The Windows Security Journey Workbook

Version 1.0
June-2025

By Dr. Shlomi Boutnaru

Created using Google Gemini

Introduction

Having explored "The Windows Security Journey," you now possess a foundational understanding of basic security features included as part of the Windows operating system This companion workbook is designed to transform that knowledge into true mastery.

Through carefully crafted multi-choice questions and challenging hand-on tasks, you will actively engage with the concepts, applying theory to practical scenarios. This hands-on approach is crucial for solidifying your understanding and developing the essential skills needed to navigate the intricacies of Windows internals.

Lastly, you can follow me on twitter - @boutnaru (https://twitter.com/boutnaru). Also, you can read my other writeups on medium - https://medium.com/@boutnaru. Lastly, You can find my free eBooks at https://TheLearningJourneyEbooks.com.

Prepare to delve deeper; true expertise is achieved through practice. Let's begin!

Multi-Choice Questions

Question 1:

What is the primary goal of a Security Identifier (SID)?

1. To uniquely identify a security principal/group
2. To manage network shares
3. To control process execution
4. To encrypt user passwords

Question 2:

Which of the following is NOT typically found in an Access Token related to a user's SID?

1. User's SID
2. A list of privileges
3. SIDs of groups the user belongs to
4. User's email address

Question 3:

What is the purpose of the Relative ID (RID) in an SID?

1. To identify the highest level of authority
2. To denote a universal well-known SID
3. To identify a specific user/group in a local computer/domain
4. To specify the SID structure version

Question 4:

Which well-known SID includes all users?

1. S-1-5-80
2. S-1-0-0
3. S-1-5-21
4. S-1-1-0

Question 5:

What is the main purpose of a Security Descriptor (SD)?

1. To define network communication protocols
2. To manage system performance logs
3. To hold security information related to a specific securable object
4. To store application configuration settings

Question 6:

What are the four main fields contained within a Security Descriptor?

1. Name, Size, Type, Date
2. Permissions, Auditing, Logging, Alerts
3. Owner, Group, DACL, SACL
4. Version, Identifier, Sub-authorities, RID

Question 7:

What is DACL primarily used for in a Security Descriptor?

1. Encrypting data
2. Allowing/denying permissions
3. Managing system processes
4. Auditing access attempts

Question 8:

What is the text-based format for representing a Security Descriptor?

1. CSV
2. SSDL
3. JSON
4. XML

Question 9:

What does a DACL (Discretionary Access Control List) within a securable object contain?

1. The object's creation date
2. Configuration settings for the object
3. A list of all system users
4. A list of group/user SIDs and their access rights

Question 10:

What is the purpose of a SACL (System Access Control List) in a securable object?

1. To encrypt the object's content
2. To state what logging/auditing should be done when accessing the object
3. To define the object's owner
4. To grant full control permissions

Question 11:

What is the main characteristic of "Privileges" in Windows security?

1. They define network connectivity
2. They are rights for an account to perform system-related operations
3. They manage application installations
4. They control access to securable objects

Question 12:

Which privilege is required for debugging processes owned by a different user account?

1. SeLoadDriverPrivilege
2. SeDebugPrivilege
3. SeShutdownPrivilege
4. SeCreatePagefilePrivilege

Question 13:

What is SAM (Security Account Manager) in Windows?

1. A network management tool
2. An application whitelisting feature
3. The database that stores local user names/hashed passwords
4. A system monitoring service

Question 14:

Where is the SAM file typically located on a Windows system?

1. %programfiles%\SAM
2. %windir%\System32\config\SAM
3. %appdata%\Microsoft\SAM
4. %temp%\SAM

Question 15:

What level of permissions is required to view the content of the SAM database?

1. Local Administrator
2. Network Service
3. SYSTEM
4. Standard User

Question 16:

What was SYSKEY created for, in relation to SAM?

1. To encrypt account password information stored in SAM
2. To audit changes to SAM
3. To synchronize SAM with Active Directory
4. To compress the SAM database

Question 17:

What does an "Access Token" represent for a specific process/thread?

1. Its network bandwidth
2. The amount of memory it can use
3. Its access rights, privileges, and identity
4. Its CPU utilization

Question 18:

Which of the following is NOT typically included in an Access Token?

1. User's preferred desktop background
2. User's SID
3. List of privileges
4. Primary group (for POSIX subsystems)

Question 19:

Which Win32 API function can be used to duplicate an access token?

1. SetTokenInformation
2. OpenProcessToken
3. DuplicateTokenEx
4. CreateProcessWithTokenW

Question 20:

Where is the access token stored in kernel mode?

1. In temporary memory, not persisted
2. In a file on disk
3. In the registry
4. Using struct _TOKEN

Answers for Multi-Choice Questions

1. 1
2. 4
3. 3
4. 4
5. 3
6. 3
7. 2
8. 2
9. 4
10. 2
11. 2
12. 2
13. 3
14. 2
15. 3
16. 1
17. 3
18. 1
19. 3
20. 4

Hand-On Tasks

Task 1	
Objective	Understand the structure and significance of SIDs for various security principals
Instructions	Identify Your User SID: 1. Open cmd.exe or PowerShell. 2. Type “whoami /user” and press Enter. 3. Note down your user's SID.
Question	Can you identify the "Identifier Authority" and "Relative ID" parts of your SID?

Task 2	
Objective	Understand how DACLs control access to securable objects and perform basic permission modifications
Instructions	1. Create a test folder on your desktop (C:\users\%username%\Desktop) 2. Examine Default Permissions ○ Right-click the folder-> Properties-> Security tab
Question	What are the default permissions for this newly created folder? Who has access and what level of access do they have?

Task 3	
Objective	Understand how DACLs control access to securable objects and perform basic permission modifications
Instructions	1. Remove “Users” or “Authenticated Users” (if present) from the list of permissions form the folder created in the previous taks 2. Add your current user account and grant it “Full Control”
Question	Explain how this action modifies the DACL of the folder. What would happen if another user (without administrative privileges) tried to access this folder?

Task 4	
Objective	Understand how DACLs control access to securable objects and perform basic permission modifications
Instructions	1. For the “Everyone” group, explicitly check the “Deny” checkbox for “Full Control” (on the same directory as the previous task) ○ If the “Everyone” group does not appear please add it
Question	What do you expect to happen if your user (who also has explicit “allow” for “Full Control”) tries to access the folder now? Test it

Task 5	
Objective	Explore Windows privileges and understand the capabilities of various built-in accounts like Local System, Network Service, and Local Service
Instructions	1. Open the Local Group Policy Editor (gpedit.msc). 2. Navigate to “Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignments” 3. Scroll through the list of privileges (e.g., "Load and unload device drivers," "Debug programs"). 4. Select three privileges
Question	For the three privileges you have selected: 1. What is their purpose (you can check the “Explain” tab after double clicking on them)? 2. Which user accounts or groups are assigned these rights by default?