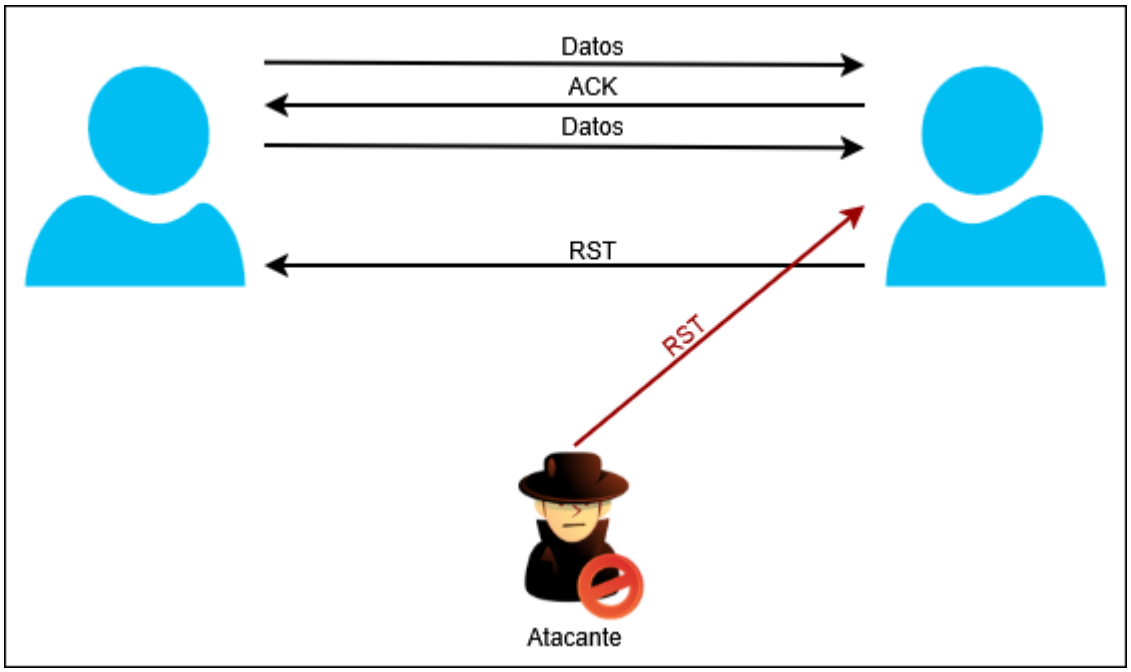
Securizando la infraestrucura de internet

Problemas de seguridad compunes en TCP

Disponibilidad

Ataque TCP reset

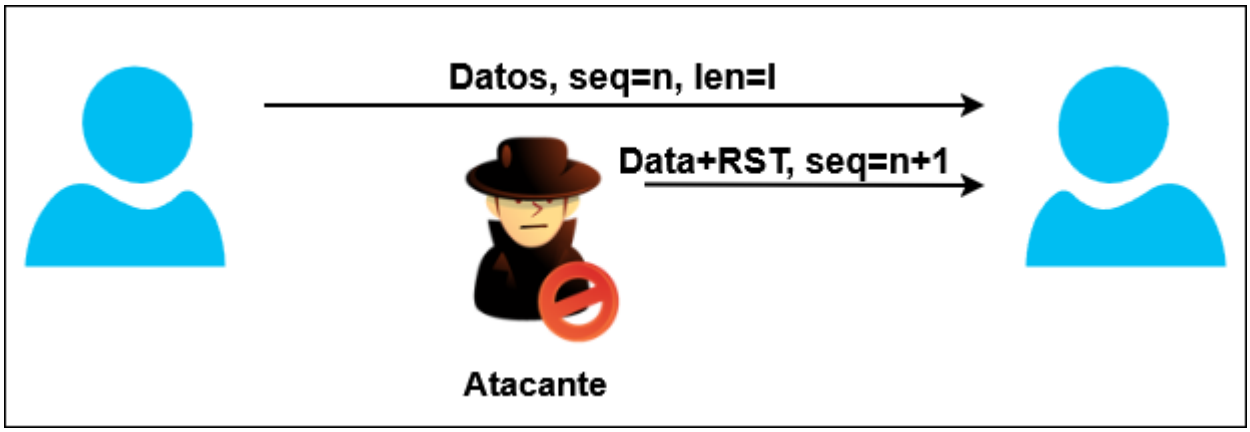
El Flag ReSeT (RST) provoca la caida de la conexión, normalmente se usa para recuperación de errores. El atacnte ijecta un marco con el flag RST activo, provocando que el receptor corte la conexión inmediatamente.



