Users and SIDs: Section 1 Transcript

Introduction

Welcome to the Users and Security Identifiers (SIDs) module.

During this module, we're going to discuss the uses and types of SIDs, how SIDs are composed, and how to identify well-known SIDs.

Throughout this module, you'll be presented with opportunities to assess and apply what you've learned.

At the end of this module, you will be able to:

- Define Security Identifiers (SIDs),
- Identify well-known SIDs,
- Decode a Machine SID, and
- Associate a User profile with a SID.

Bypass Exam Introduction

If you are already familiar with the subject matter presented in this module, you can choose to take a Bypass Exam to skip this module.

The Bypass Exam option provides a single opportunity to successfully demonstrate your competence with the material presented within the module. If you pass, you'll receive credit for completing the module, unlocking the content within, and you will be free to proceed to the next module. If you do not pass, you will need to successfully complete the module, including all exercises and the Module Exam, to receive credit.

Click the Next Section button to continue.

Users and SIDs: Section 2 Transcript

SIDs 1/9

Before we discuss SIDs, we need to mention access tokens which contain a SID. Access tokens contain information about the owner (user) and the network privileges assigned to them.

Access tokens contain a:

- SID,
- Group IDs,
- User rights, and
- Privileges.

SIDs 2/9

A SID is produced when the account is first created in Windows.

A SID is a unique value of variable length and is used to identify:

- Users,
- Groups,
- Domains, or
- Computers.

SIDs 3/9

SIDs consist of:

- A revision level,
- An identifier-authority value,
- One or more subauthority values, and
- A Relative ID (RID).

Let's look at an example of the SID ending with the Relative ID of 1010.

When displayed textually, all SIDs have an "**S**" prefix.

The revision level is the version of the SID specification - within this SID, it's a "**1**".

The identifier-authority value is "**5**" which is the Windows security authority.

Other possible identifier-authority values are:

- 0 - Null Authority,
- 1 - World Authority,

- 2 - Local Authority,
- 3 - Creator Authority,
- 4 - Non-unique Authority,
- 5 - NT Authority, and
- 9 - Resource Manager Authority.

The subauthority value is the domain or local computer identifier, which in this example is the long string of numbers beginning with "21".

Any group or user that is not created by default, has a RID of 1000 or greater - "**1010**" is the RID in this example.

The RID starts at 1000 and increases in increments of 1 for each new user or group. So, for this example, this SID is the 11th SID the domain has issued.

Note: A SID, not including the RID, is either the current machine's SID or the domain's SID.

Well-known SIDs

Well-known SIDs identify generic groups and generic users.

For example, there are well-known SIDs to identify the following groups and users:

- Everyone or Users, which is a group that includes all users,
- CREATOR_OWNER, which is used as a placeholder in an inheritable Access Control Entry (ACE). When the ACE is inherited, the system replaces the CREATOR_OWNER SID with the SID of the object's creator, and
- The Administrators group for the built-in domain on the local computer.

Well-known SIDs

Here are some well-known SIDs:

- S-1-5-18 is the well-known SID for the LocalSystem account. Windows loads this account's profile when a **program** or **service** runs in the LocalSystem account.
- S-1-5-19 is the well-known SID for the LocalService account. Service Control Manager uses this account to run **local** services that don't need to run as the LocalSystem account.
- S-1-5-20 is the well-known SID for the NetworkService account. Service Control Manager uses this account to run **network** services that don't need to run as the LocalSystem account.
- S-1-5-21 is the <Non-Unique Authority Name>.

Decoding a Machine SID

Machine SIDs are stored in this registry key: HKLM\SAM\SAM\Domains\Account.

This key has two values, F and V.

The F value maintains an incremental record of RIDs which is covered later in this module.

The V value is a binary value that contains the computer SID within the last 12 bytes of data.

Machine SIDs can also be retrieved from the Security Account Manager (SAM) file, which in a default Windows installation will be located here: C:\Windows\System32\config\SAM.

If the SAM file is missing at startup, a backup can be retrieved from the last 12 bytes of the registry hive: \HKEY_LOCAL_MACHINE\SECURITY\Policy or from the Windows file system found here: C:\Windows\System32\config\SECURITY.

Decoding a Machine SID

Let's review an example of decoding a machine SID:

1. Divide the bytes into 3, four-byte sections,
2. Reverse the order of bytes in each section,
3. Convert each section into decimal, and
4. Add the machine SID prefix.

User Relative ID (RID)

The User Relative ID (RID) is a variable length number that is assigned to objects at creation and becomes part of the object's SID that uniquely identifies an account or group within a domain.

Windows allocates RIDs starting at 1000 for users; RIDs having a value of less than 1000 are considered reserved and are used for special accounts. For example, all Windows accounts with a RID of 500 are considered built-in Administrator accounts in their respective issuing authorities.

RIDs increment and are not reused when a user is deleted. A record of this is kept here: HKLM\SAM\SAM\Domains\Account\F. This value is stored in reverse hex or little endian with an offset of 0x48 and a length of 4.This is the next number that will be used. When the value reaches its maximum hexadecimel number, it will rollback and start incrementing from 0.

When a user account is added, the following keys are added to the registry under HKEY Local Machine\SAM.

Click each registry key for more information.

HKLM\SAM\SAM\Domains\Account\Users\Names\%username%

- This key determines the login name
- The (Default) values holds a number which matches up to an 8-digit number located here (nulls are prefixed to the number if they are less than 8).

HKLM\SAM\SAM\Domains\Account\Users\00000XXX

- Within this key are to REG_BINARY values: F and V

Exercise Introduction

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Users and SIDs: Section 3 Transcript

Summary

You have completed the Users and SIDs module.

During this module, we discussed the uses and types of SIDs, how SIDs are composed, and how to identify well-known SIDs. Then we focused on applying what was learned by using a practical exercise to associate a User profile with a SID.

You should now be able to:

- Define Security Identifiers (SIDs),
- Identify well-known SIDs,
- Decode a Machine SID, and
- Associate a User profile with a SID.

To receive credit and advance to the next module, you must achieve a passing score on the Module Exam.

Click the Next Section button to begin the Module Exam.