在 Active Directory 中发现服务的最佳方式是 SPN 扫描。这种方式不一定是全的，但是是完全不会产生任何告警的让你了解域框架的方式。

作者系统的说明了相关的技巧并且在下面的链接里详细描述了 SPN 的各种服务的格式。
https://adsecurity.org/?page_id=183

例：
MSSQL Server 数据库
MSSQLSvc /adsmsSQLAP01.adsecurity.org ： 1433

exchange
exchangeMDB /adsmsEXCAS01.adsecurity.org

RDP
TERMSERV /adsmsEXCAS01.adsecurity.org

WSMan / WinRM / PS Remoting
WSMAN /adsmsEXCAS01.adsecurity.org

Hyper-V 主机
Microsoft Virtual Console Service/adsmsHV01.adsecurity.org

VMWare VCenter
STS /adsmsVC01.adsecurity.org

作者放出了一个工具包，关于 AD Recon
https://github.com/PyroTek3/PowerShell-AD-Recon

```
PS [redacted]\PowerShell-AD-Recon-master> ls


    目录: E:\2_neiwang\powershell\tools\PowerShell-AD-Recon-master


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---          2015/3/9      9:20      15963 Discover-PSInterestingServices.ps1
-a---          2015/3/9      9:20       8169 Discover-PSMSExchangeServers.ps1
-a---          2015/3/9      9:20      13748 Discover-PSMSSQLServers.ps1
-a---          2015/3/9      9:20       9493 Find-PSServiceAccounts.ps1
-a---          2015/3/9      9:20        989 Get-DomainKerberosPolicy.ps1
-a---          2015/3/9      9:20      14531 Get-PSADForestInfo.ps1
-a---          2015/3/9      9:20       4412 Get-PSADForestKRBTGTInfo.ps1
-----          2015/3/9      9:20       1485 LICENSE
-----          2015/3/9      9:20         56 README.md
```

其中包括了几种信息的查询工具，举例 Discover-PSMSSQLServers.ps1

```
PS [redacted] Import-Module .\Discover-PSMSSQLServers.ps1
PS [redacted] Discover-PSMSSQLServers
Processing 56 (user and computer) accounts with MS SQL SPNs discovered in AD Forest DC=ESG,DC=360ES,DC=CN
无法对 Null 数组进行索引。
所在位置 E:\2_neiwang\powershell\tools\PowerShell-AD-Recon-master\Discover-PSMSSQLServers.ps1:166 字符: 29
+                              [string]$ADServiceAccountSAMAccountName = $ADService ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [], RuntimeException
    + FullyQualifiedErrorId : NullArray


Domain            : ESG.360ES.CN
ServerName        : hand-白文斌.ESG.360ES.CN
Port              : 1433
Instance          :
ServiceAccountDN  :
OperatingSystem   : {Windows 10 企业版}
OSServicePack     :
LastBootup        : 2018/9/12 14:25:31
OSVersion         : {10.0 (17134)}
Description       :

Domain            : ESG.360ES.CN
ServerName        : CP-SQL2.ESG.360ES.CN
Port              : 1433
Instance          :
ServiceAccountDN  :
OperatingSystem   : {Windows Server 2016 Standard}
OSServicePack     :
LastBootup        : 2019/7/13 4:56:30
OSVersion         : {10.0 (14393)}
Description       :

Domain            : ESG.360ES.CN
ServerName        : A004602-NC.ESG.360ES.CN
Port              : 1433
Instance          :
ServiceAccountDN  :
OperatingSystem   : {Windows 7 企业版}
OSServicePack     : {Service Pack 1}
LastBootup        : 2019/7/11 17:53:02
OSVersion         : {6.1 (7601)}
Description       :
```

可以看到域中注册了的 MSSQL