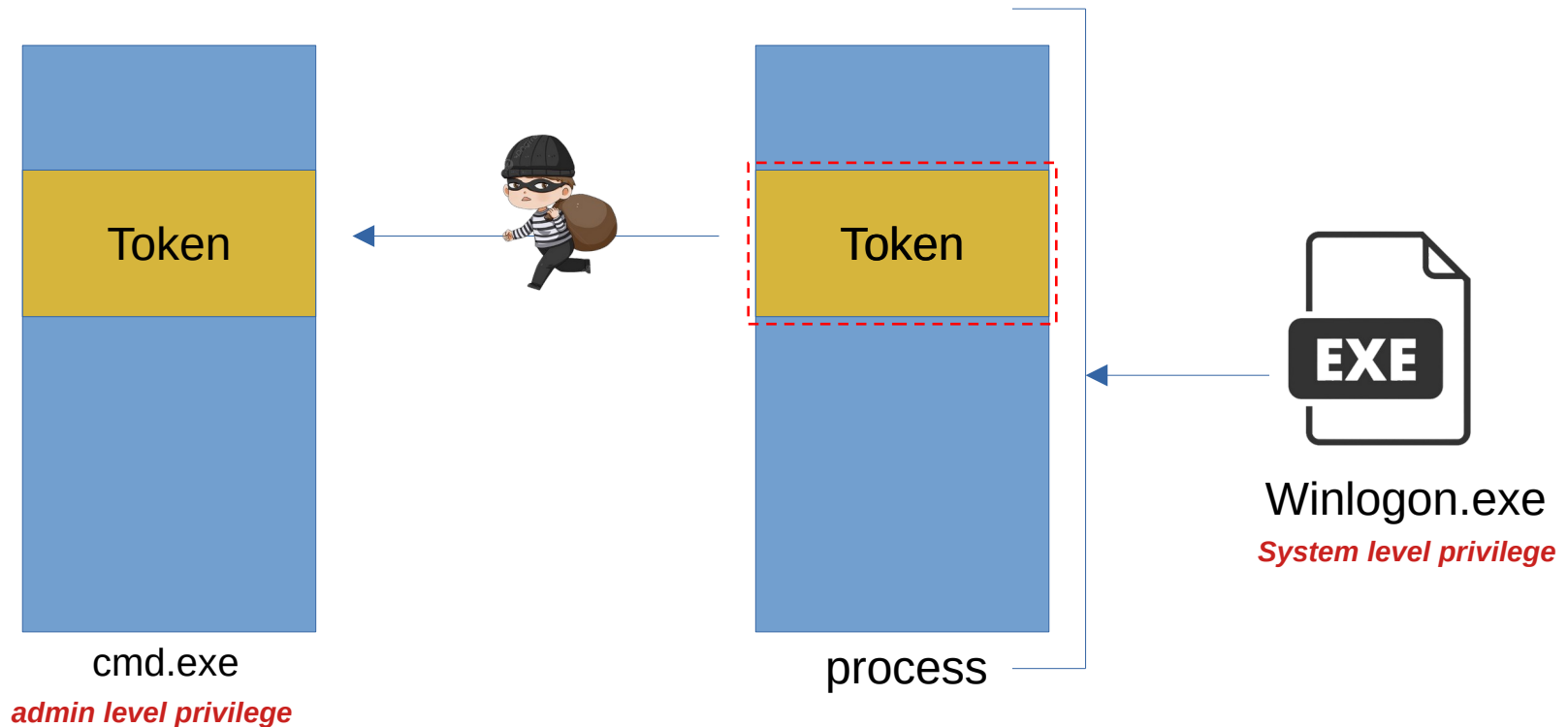


# Privilege escalation

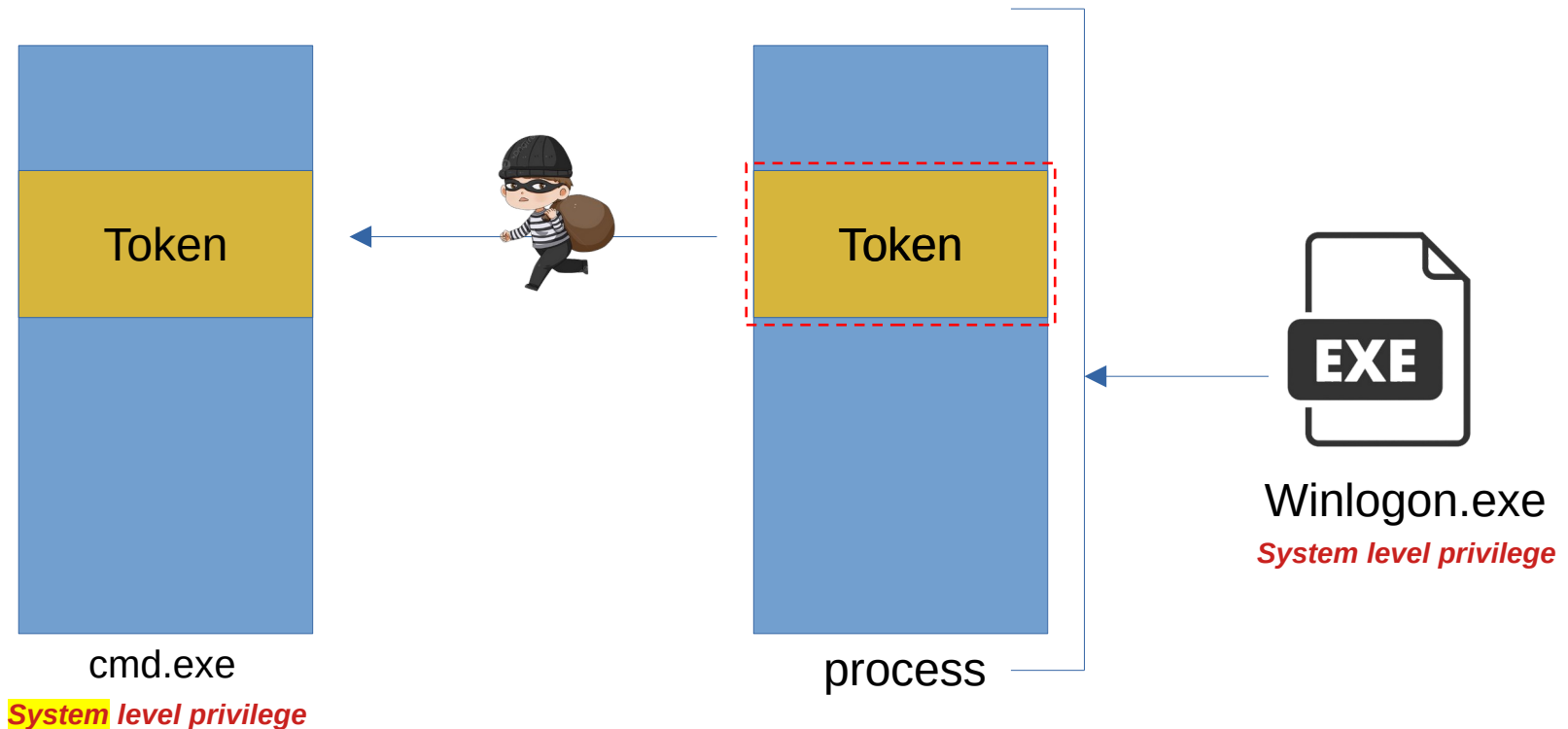
Privilege escalation is the process of gaining higher access rights or permissions on a system than were originally granted.

