lsadump::changentlm and lsadump::setntlm work, but generate Windows events

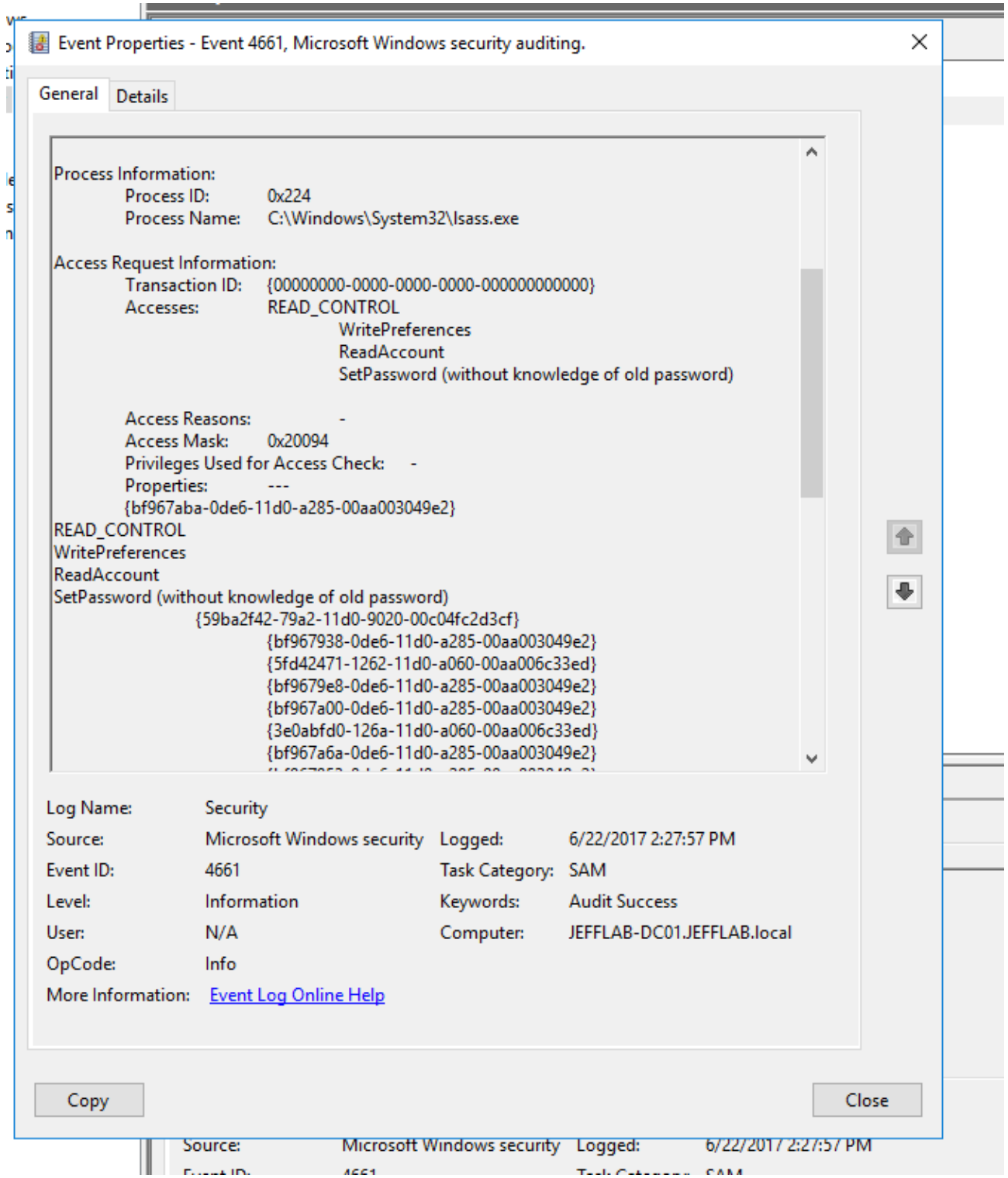
By JeffAWarren

Published: 2017-06-22 · Archived: 2026-04-06 01:55:33 UTC

I noticed when using the lsadump::changentlm and lsadump::setntlm, that the SETPASSWORD privilege is still being requested. I see the following information in my Active Directory event logs after performing a password change:
*Event 4661 with privilege request for SetPassword (without knowledge of old password) *(screenshot attached)*
*Event 4723 for an attempt made to change an account's password
*Event 4738 for a user account being changed for the Password Last Set value

Domain Controller is Windows Server 2016:
Major: 10
Minor: 0
Build: 14393

Revision: 0



Source: https://github.com/gentilkiwi/mimikatz/issues/92