

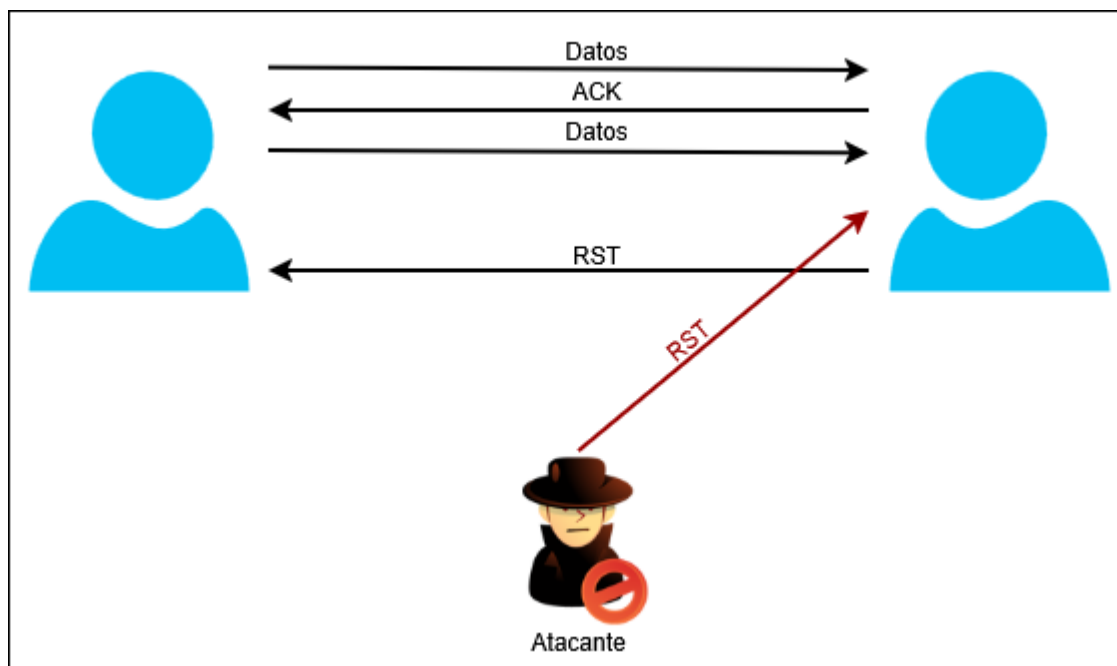
# Securizando la infraestructura de internet

## Problemas de seguridad comunes en TCP

### Disponibilidad

#### Ataque TCP reset

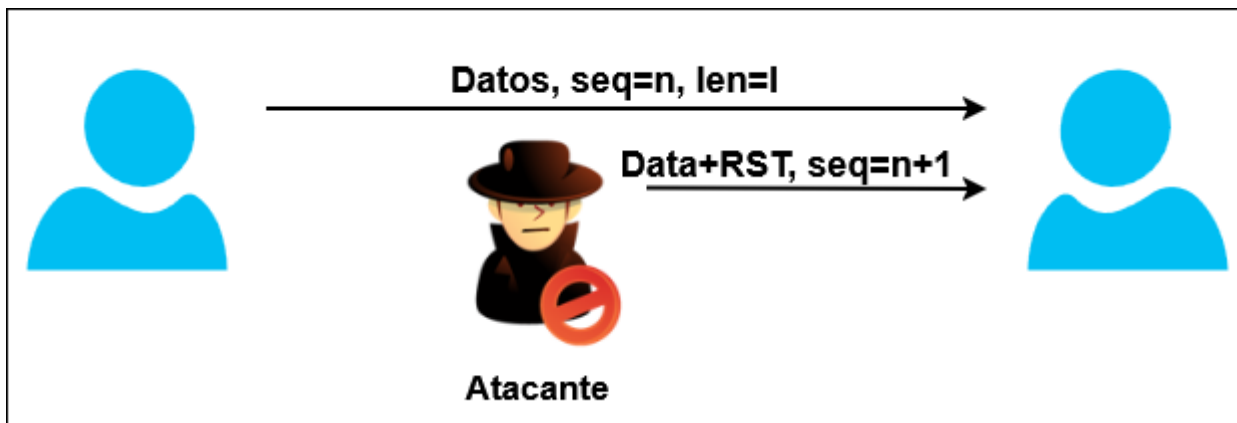
El Flag ReSeT (RST) provoca la caída de la conexión, normalmente se usa para recuperación de errores. El atacante inyecta un marco con el flag RST activo, provocando que el receptor corte la conexión inmediatamente.