# Token theft

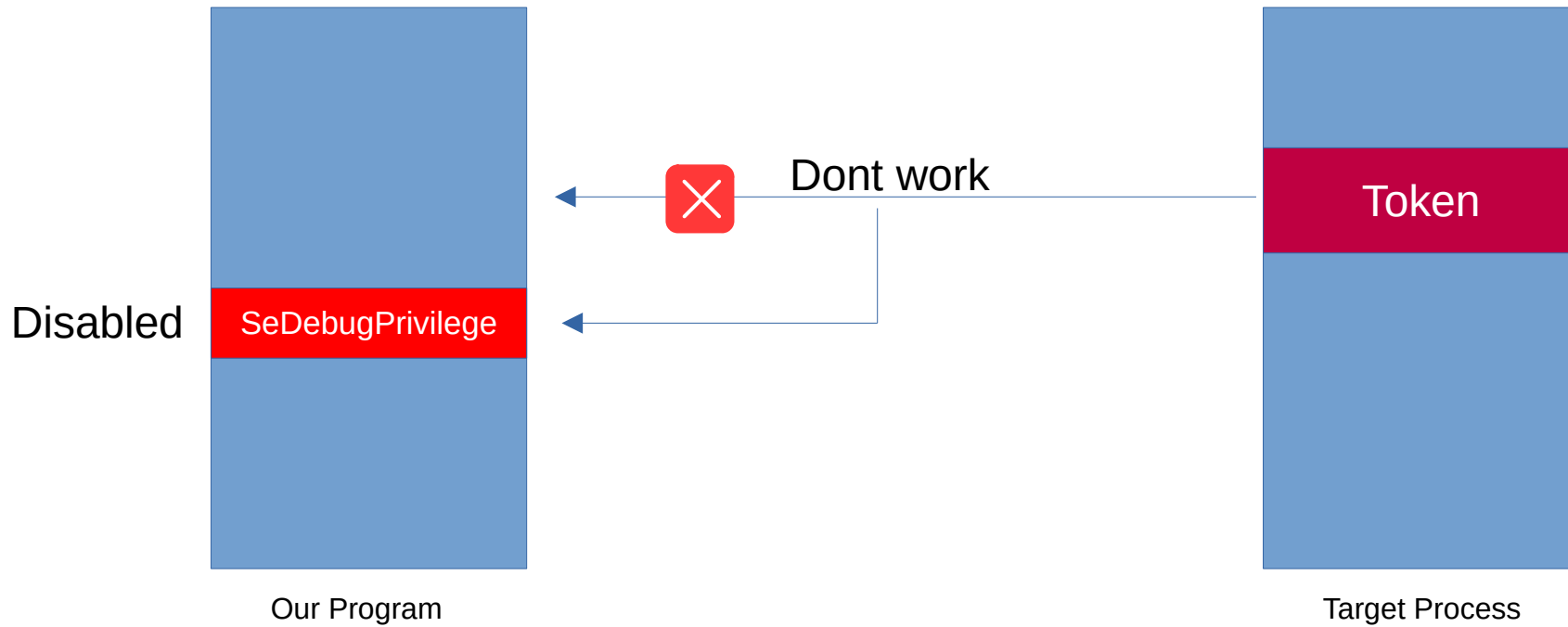
# Token theft



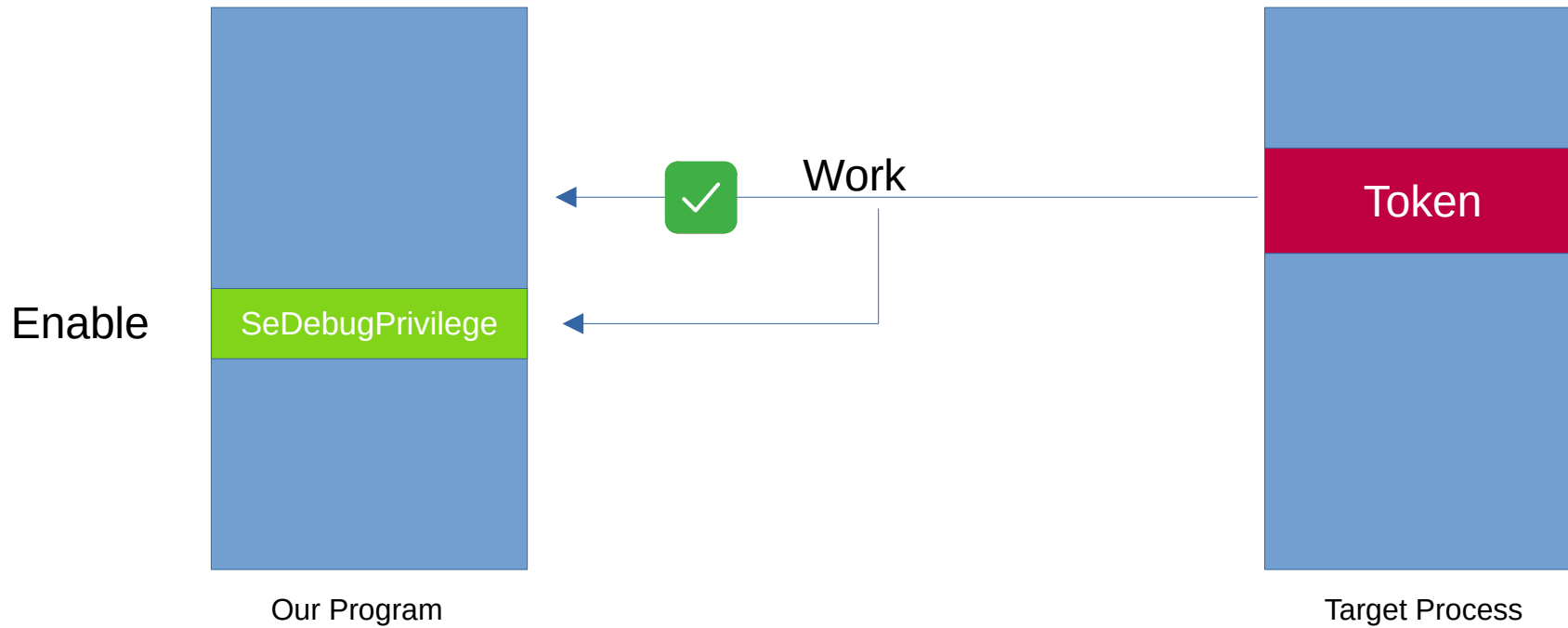
