ACCESS TOKEN

1. Khái niệm:

+ Là đối tượng mô tả ngữ cảnh bảo mật của một quy trình hoặc luồng

+ Thông tin trong access token gồm danh tính (identity) và đặc quyền (privilege) của tài khoản người dùng được liên kết với tiến trình hoặc luồng

+ Quy trình: Khi người dùng đăng nhập vào hệ thống => hệ thống xác minh mật khẩu của người dùng = so sánh với thông tin được lưu trữ trong cơ sở dữ liệu bảo mật => Nếu mk được xác thực => access token được tạo bởi hệ thống

2. Thông tin chứa trong access token:

+ Mã định danh bảo mật (SID) cho tài khoản người dùng (user’s account)

+ SIDs cho các nhóm mà người dùng thành viên

+ SID đăng nhập xác định phiên đăng nhập hiện tại

+ Danh sách các đặc quyền được nắm giữ bởi người dùng hoặc nhóm người dùng

+ SID của chủ sở hữu

+ SID cho nhóm chính

+ DACL mặc định mà hệ thống sử dụng khi người dùng sử dụng khi người dùng tạo đối tượng có thể bảo mật mà không chỉ định mô tả bảo mật

+ Nguồn gốc của mã thông báo truy cập

+ Mã thông báo là mã thông báo chính hay mã thông báo giả mạo

+ Danh sách tùy chọn hạn chế SID

+ Mức độ mạo danh hiện tại

+ Số liệu thống kê khác

\*\* Mã thông báo chính (primary token):

+ Mỗi tiến trình đều có một primary token mô tả ngữ cảnh bảo mật (security context) của tài khoản người dùng được liên kết với tiến trình

+ Mặc định, hệ thống sử dụng mã thông báo chính khi một luồng của tiến trình tương tác với một đối tượng có thể bảo mật. Một luồng đang mạo danh một khách hàng có cả mã thoogn báo chính và mã thông báo mạo danh

3. Các chức năng:

\* thao tác với mã thông báo truy cập

A screenshot of a web page

Description automatically generated

A screenshot of a computer

Description automatically generated

\*\* Mô tả các phần của Access Token:

A screenshot of a computer

Description automatically generated

A screenshot of a text box

Description automatically generated

\*\* Các kiểu liệt kê:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated