




Some ways to dump LSASS.exe





Mark Mo · Follow


5 min read · Jul 2, 2019

 200



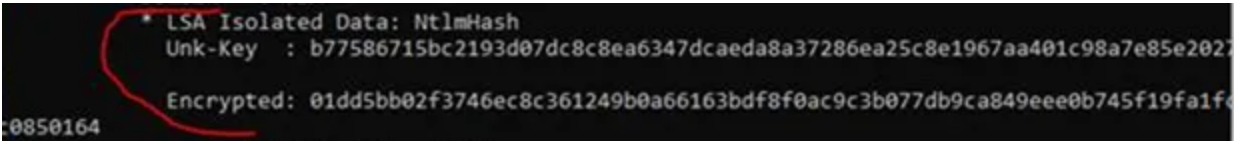






As always this is for educational purposes. I like to find multiple ways to do the same thing. It helps me learn and writing about it help me learn too. This is a list of several ways to dump LSASS.exe (Local Security Authority Subsystem Service).

Before I begin, when I’m running Windows 10 or Windows Server 2016 (or higher) and Credential Guard is configured and running, dumping LSASS won’t be super useful for NTLM Hashes. This is what it looks like if Credential Guard is running and I try to get NTLM hash. No good for dumping 😊



However, If I’m running older windows OS’s or Credential Guard is not configured and running, I may be able to pull the NTLM hashes (or even

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

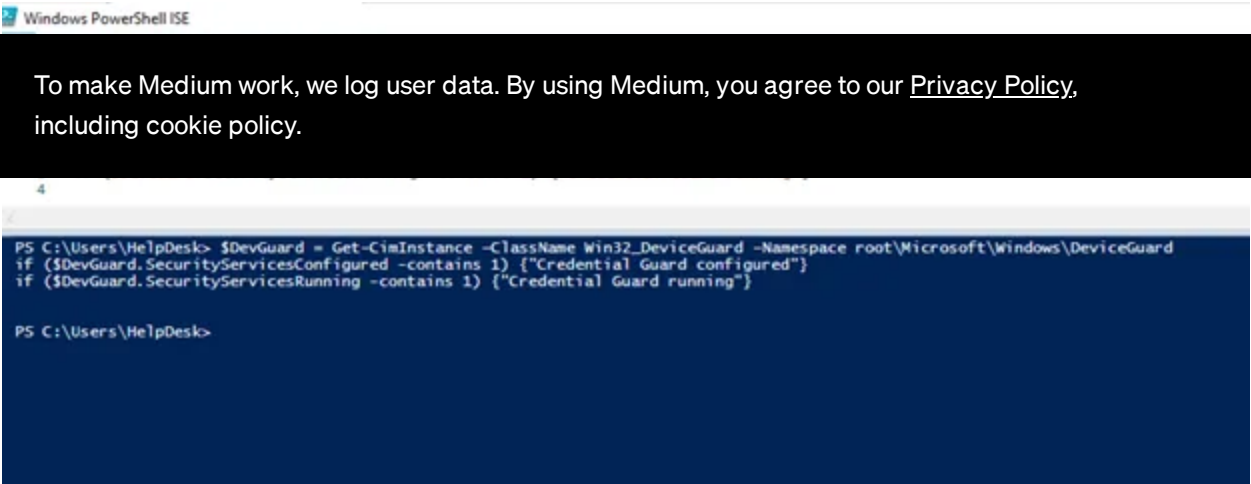
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

★ Membership

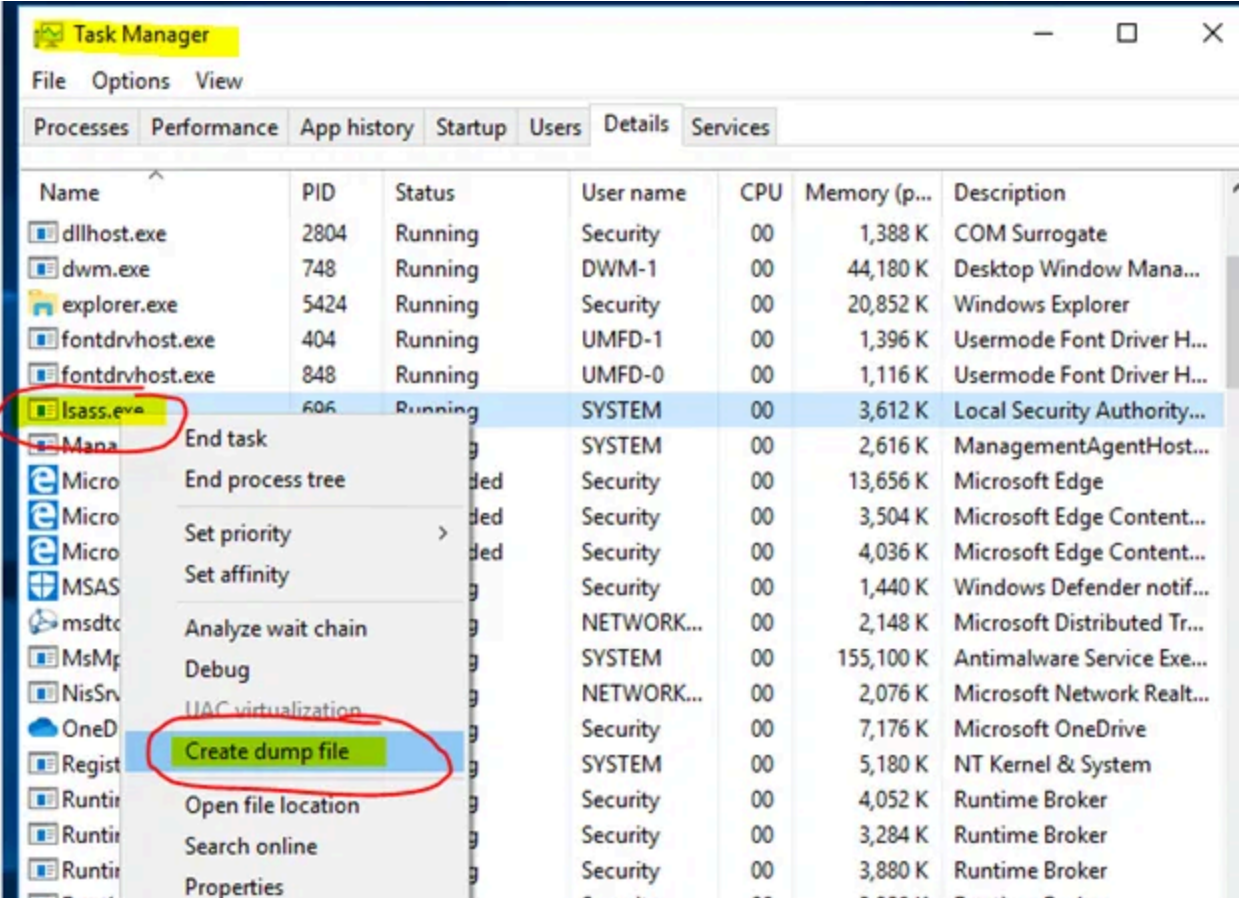
- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month



Let’s start Dumping LSASS.EXE.

The first way is to use task manager (running as admin). Click on lsass.exe and select “Create Dump File”



Medium

Sign up to discover human stories that deepen your understanding of the world.