# Token theft



# Stealing token



# Stealing token



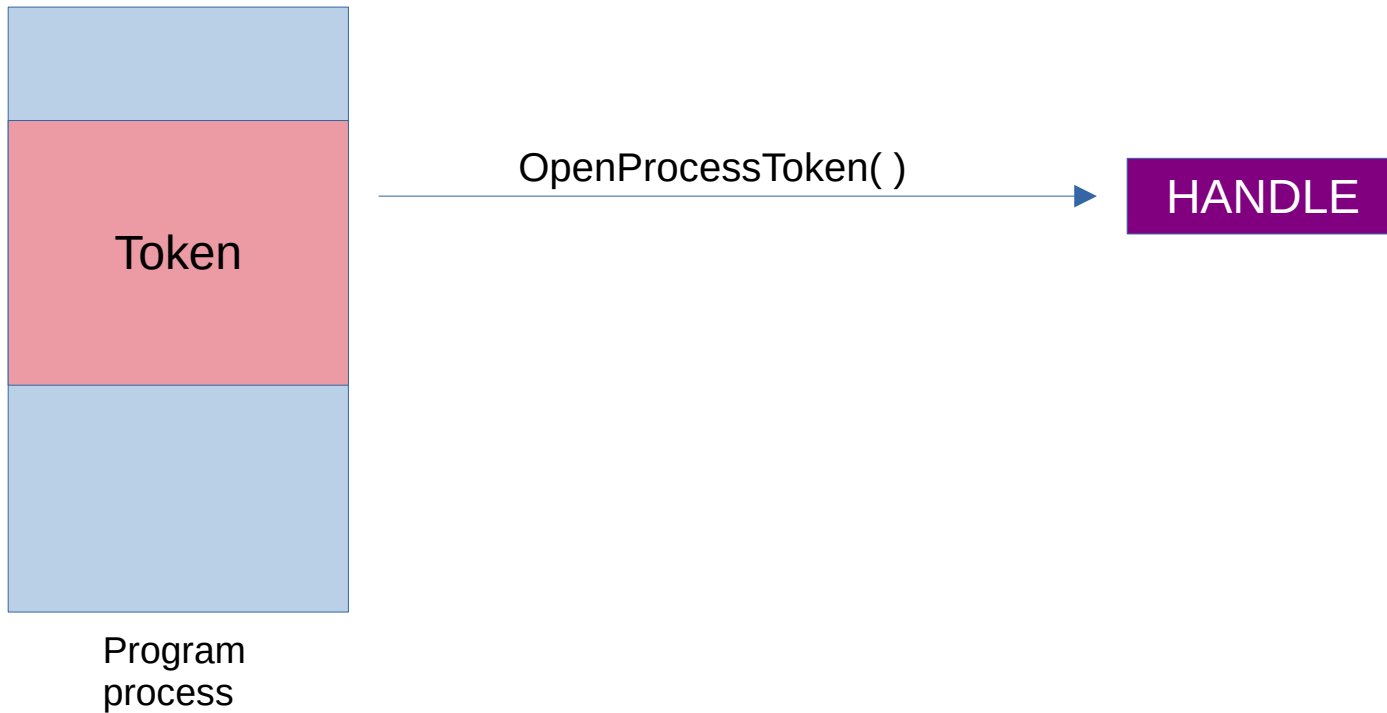
