LKSP Jawa Tengah 2026
Cyber Security
Module C (Blue Team CTF)

Nama Peserta :

1. Khoirun Fadillah Nu’ma
2. Arjuna Nazril Ramadhan

Daftar Isi

Forensic

1. Indicator:

Description:

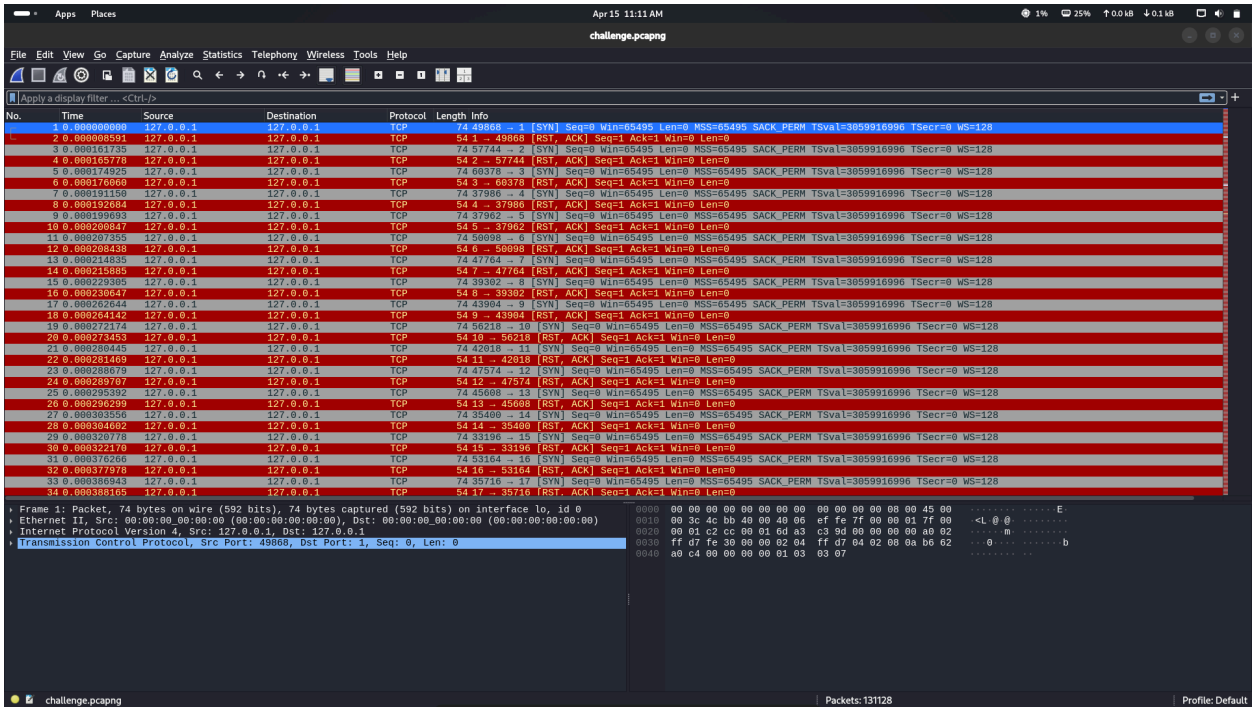
There's a port scan going in my own localhost, strangely it spotted one additional port which seems **FALSE POSITIVE**. Can you help me to find which port that is flagged by those scanners but actually **CLOSED** due to lack of/valid ACK reply ?

