LOLBin — Execution via Diskshadow

Harjot Shah Singh · Follow
2 min read · Aug 30, 2023

Diskshadow.exe is a tool that exposes the functionality offered by the volume shadow copy Service (VSS). By default, Diskshadow uses an interactive command interpreter similar to that of Diskraid or Diskpart. Diskshadow also includes a scriptable mode.

DiskShadow is included in Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

. . .

Syntax

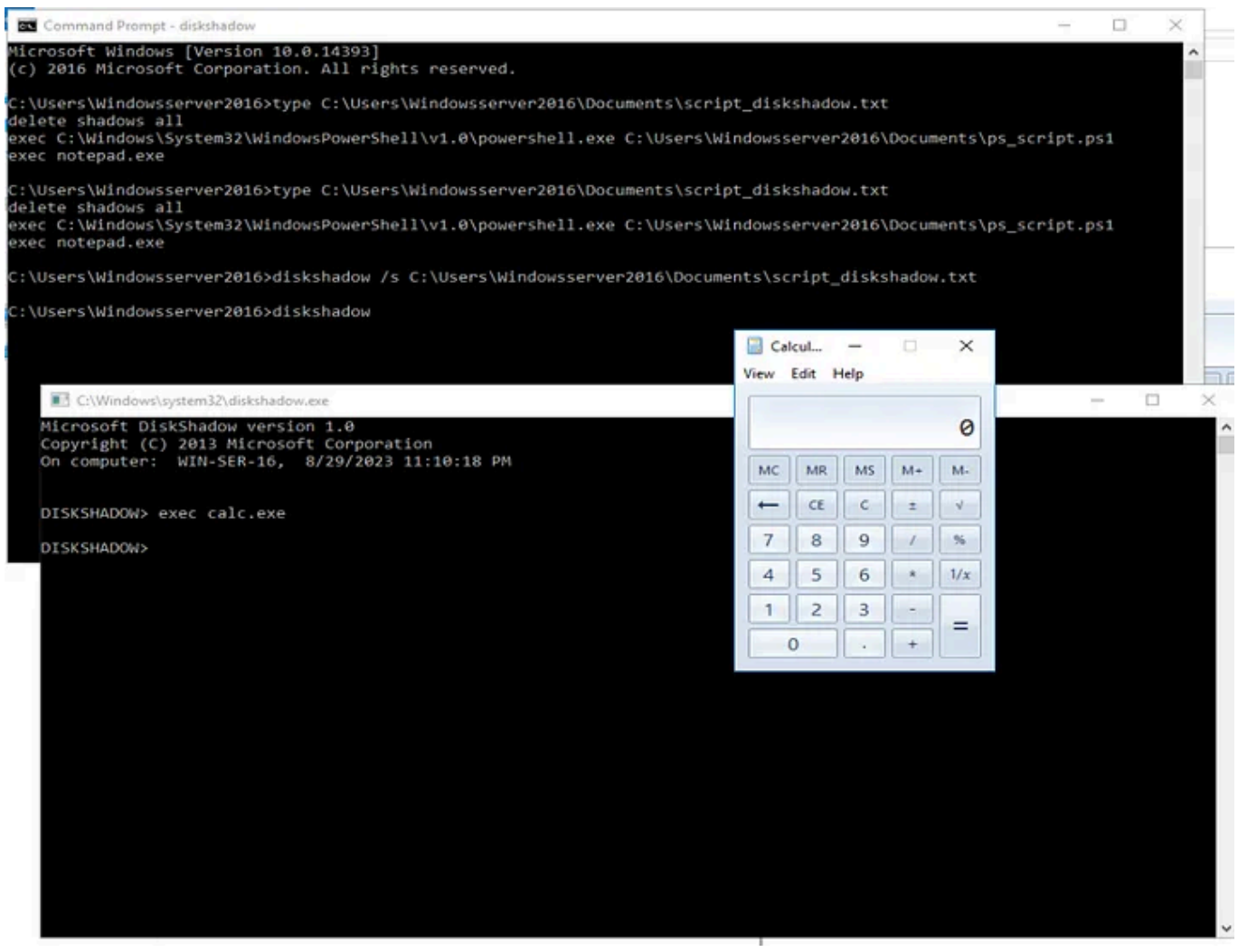
For interactive mode, type the following at the command prompt to start the Diskshadow command interpreter:

```
diskshadow
```