# Enable “SeDebugPrivilege”



Program  
process

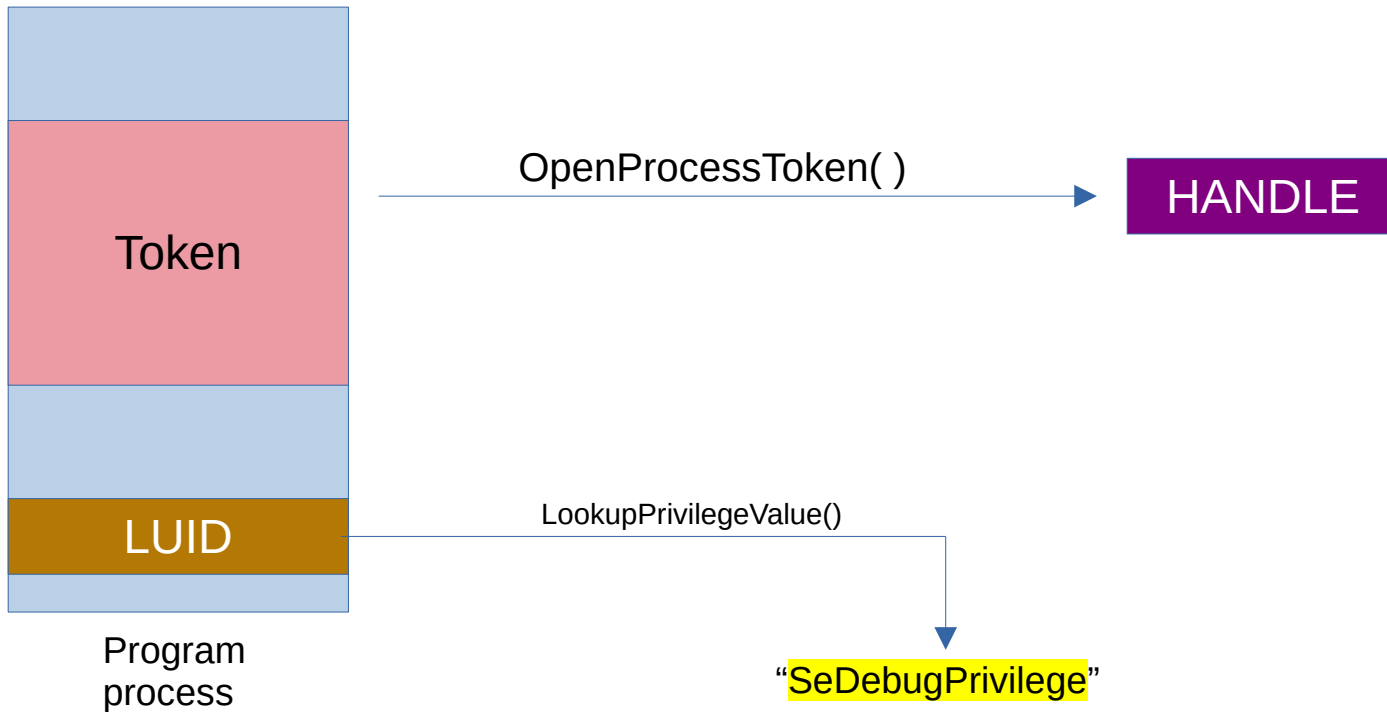
# Enable “SeDebugPrivilege”