Wrap your answer in `LKS{portnumber}`

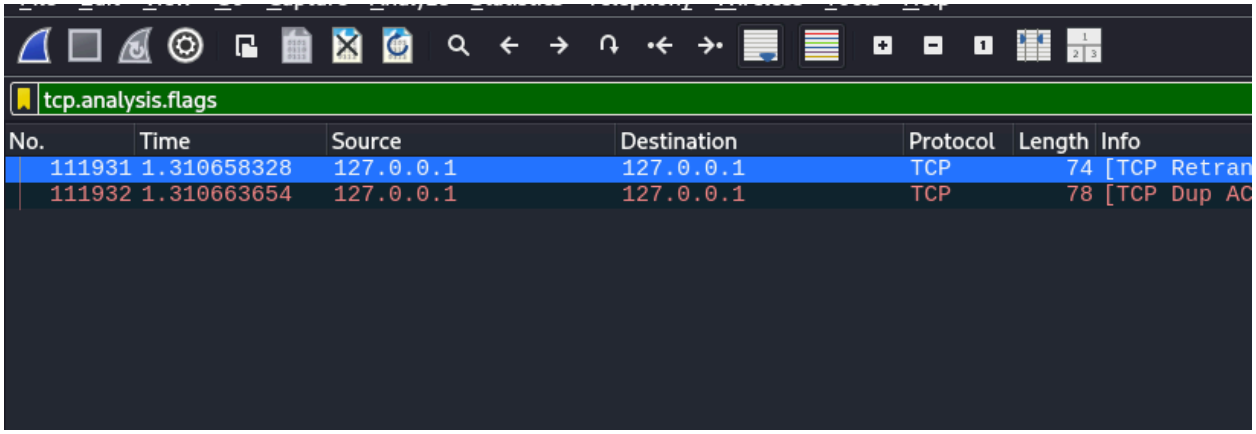
author: aseng

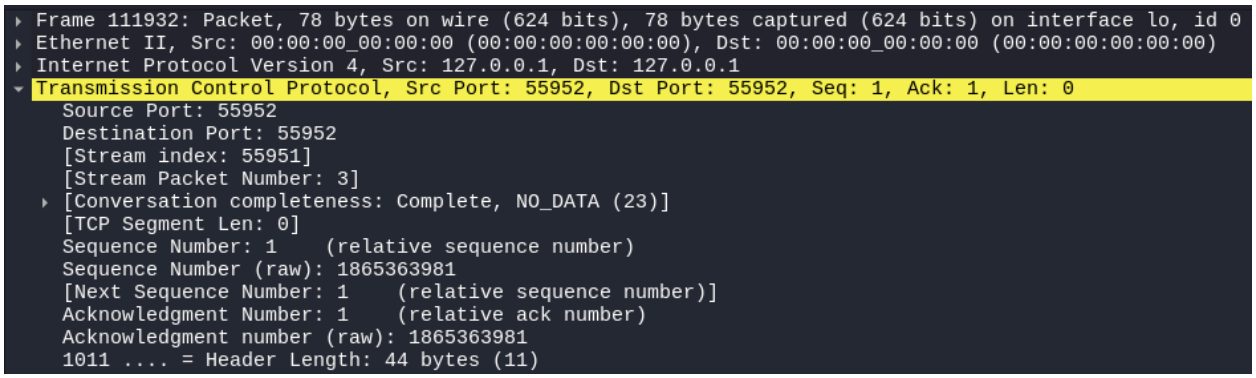
Walkthrough:

Pada challenge ini kami diberikan sebuah file challenge.pcapng yang berisi history lalu lintas jaringan pada localhost



Challenge ini meminta player untuk mencari port yang diclose oleh sistem karena kurangnya reply ACK yang valid, untuk mencarinya kami hanya perlu untuk menambahkan display filter `tcp.analysis.flags`





Flag: LKS{55952}

SIEM SOC

1. Hihi:

Description:

This challenge is SIEM SOC series for LKS. The `artifact.zip` password is `ODhDBe825sjfRBCysCN13blIHtj6lAi/9d3r2gAdfDo=`.

You **SHOULD** solve this challenge with your SIEM (Wazuh/Splunk/ELK/any other SIEM product).

There's a targeted AD attack in July 2025. I need you to gather some basic questions for your finale.