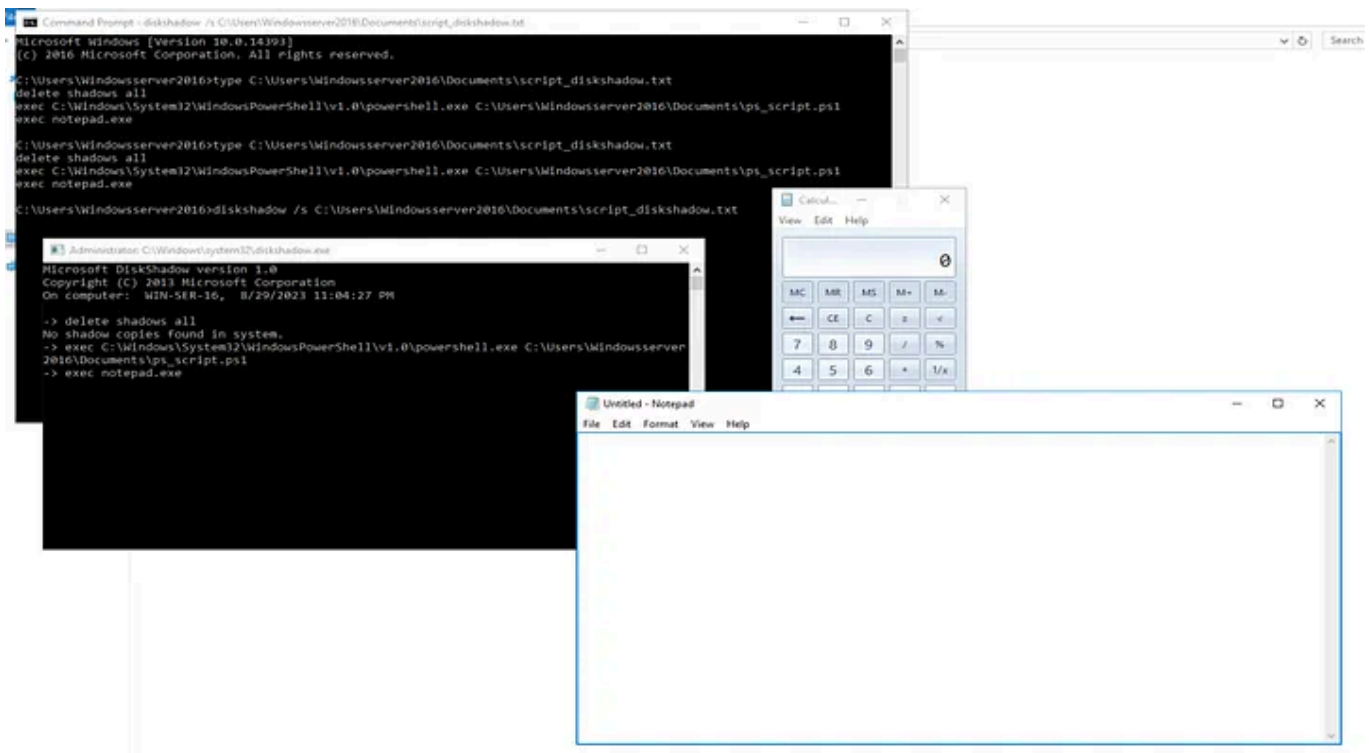
Note: These examples are taken from the usage of Diskshadow on Windows Se

Interactive Mode

```
C:\Users\Windowsserver2016>diskshadow
diskshadow> exec calc.exe
```