Step 1: Get the token handle of our program



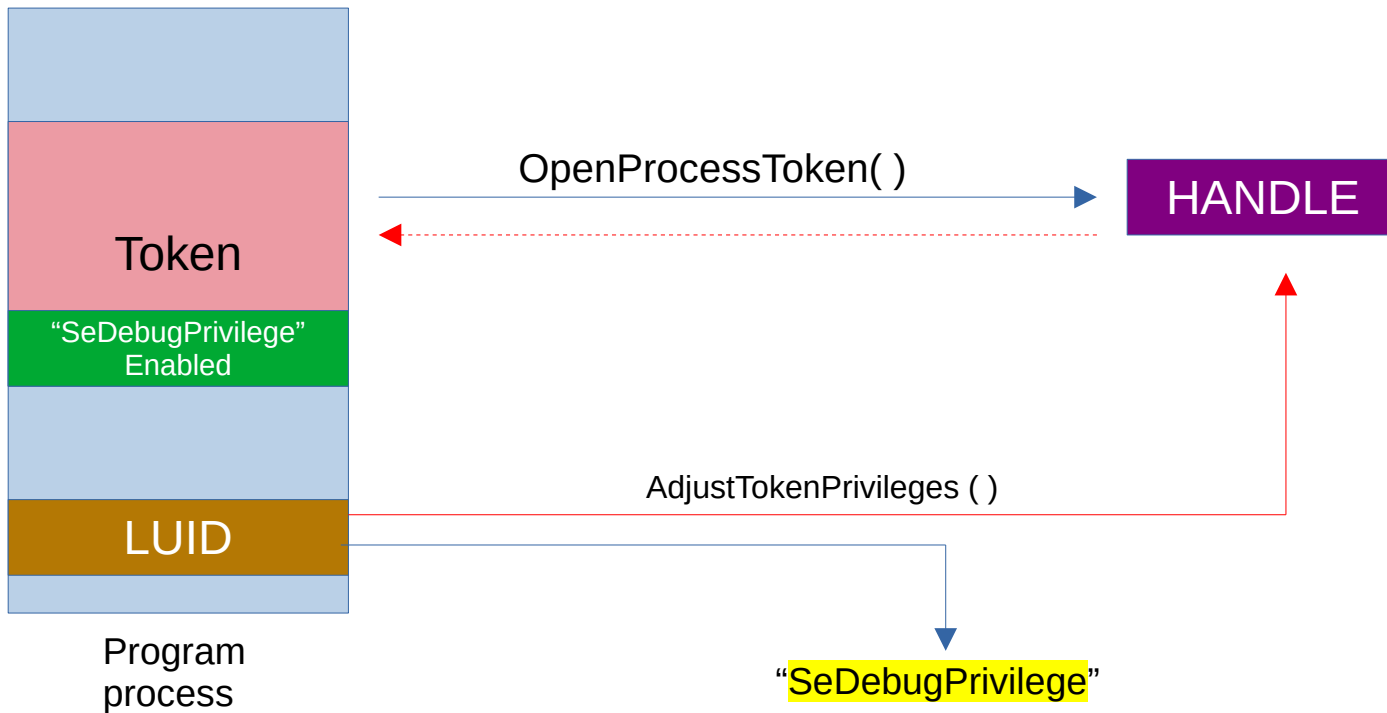
# Enable “SeDebugPrivilege”