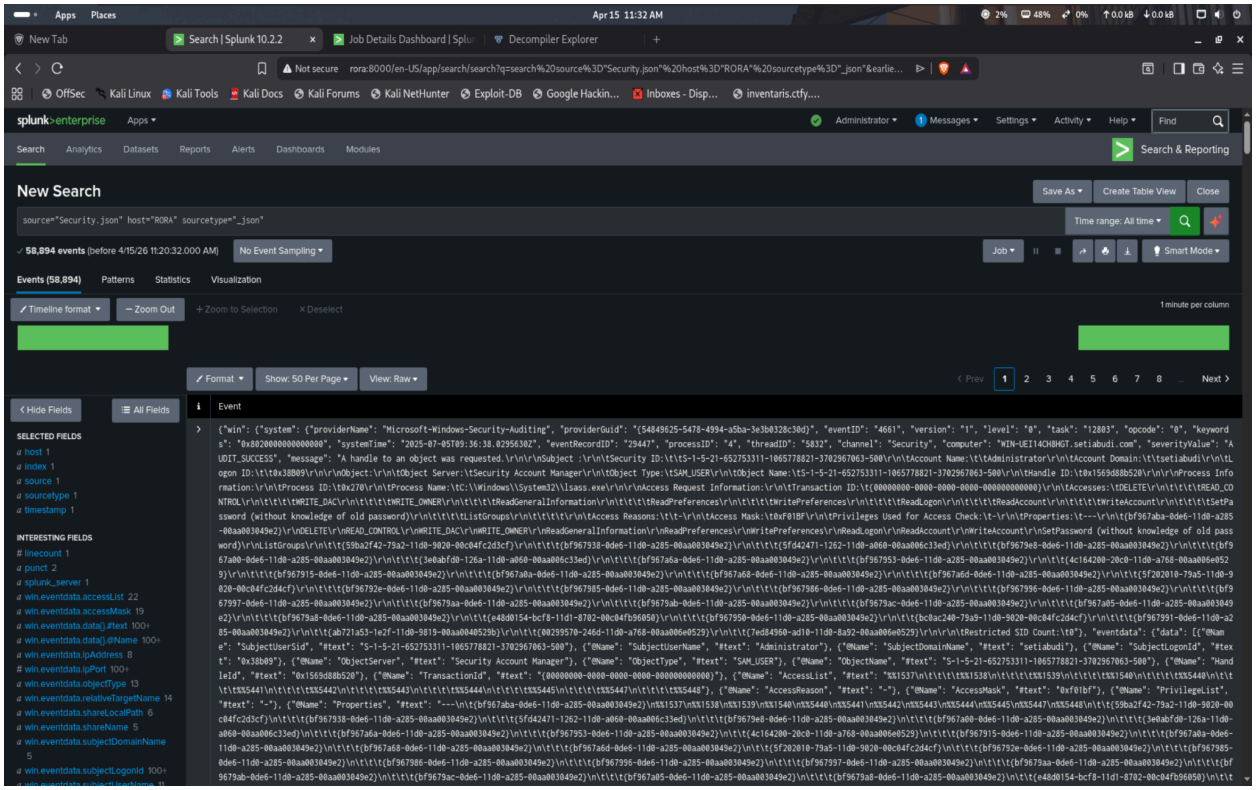
What's the hostname of the machine?

Example: If you found the hostname is HARBAHKXOOEL then the answer is `LKS{HARBAHKXOOEL}`.

author: aseng

Walkthrough:

Di Chall ini di berikan sebuah file zip artifact.zip yang dimana setelah di extract dengan password yang sudah diberikan akan ada dua file .evtx dan .json, karna sy pakek splunk jadi import file .json lebih enak, ketika uda disearch



Setelah sy baca semua log yang ada ada satu patokan yaitu setiabudi, tapi setelah dibaca lebih teliti di bagian lognya ada parameter “computer” di situ lengkap seperti ada pada di desc.

Di system time ada tahun dan bulannya yaitu Juli, 2025 dan jelas computer adalah hostname dari machine itu.

Flag: LKS{WIN-UEI14CH8HGT}