Get all OU via powerview.

```
PS C:\ad\ADModule-master\ActiveDirectory> Get-NetOU -FullData|select name, ou, gplink

name               ou                 gplink
----               --                 ------
Domain Controllers Domain Controllers [LDAP://CN={6AC1786C-016F-11D2-945F-
00C04fB984F9},CN=Policies,CN=System,DC=dollarcorp,DC=moneycorp,DC=local;0]
DCORPUSERS         DCORPUSERS
DCORPCOMPUTERS     DCORPCOMPUTERS     [LDAP://cn={0EDA91A0-9237-49C0-A172-
E1802566B29B},cn=policies,cn=system,DC=dollarcorp,DC=moneycorp,DC=local;0]
DCORPSERVERS       DCORPSERVERS       [LDAP://cn={582FF5A8-604C-42A7-81CB-
1C4D683597F4},cn=policies,cn=system,DC=dollarcorp,DC=moneycorp,DC=local;0]
DCORPPENTEST       DCORPPENTEST       [LDAP://cn={86D9D336-3C2D-4E02-AD67-
58CE78CA419D},cn=policies,cn=system,DC=dollarcorp,DC=moneycorp,DC=local;0]
```

Get computers in specific OU.

```
PS C:\ad\ADModule-master\ActiveDirectory> Get-NetOU -OUName "*pentest*" | %{Get-NetComputer -
ADSpath $_}
red.dollarcorp.moneycorp.local
```

List all GPO.

```
PS C:\ad\ADModule-master\ActiveDirectory> Get-NetGPO | select displayname, name

displayname                      name
-----------                      ----
Default Domain Policy            {31B2F340-016D-11D2-945F-00C04FB984F9}
Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04fB984F9}
PRODUCTION POLICY                {0EDA91A0-9237-49C0-A172-E1802566B29B}
SERVERS POLICY                   {582FF5A8-604C-42A7-81CB-1C4D683597F4}
PENTEST POLICY                   {86D9D336-3C2D-4E02-AD67-58CE78CA419D}
```

Get pentest OU gplink.

```
PS C:\ad\ADModule-master\ActiveDirectory> (Get-NetOU "*pentest*" -FullData)."gplink"
[LDAP://cn={86D9D336-3C2D-4E02-AD67-
58CE78CA419D},cn=policies,cn=system,DC=dollarcorp,DC=moneycorp,DC=local;0]
PS C:\ad\ADModule-master\ActiveDirectory>
```

Pentest policy is applied at pentest OU.

```
PS C:\ad\ADModule-master\ActiveDirectory> Get-NetGPO -ADSpath "LDAP://cn={86D9D336-3C2D-4E02-
AD67-58CE78CA419D},cn=policies,cn=system,DC=dollarcorp,DC=moneycorp,DC=local"


usncreated              : 21422
displayname             : PENTEST POLICY
whenchanged             : 26/10/2021 6:58:19 am
objectclass             : {top, container, groupPolicyContainer}
gpcfunctionalityversion : 2
showinadvancedviewonly  : True
usnchanged              : 21427
dscorepropagationdata   : 1/1/1601 12:00:00 am
name                    : {86D9D336-3C2D-4E02-AD67-58CE78CA419D}
adspath                 : LDAP://CN={86D9D336-3C2D-4E02-AD67-
58CE78CA419D},CN=Policies,CN=System,DC=dollarcorp,DC=moneycorp,DC=local
flags                   : 0
cn                      : {86D9D336-3C2D-4E02-AD67-58CE78CA419D}
gpcfilesyspath          :
\\dollarcorp.moneycorp.local\SysVol\dollarcorp.moneycorp.local\Policies\{86D9D336-3C2D-4E02-
AD67-58CE78CA419D}
distinguishedname       : CN={86D9D336-3C2D-4E02-AD67-
58CE78CA419D},CN=Policies,CN=System,DC=dollarcorp,DC=moneycorp,DC=local
whencreated             : 26/10/2021 6:58:18 am
versionnumber           : 0
```

```
instancetype             : 4
objectguid               : b47c936e-2649-46e0-94c3-3bd2b97de369
objectcategory           : CN=Group-Policy-
Container,CN=Schema,CN=Configuration,DC=moneycorp,DC=local
```