Step 2: Get LUID (id) of “SeDebugPrivilege”



# Enable "SeDebugPrivilege"

Step 3: Set "SeDebugPrivilege" to our token



Lets see the program code

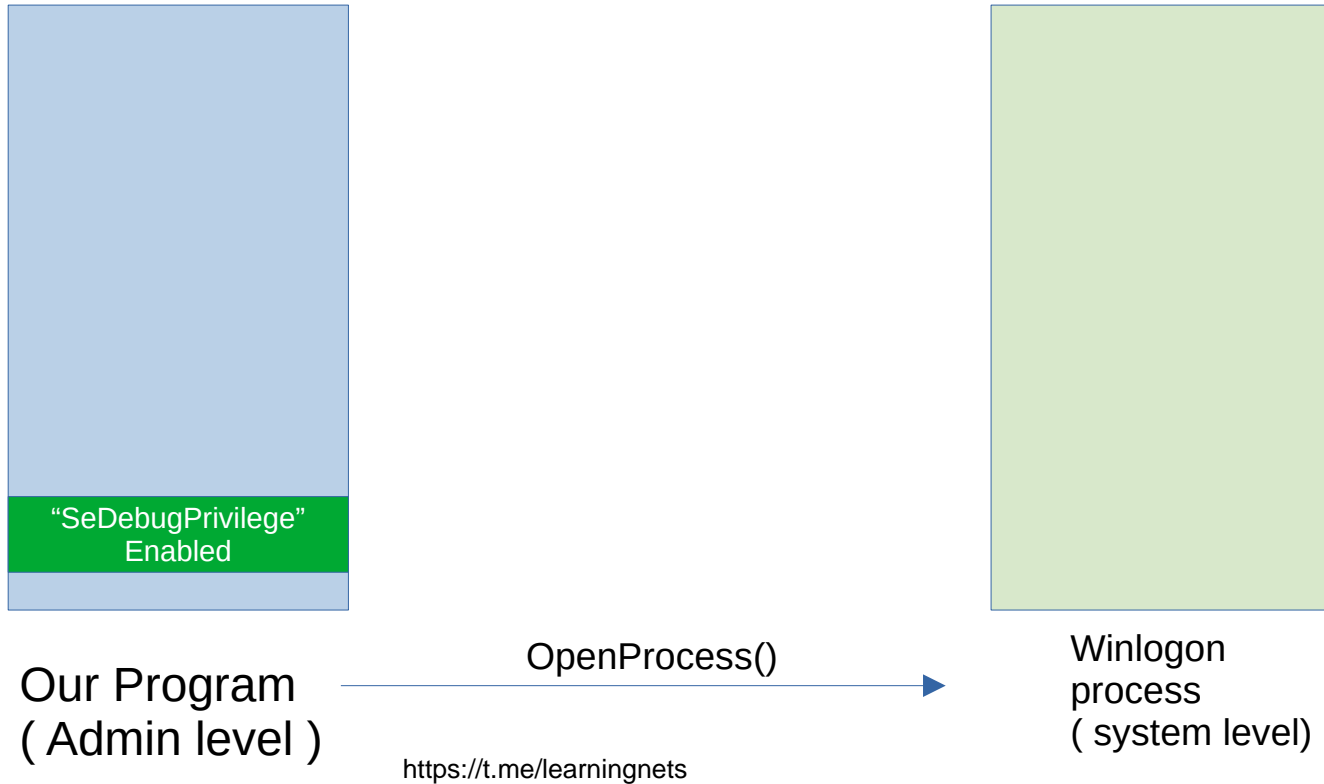
# Steal the token



Our Program