El ataque tiene los siguientes requisitos:

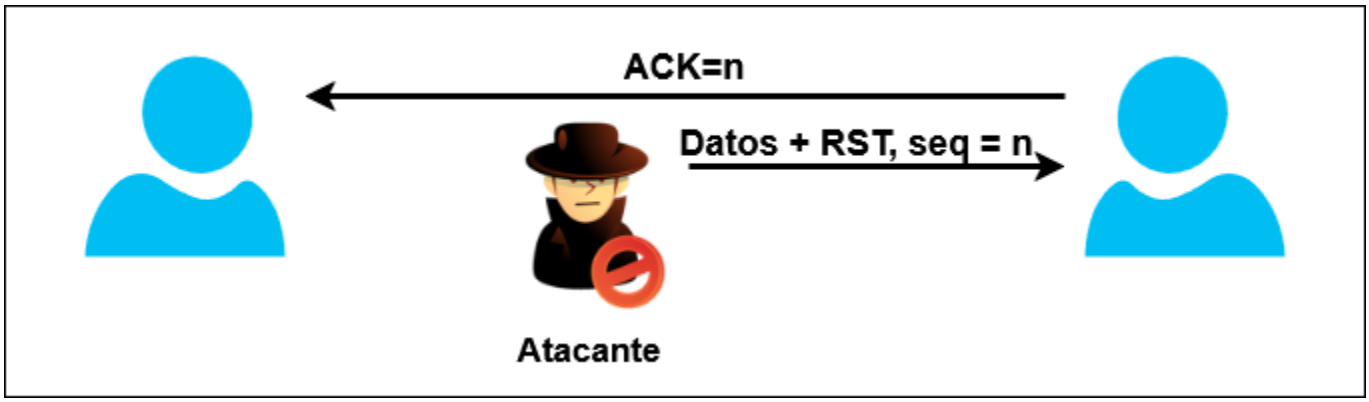
- RST se encuentra dentro del rango permitido
  - En todos los estados salvo SYN-SENT, todos los fragmentos RST son validados revisando sus campos SEQ (Número de secuencia).
  - Un reset es válido si el número de secuencia está dentro del rango
  - En el estado SYN-SENT el RST es aceptable si el campo ACK reconoce el SYN
  - Número de escuencia 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 conoce 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



- El atacante inspecciona el tráfico del segundo equipo al primero
- Antes de que el primer equipo envíe el siguiente paquete, se genera un paquete RST válido
  - Misma IP
  - Mismos puertos TCP
  - Número de secuencia correcto

Ataque TCP reset - Posición limitada: Blind Data/RST Injection

Es un ataque difícil de realizar, las direcciones de ambos extremos no suelen ser conocidas, aunque se suelen conocer las direcciones de los servidores, las de los servidores suelen ser desconocidas. Los puerto de los dos extremos suelen ser desconocidos, el de server a veces es conocido, pero el de los clientes suele ser impredecible. El número de secuencia tampoco es conocido. Las conexiones suelen tener un tiempo de vida muy corto y el rango del número de secuencia valido cambia, por lo que cualquier intento de adivinar estos datos es poco útil.

Por otro lado, los protocolos tienen un amplio tiempo de vida y las direcciones se pueden saber por adelantado.

Defensas contra ataque TCP reset

- Solo aceptar el segmento RST si el número de secuencia es el primero en el rango (proveido por el sistema operativo)
- Filtrar paquetes spoofeados a nivel IP (Tiene que ser realizado por los servidores de autenticación en los extremos)
- Usar tmarcas de tiempo como defensa adicional: PAWS (Protection Against Wrapped Sequences)
- Paquetes TCP autenticados (TCP-AO)

Ataque SYN Flooding