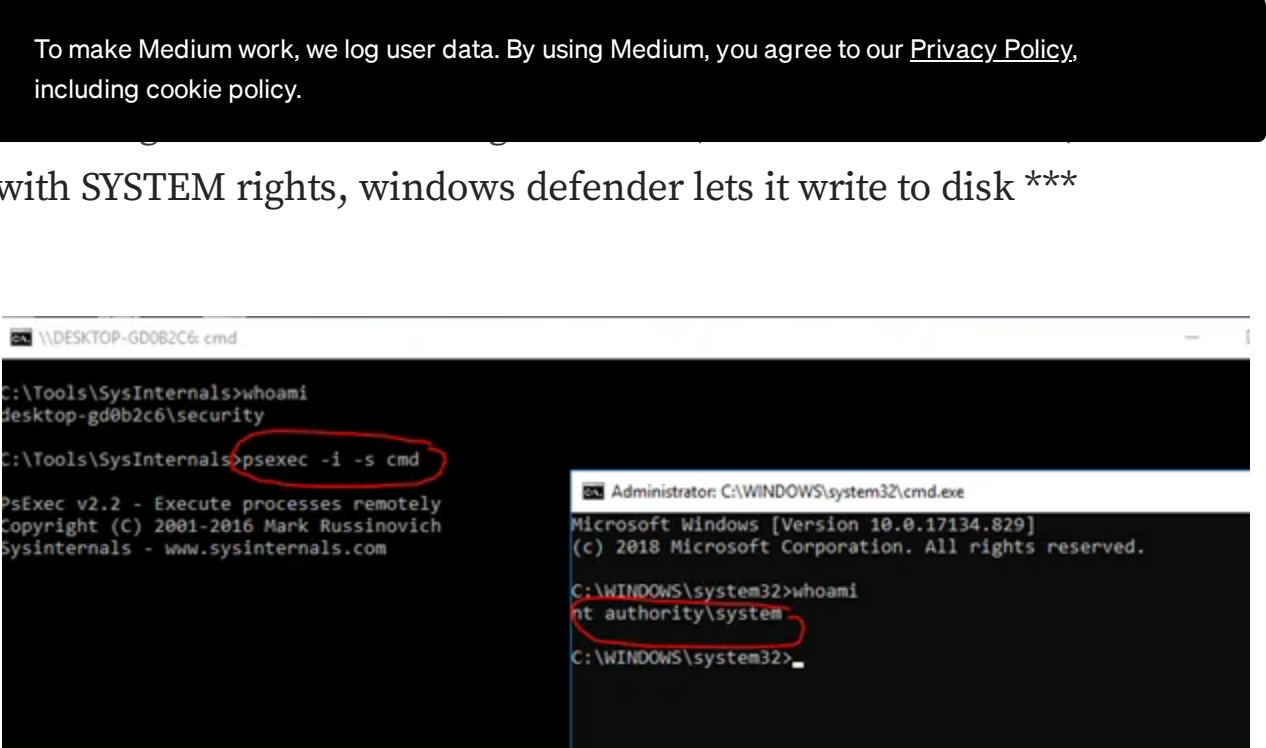
Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

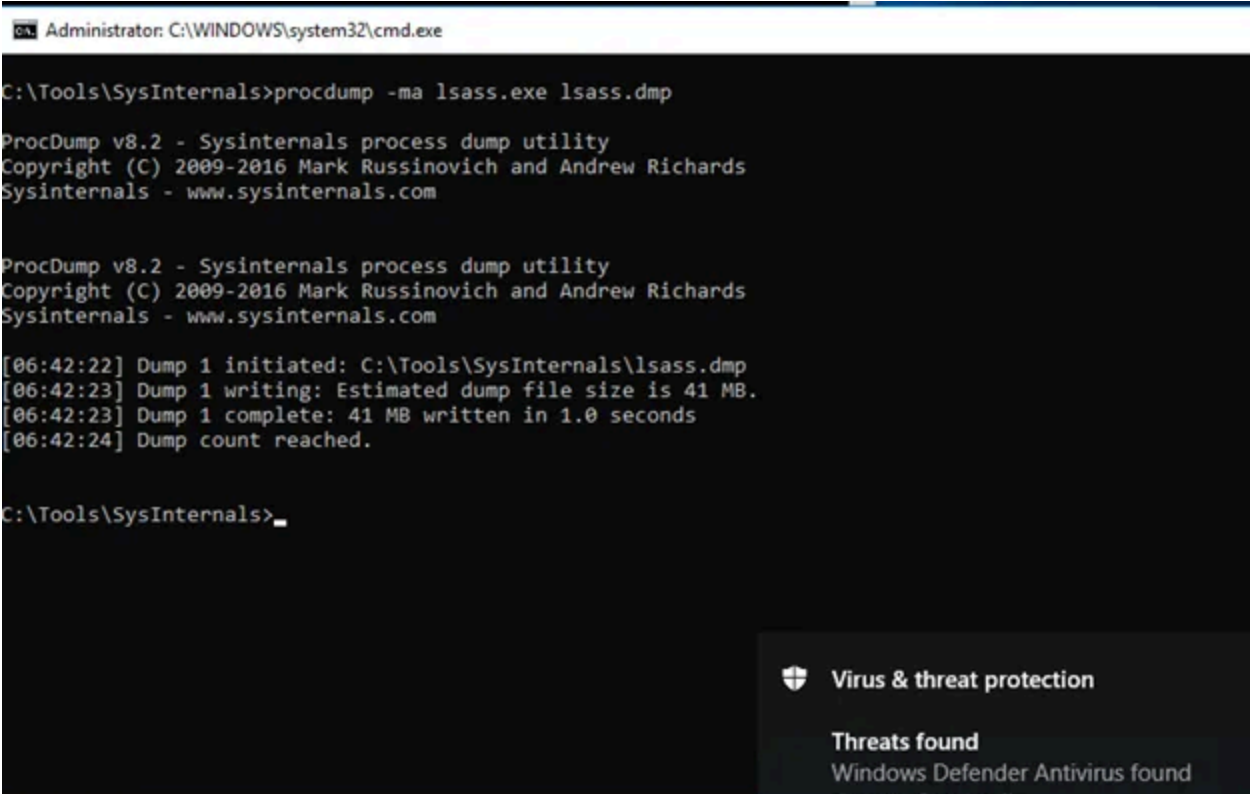
✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

