Security Identifiers (Mã định danh bảo mật)

**I. Khái niệm:**

+ Là mã được sử dụng để nhận dạng một nguyên tắc bảo mật (security principle) hoặc nhóm bảo mật (security group)

+ Nguyên tắc bảo mật có thể đại diện cho các thực thể được xác thực bởi OS như: user account, computer account hoặc 1 luồng hoặc 1 tiến trình chạy trong bối cảnh bảo mật của tài khoản người dùng/máy tính

+ Mỗi tài khoản/nhóm/tiến trình chạy trong bối cảnh bảo mật của tài khoản đều có 1 SID duy nhất (do nhà phát hành cung cấp). SID sẽ không được sử dụng lại để nhận dạng người dùng hoặc nhóm khác

+ Mỗi khi người dùng đăng nhập, hệ thống 1 mã thông báo truy cập (access token) cho người dùng đó. Mã thông báo truy cập gồm: user’s SID, quyền của người dùng (user right) và SID cho bất kỳ nhóm nào mà người dùng thuộc về

**II. Cách thức hoạt động**

**+** Hệ điều hành đề cập đến các tài khoản và quy trình chạy trong bối cảnh bảo mật của tài khoản bằng cách sử dụng SID của họ

**+** Với tài khoản tên miền, SID của nguyên tác bảo mật được tạo bằng cách ghép SID của miền với mã định danh tương đối (RID-relative identifier) cho tài khoản

**III. Cấu trúc**

**+** SID là cấu trúc dữ liệu ở định dạng nhị phân chứa một số giá trị thay đổi. Các giá trị đầu tiên trong cấu trúc chứa thông tin về cấu trúc SID. Các giá trị còn lại được sắp xếp theo thứ bậc (như SĐT) và giúp xác định cơ quan cấp SID, miền cấp SID và nhóm/nguyên tắc bảo mật cụ thể.

A close-up of a list

Description automatically generated

- Revision: Chỉ ra phiên bản cấu trúc SID được sử dụng trong một SID cụ thể

- Identifier Authority: Xác định cấp độ thẩm quyền cao nhất có thể cấp SID cho 1 loại nguyên tắc bảo mật cụ thể. VD: SID cho Everyone Group là 1 (World Authority), SID cho 1 tài khoản hoặc nhóm Window Server là 5 (NT Authority)

A blue and white table with black text

Description automatically generated

- Subauthorities: Chứa thông tin quan trọng nhất trong SID, được chứa trong một chuỗi gồm 1 hoặc nhiều giá trị quyền phụ. Một loạt các giá trị (không bao gồm giá trị cuối) giúp xác định chung tên miền trong danh nghiệp và được gọi là bộ nhận dạng tên miền. Giá trị cuối cùng trong chuỗi, được gọi là mã định danh tương đối (RID), xác định 1 tài khoản hoặc nhóm cụ thể có liên quan đến 1 miền

- Chuyển đổi SID từ nhị phân sang chuỗi bằng sử dụng ký hiệu chuẩn

S-RX-Y1-Y2-Yn-1-Yn

Trong đó:

S – chỉ ra chuỗi là SID

R- Chỉ ra mức độ sửa đổi

X- Chỉ ra giá trị thẩm quyền nhận dạng

Yn- Biểu thị một loạt các giá trị cấp dưới, trong đó n là số giá trị

- Thông tin quan trọng nhất trong SID nằm trong chuỗi giá trị subauthority. Phần đầu tiên của chuỗi (-Y1-Y2-Yn-1) là định danh miền. Định danh miền phân biệt các SID do 1 miền cấp với các SID do tất cả các miền khác trong doanh nghiệp cấp. Không có 2 miền nào trong 1 doanh nghiệp chi sẻ cùng 1 định danh miền

- Mục cuối trong subauthority (-Yn) là định danh tương đối. Nó phân biệt 1 tài khoản hoặc nhóm với tất cả các tài khoản và nhóm khác trong miền. Không có 2 tài khoản hoặc nhóm nào trong bất kỳ miền nào có cùng định danh tương đối

- VD: SID cho nhóm built-in Administrators

S-1-5-32-544

SID có:

+ Mức độ sửa đổi (1)

+ Giá trị thẩm quyền nhận dang (5, NT Authority)

+ Mã định danh miền (32, Builtin)

+ Mã định danh tương đối (544, Administrators)

