

# 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

**Event Properties - Event 4661, Microsoft Windows security auditing.**

**General** Details

**Process Information:**  
Process ID: 0x224  
Process Name: C:\Windows\System32\lsass.exe

**Access Request Information:**  
Transaction ID: {00000000-0000-0000-0000-000000000000}  
Accesses: READ\_CONTROL  
WritePreferences  
ReadAccount  
SetPassword (without knowledge of old password)

Access Reasons: -  
Access Mask: 0x20094  
Privileges Used for Access Check: -  
Properties: ---  
{bf967aba-0de6-11d0-a285-00aa003049e2}

READ\_CONTROL  
WritePreferences  
ReadAccount  
SetPassword (without knowledge of old password)  
{59ba2f42-79a2-11d0-9020-00c04fc2d3cf}  
{bf967938-0de6-11d0-a285-00aa003049e2}  
{5fd42471-1262-11d0-a060-00aa006c33ed}  
{bf9679e8-0de6-11d0-a285-00aa003049e2}  
{bf967a00-0de6-11d0-a285-00aa003049e2}  
{3e0abfd0-126a-11d0-a060-00aa006c33ed}  
{bf967a6a-0de6-11d0-a285-00aa003049e2}

**Log Name:** Security  
**Source:** Microsoft Windows security **Logged:** 6/22/2017 2:27:57 PM  
**Event ID:** 4661 **Task Category:** SAM  
**Level:** Information **Keywords:** Audit Success  
**User:** N/A **Computer:** JEFFLAB-DC01.JEFFLAB.local  
**OpCode:** Info  
**More Information:** [Event Log Online Help](#)

Copy Close

Source: Microsoft Windows security Logged: 6/22/2017 2:27:57 PM  
Event ID: 4661 Task Category: SAM

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