El ataque tiene los siguientes requisitos:

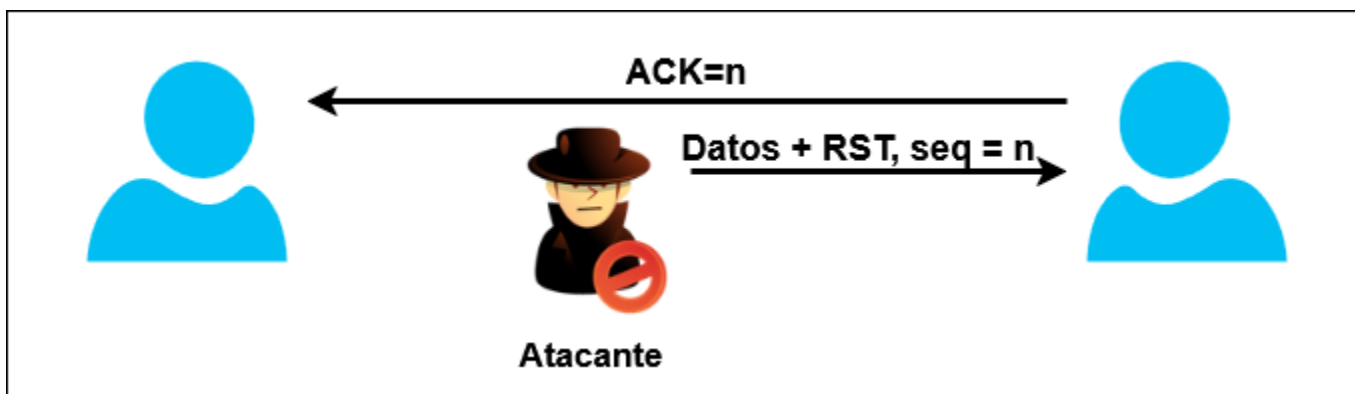
- RST se encuentra dentro del rango permitido
  - En todos los estados salvo SYN-SENT, todos los fragmentos RST son validados revisando sus campos SEQ (Número de secuencia).
  - Un reset es válido si el número de secuencia está dentro del rango
  - En el estado SYN-SENT el RST es aceptable si el campo ACK reconoce el SYN
  - Número de secuencia entre RCV.NXT y RCV.NXT+RCV.WND
  - Rangos históricos < 64 kbytes.
- Right 4-tuple
  - Se deben conocer la IP y puerto del server
  - Se deben conocer la IP y el puerto del cliente

## Ataque TCP reset - Sin limitación de posición: Atacante en la red del cliente



- El atacante inspecciona los datos enviados por el primer equipo al segundo equipo
- Antes de que el primer equipo envíe el siguiente paquete, el atacante genera un paquete RST válido con:
  - Misma Dirección IP
  - Mismos Puertos TCP
  - Número de secuencia correcto.

## Ataque TCP reset - Sin limitación de posición: Atacante en la red del servidor



From:  
<https://knoppia.net/> - Knoppia

Permanent link:  
[https://knoppia.net/doku.php?id=master\\_cs:secom:tm4\\_v2&rev=1779959264](https://knoppia.net/doku.php?id=master_cs:secom:tm4_v2&rev=1779959264)

Last update: 2026/05/28 09:07