\*\* SID cho các tài khoản và nhóm built in luôn có cùng giá trị nhận dạng miền là 32. Giá trị này xác định miền, Builtin tồn tại trên mọi máy tính đang chạy phiên bản của HĐH Window Server. Phạm vi của chúng là cục bộ, có thể là cục bộ của một số máy tính hoặc trong trường hợp bộ điều khiển cho 1 miền mạng, chúng là cục bộ của một số máy tính hoạt động như 1

\*\* Không có tài khoản/ nhóm nào khác trong miền Built-in có SID cuối cùng là 544 (chỉ dành cho nhóm Built-in Administrator)

-VD: SID cho global group, Domain Admin:

S-1-5-21-1004336348-1177238915-682003330-512

+ Mức độ sửa đổi (1)

+ Cơ quan nhận dạng (5, NT Authority)

+ Mã định danh miền: 21-1004336348-1177238915-682003330

+ RID: 512 (Domian Admins)

\*\* Windows phân bổ RID bắt đầu từ 1000; các RID có giá trị nhỏ hơn 1000 được coi là dành riêng và sử dụng cho các tài khoản đặc biệt

**IV. Phân bổ (allocation)**

+ Quá trình tạo ra các RID duy nhất là một hoạt động đơn lẻ. Một bộ điều khiển miền được gán vai trò RID master và nó phân bổ một chuỗi các mã định danh tương đối cho mỗi bộ điều khiển miền trong miền

+ Khi một tài khoản hoặc nhóm miền mới được tạo trong bản sao Active Directory của một bộ điều khiển miền, nó sẽ được gán một SID. RID cho SID mới được lấy từ việc phân bổ các RID của bộ điều khiển tên miền

+ Khi nguồn cung cấp số nhận dạng tương đối của nó bắt đầu cạn kiệt, bộ điều khiển miền sẽ yêu cầu một khối khác từ RID master

+ Mỗi bộ điều khiển miền chỉ sử dụng mỗi giá trị trong một khối định danh tương đối một lần. RID master chỉ phân bổ mỗi khối giá trị định danh tương đối một lần. Quá trình này đảm bảo rằng mọi tài khoản và nhóm được tạo trong miền đều có một mã định danh tương đối duy nhất

**V. SID và Global unique identifiers**

**VI. SID phổ biến**

**A screenshot of a white page

Description automatically generated**

**A close up of text

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a list of numbers

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a group

Description automatically generated**

**A screenshot of a white page

Description automatically generated**

**A screenshot of a group

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a group

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**VII. Capability SIDs**

+ Capability SID được sử dụng để xác định duy nhất và bất biến các khả năng đại diện cho một unforgettable token (cấp quyền truy cập vào tài nguyên như: tài liệu, camera,…) cho Universal Windows Application

+ Một ứng dụng có khả năng được cấp quyền truy cập vào tài nguyên mà khả năng đó được liên kết và một ứng dụng không có khả năng sẽ bị từ chối quyền truy cập vào tài nguyên.

+ Các Capability SID mà hệ điều hành nhận biết được đều được lưu trữ trong Windows Registry theo đường dẫn 'HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityClasses\AllCachedCapabilities'. Bất kỳ SID khả năng nào được thêm vào Windows bởi các ứng dụng của bên thứ nhất hoặc bên thứ ba đều được thêm vào vị trí này

RID Hijacking

I. Kỹ thuật (Thuộc về cover tracking):

- Là chiến thuật để kẻ tấn công duy trì bên trong hệ thống của nạn nhân bằng cách chiếm đoạt RID tài khoản Admin cho tài khoản Guest hoặc một tài khoản cục bộ khác

- Việc tạo ra sự duy trì trong hệ thống của nạn nhân cho phép kẻ tấn công thiết lập một chỗ đứng, liên tục lấy lại quyền truy cập mà bạn không nhìn thấy và cho phép kẻ tấn công đăng nhập như một tài khoản được ủy quyền mà kẻ tấn công đã chiếm đoạt

II. Lab

1. Lấy phiên của tài khoản có quyền admin

A screenshot of a computer screen

Description automatically generated

2. Tạo sessions

A screen shot of a computer

Description automatically generated

3. Sử dụng payload **post/windows/manage/rid\_hijack**

A screenshot of a computer program

Description automatically generated

4. Giá trị RID từ 501 được ghi đè thành 500 (RID của quản trị viên)

A screenshot of a computer

Description automatically generated

5. Sử dụng tools impacket để lấy shell CMD của may mục tiêu

A computer screen with white text

Description automatically generated

A screenshot of a computer screen

Description automatically generated