Diskshadow spawning Calc.exe



Diskshadow executing instructions in the script file

@timestamp	ev...	process.name	process.command_line	process.parent.name	process.parent.command_line
Aug 29, 2023 @ 23:04:27.826	1	win32calc.exe	"C:\Windows\System32\win32calc.exe"	calc.exe	"C:\Windows\system32\calc.exe"
Aug 29, 2023 @ 23:04:27.615	1	notepad.exe	notepad.exe	diskshadow.exe	"C:\Windows\system32\diskshadow.exe" /s C:\Users\Windowsserver2016\Documents\script_diskshadow.txt
Aug 29, 2023 @ 23:04:27.564	1	calc.exe	"C:\Windows\system32\calc.exe"	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Users\Windowsserver2016\Documents\ps_script.ps1
Aug 29, 2023 @ 23:04:27.336	1	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Users\Windowsserver2016\Documents\ps_script.ps1	diskshadow.exe	"C:\Windows\system32\diskshadow.exe" /s C:\Users\Windowsserver2016\Documents\script_diskshadow.txt
Aug 29, 2023 @ 23:04:27.302	1	VSSVC.exe	C:\Windows\system32\vssvc.exe	services.exe	C:\Windows\system32\services.exe
Aug 29, 2023 @ 23:04:27.230	1	conhost.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	diskshadow.exe	"C:\Windows\system32\diskshadow.exe" /s C:\Users\Windowsserver2016\Documents\script_diskshadow.txt
Aug 29, 2023 @ 23:04:27.221	1	diskshadow.exe	"C:\Windows\system32\diskshadow.exe" /s C:\Users\Windowsserver2016\Documents\script_diskshadow.txt	cmd.exe	"C:\Windows\system32\cmd.exe"

Captured logged when Diskshadow used in scripting mode

References

Diskshadow

Reference article for the Diskshadow command, which is a tool that exposes the functionality offered by the volume...

learn.microsoft.com

Diskshadow | LOLBAS

Diskshadow.exe is a tool that exposes the functionality offered by the volume shadow copy Service (VSS).

lolbas-project.github.io

DiskShadow: The Return of VSS Evasion, Persistence, and Active Directory Database Extraction

Source: blog.microsoft.com] Introduction Not long ago, I blogged about Vshadow: Abusing the Volume Shadow Service for...

bohops.com

Windows Diskshadow Proxy Execution

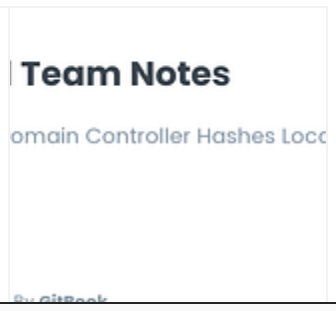
System Binary Proxy Execution

research.splunk.com

Dumping Domain Controller Hashes Locally and Remotely

Dumping NTDS.dit with Active Directory users hashes

www.ired.team



Written by Harjot Shah Singh

Follow

0 Followers

Cyb3rjy0t

More from Harjot Shah Singh

Harjot Shah Singh

T1218.008 — DLL execution using ODBCCONF.exe

What is ODBCConf.exe?

May 8, 2023

See all from Harjot Shah Singh

Recommended from Medium

Tech & Tools

Staff Picks

755 stories · 1416 saves

Medium's Huge List of

Natural Language Processing

1788 stories · 1391 saves

Dean

Setting Up Velociraptor for Forensic Analysis in a Home Lab |...

Before I start, Update you will not find article related to setting up Velociraptor in home la...

Oct 6

Austin Starks in DataDrivenInvestor

I used OpenAI's o1 model to develop a trading strategy. It is...

It literally took one try. I was shocked.

Sep 15 5.3K 138

Sagar Pandita

Understanding AMSI Bypass

Satyam Pathania in InfoSec Write-ups

Why I Don't Recommend People To