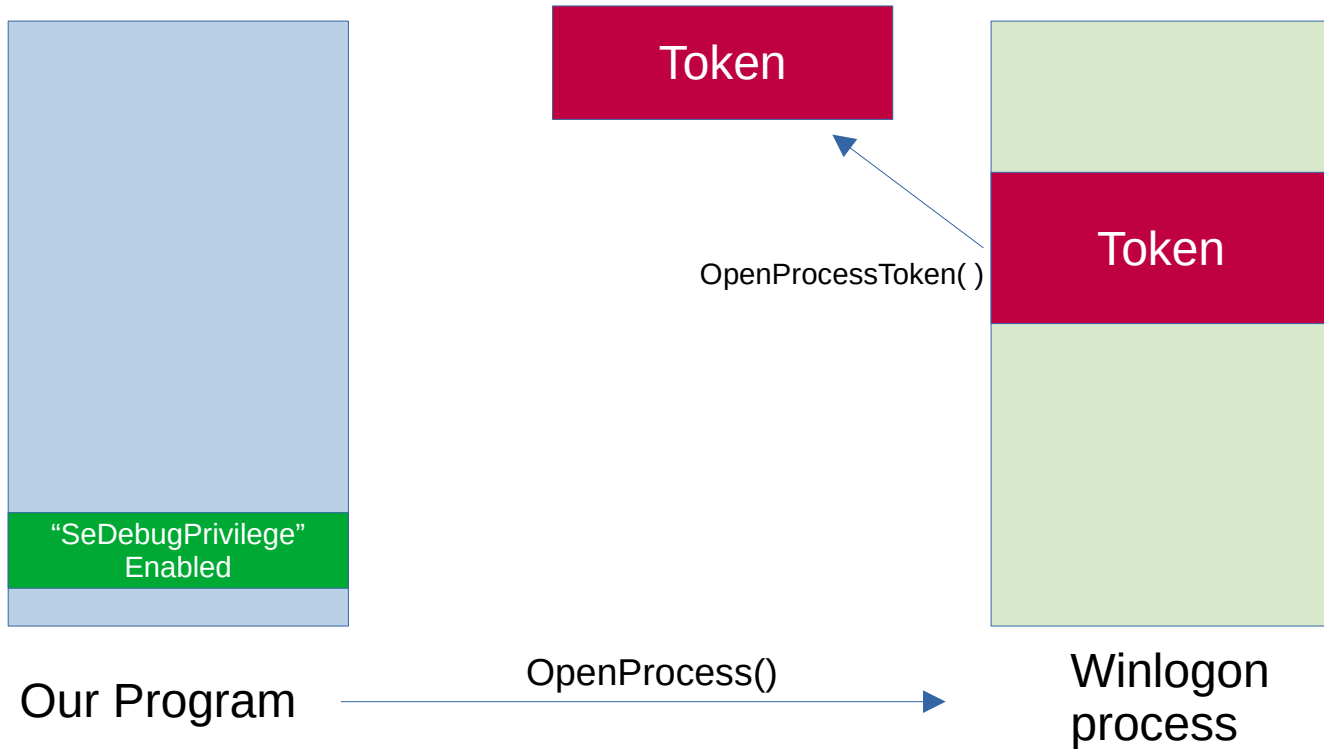
# Steal the token

Step 1: Open winlogon process



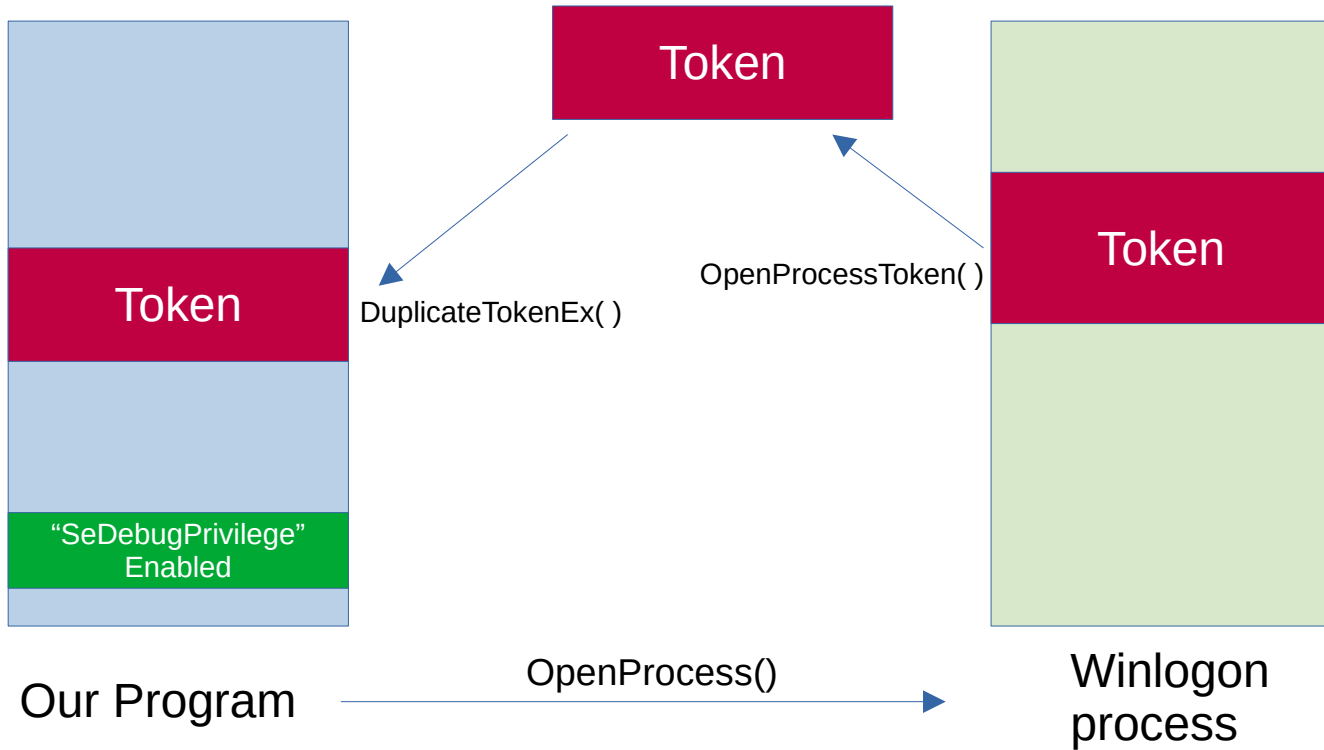
# Steal the token

Step 2: Open token of winlogon process



