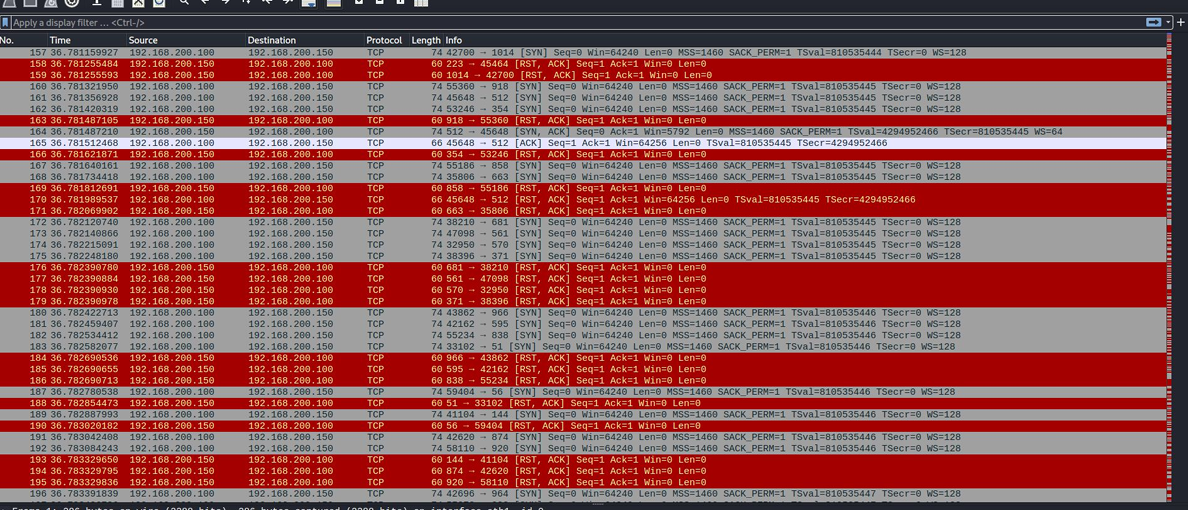
Inoltre l’assenza di porte comuni come *80, 443 (HTTP/HTTPS)*, rende il traffico ancora più sospetto.



**IOC Identificati**

Le porte sospette sono sempre alte e non comuni, come: 43140, 46868, 40282.

Motivo: Le porte alte non sono controllate e possono essere usate per traffico malevolo o per sfruttare le vulnerabilità. Ip e comportamenti anomali, già descitti.



Le porte sono sempre alte non comuni, come: 45464, 42120, 59344.

Porte alte non comuni sono considerati IOC in quanto sono associate ad attività malevole

e a tentativi di bypassare regole del firewall. La mancanza di porte comuni insospettisce di più.

**Riassunto generale**

### **IOC Sicuri Identificati**

1. **Indirizzi IP:**
   1. **192.168.200.150** (sorgente).
   2. **192.168.200.100** (destinazione).
2. **Porte coinvolte:**
   1. **41104**, **42620**, **58116**, e altre porte elevate.
3. **Comportamenti sospetti:**
   1. Flag **RST, ACK** ripetuti.
   2. Tentativi SYN senza completamento delle connessioni.
4. **Traffico mirato:**
   1. Interazioni esclusivamente tra i due IP, con un volume anomalo.

**Azioni consigliate**

1. Bloccare le porte elevate
2. Continua analisi di pacchetti
3. Isolare il dispositivo 192.168.200.150
4. Controllare il target 192.168.200.100 (compromesso o vittima di attacco)