07

# Para saber mais: Identificar roubos de refresh tokens

Nesse curso, não será detalhado um sistema que faz a identificação do roubo de *refresh tokens*. Mesmo assim, esse sistema, como já apresentado pelo SuperTokens (https://supertokens.io/blog/the-best-way-to-securely-manage-user-sessions), funcionaria da seguinte forma.

Para detectar o roubo, é necessário que tanto o atacante quanto a vítima usam o token após o ataque. Por exemplo:

- Digamos que o *refresh token* `refresh_token_0` da vítima foi roubado.
- Em algum momento, o *access token* ( `access_token_0` ) da vítima expirará e, por isso, ambos terão que atualizar seus tokens.
- Dessa forma, se o atacante usar `refresh_token_0` antes, ele receberá novos tokens `refresh_token_1` e `access_token_1` , invalidando o antigo.
- Em seguida, quando a vítima tentar atualizar seus tokens, ela usará o `refresh_token_0` invalidado. Isso dispara uma possível indicação de roubo, pois é esperado que a pessoa tivesse utilizado o `refresh_token_1` .
    - Numa outra situação, se a vítima usar `refresh_token_0` antes, o argumento é análogo ao anterior.

Assim, se um roubo de *refresh tokens* for detectado, é possível disparar uma rotina que remove esse token da *allowlist*, cessando o ataque.