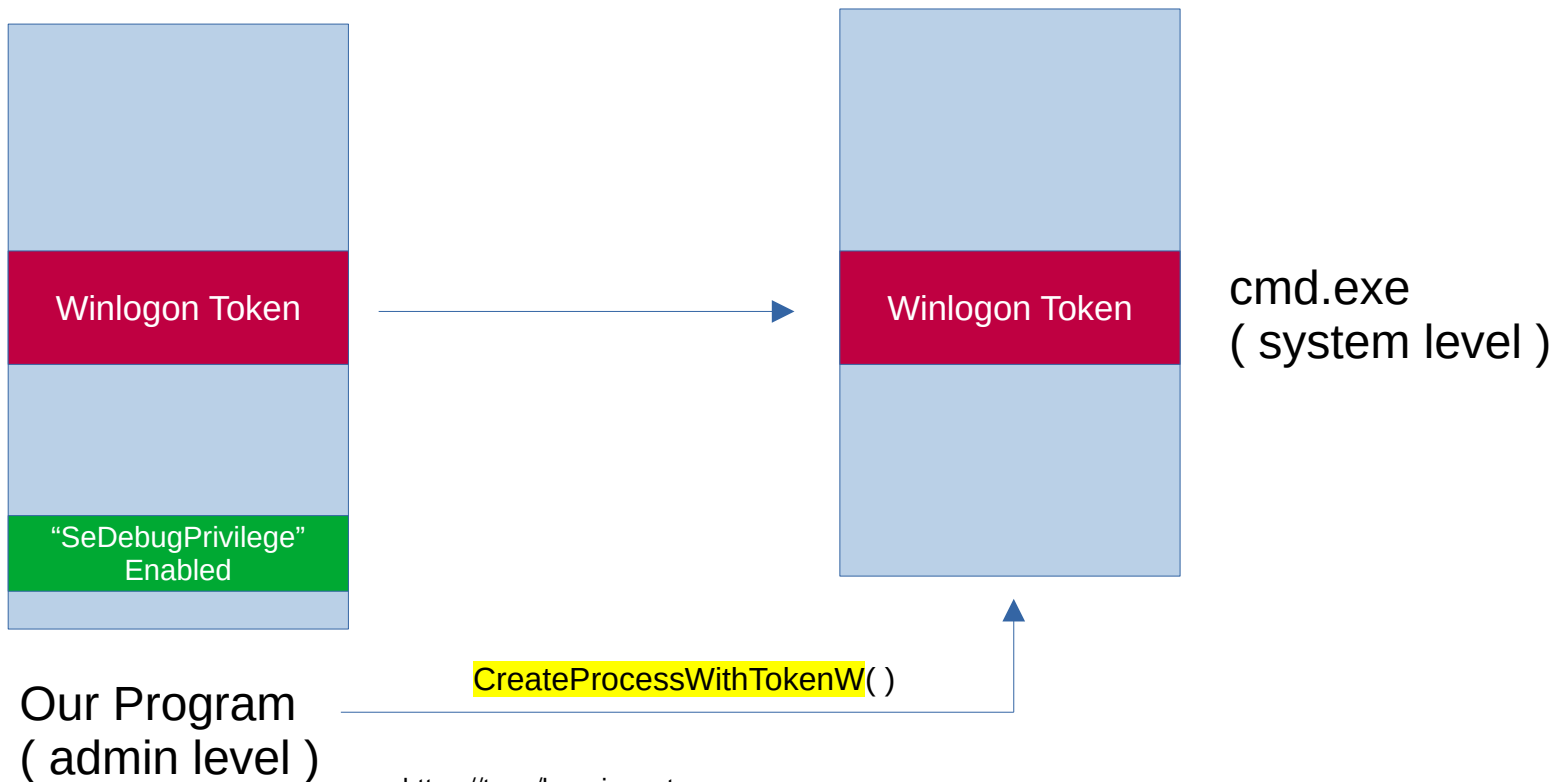
# Steal the token

Step 3: Duplicate the token



# Steal the token

Step 4: create a process with the duplicated token to get system level privilege



Lets see the program code