First run a command as admin and run “psexec -i -s cmd” This will launch a command prompt as SYSTEM. This is the same as running “cmd” as with SYSTEM rights, windows defender lets it write to disk ***



Next run “procdump -ma lsass.exe lsass.dmp”



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

The dmp file is still produced though.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Here is the output file. As it suggests, rename the file to .GZ and you can unzip it and use it on your attacking machine to extract the NTLM hashes for cracking.

Next is Mini-Dump from @mattifestation
(<https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Out-Minidump.ps1>).

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Another way someone shared recently is Dumpert. Dumpert may be able to bypass AV (<https://github.com/outflanknl/Dumpert>) Here is a quote from the GitHub Repo

“This tool demonstrates the use of direct System Calls and API unhooking and combine these techniques in a proof of concept code which can be used to create a LSASS memory dump using Cobalt Strike, while not touching disk and evading AV/EDR monitored user-mode API calls.”

After compiling it, the repository suggests two ways to run it. First the EXE

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The second way is to run it using the dll. I copied all of the files from the

DI To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

co

```
rundll32 Outflank-Dumpert-DLL.dll,Dump
```

Also, I saw this technique recently as well from [@kondencuotas](#) but I wasn’t able to get it to work. I’m sure I’m doing something wrong. It may be worth a look as well.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

I’ll copy the NTLM hash and put it in a file for cracking on my Kali box

Here is a sample of some hashes I’m going to crack

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

When it finishes it will provide some feedback. I put the passwords in my
ro
th

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

I hope you learned at least one new way of dumping LSASS. Feel free to follow me on Twitter [_@markmo_](#) (yes with the underscores). Cheers!

- Infosec
- Security
- Purple Team

 200 

Medium

Sign up to discover human stories that deepen your understanding of the world.


Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app


To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

 Mark Mo

How to capture MSSQL credentials with xp_dirtree, smbserver.py

In security, we must show people how things can be misused before they take a threat...


Sep 22, 2018  186  1 

 Mark Mo

Kerberoasting - From setup to cracking

Feel free to follow me on Twitter at [@_markmo_](#) (yes with the underscores)


Dec 16, 2018  200  1 

 Mark Mo

Enable All Token Privileges

This is not new and all credit goes to Lee Holmes (@Lee_Holmes on twitter).

Sep 27, 2019  11  1 

 Mark Mo

Quick Introduction to ConfuserEX

I wanted to test this tool as soon as I saw it. I downloaded the binary from here linked in...

Aug 6, 2019  5 

See all from Mark Mo

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app


“From the author of the book ‘Red Team Shell A Shell Scripting Guide’”

Re

★


To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Lists




Staff Picks

755 stories · 1416 saves




Stories to Help You Level-Up at Work

19 stories · 852 saves




Self-Improvement 101

20 stories · 2960 saves




Productivity 101

20 stories · 2506 saves



Mavrogiannis Panagiotis



Nathan Hueck

Red Team Tactics: Exploiting Paste Jacking with PsycheShell for...

Introduction

Oct 8 🖱️ 1

🔖 +

KQL, XQL, and Splunk script to identify executable files in the...

We can begin with comprehensive approach to identifying executable files in the Window...

Jun 7

🔖 +

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Hel

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app