说明

2015 年 8 月 Mimkatz 增加的一个主要功能是“DCSync”，它有效地“模仿”域控制器并从目标域控制器请求帐户密码数据。DCSync 由 Benjamin Delpy 和 Vincent Le Toux 编写。

DCSync 之前的利用方法是在域控制器上运行 Mimikatz 或 Invoke-Mimikatz 以获取 KRBTGT 密码哈希来创建 Golden Tickets。然而借助 Mimikatz 的 DCSync 和相应的权限，攻击者可以通过网络从域控制器提取密码哈希以及以前的密码哈希，而无需交互式登录或复制 Active Directory 数据库文件（ntds.dit）。（也就是说从本地转为远程）。

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::dcsync /user:xiaom /domain:yunying.lab
[DC] 'yunying.lab' will be the domain
[DC] 'dc2012.yunying.lab' will be the DC server
[DC] 'xiaom' will be the user account

Object RDN           : xiaom

** SAM ACCOUNT **

SAM Username         : xiaom
User Principal Name  : xiaom@yunying.lab
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 2019/7/11 0:42:00
Object Security ID   : S-1-5-21-4054579877-26337388-655639334-1133
Object Relative ID   : 1133

Credentials:
  Hash NTLM: 8bbe95fcb83756d902da7faccd2fa6e1
    ntlm- 0: 8bbe95fcb83756d902da7faccd2fa6e1
    lm  - 0: 657bc75bb0655c66d50ab93025c1f510

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : YUNYING.LABxiaom
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 241fa5dbb318fd813707abf146c1d006bba732f7996c0d2732df19f2ea9af5da
      aes128_hmac       (4096) : a07322ecda4b7e2145a5d35c7fe102b6
      des_cbc_md5       (4096) : 0b37b0804a89b3b9
```

同时要说明的是在最新的 Exchange 中通过 NTLMRelay 最后实现的功能也是 DCSync

工作原理

1、 在指定的域名中发现域控
2、 通过 GetNCChanges 请求域控复制用户凭据。（使用 Directory Replication Services DRS 目录复制服务远程协议）

[MS-DRSR]：目录复制服务（DRS）远程协议

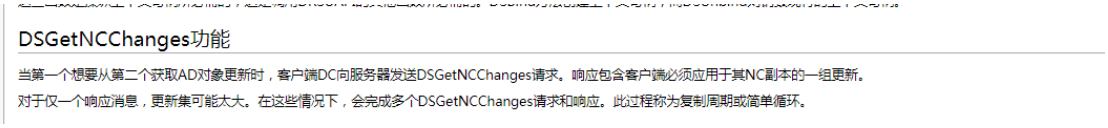
2019年2月15日 • 4分钟阅读

指定目录复制服务（DRS）远程协议，这是一种用于在Active Directory中复制和管理数据的RPC协议。

可以频繁更新该页面和相关内容。我们建议您订阅RSS源以接收更新通知。

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-drsr/f977faaa-673e-4f66-b9bf-48c640241d47
详细信息可以参考官方文档提供的关于目录复制服务的简单说明
这个协议的主要作用其实是为了多个域控的环境中不同域控之间同步信息时使用的，主要是为了域控之间信息的一致性。

大多数复制相关任务都在目录复制服务（DRS）远程协议上指定。实现此类协议的 Microsoft API 称为 DRSUAPI。
https://wiki.samba.org/index.php/DRSUAPI

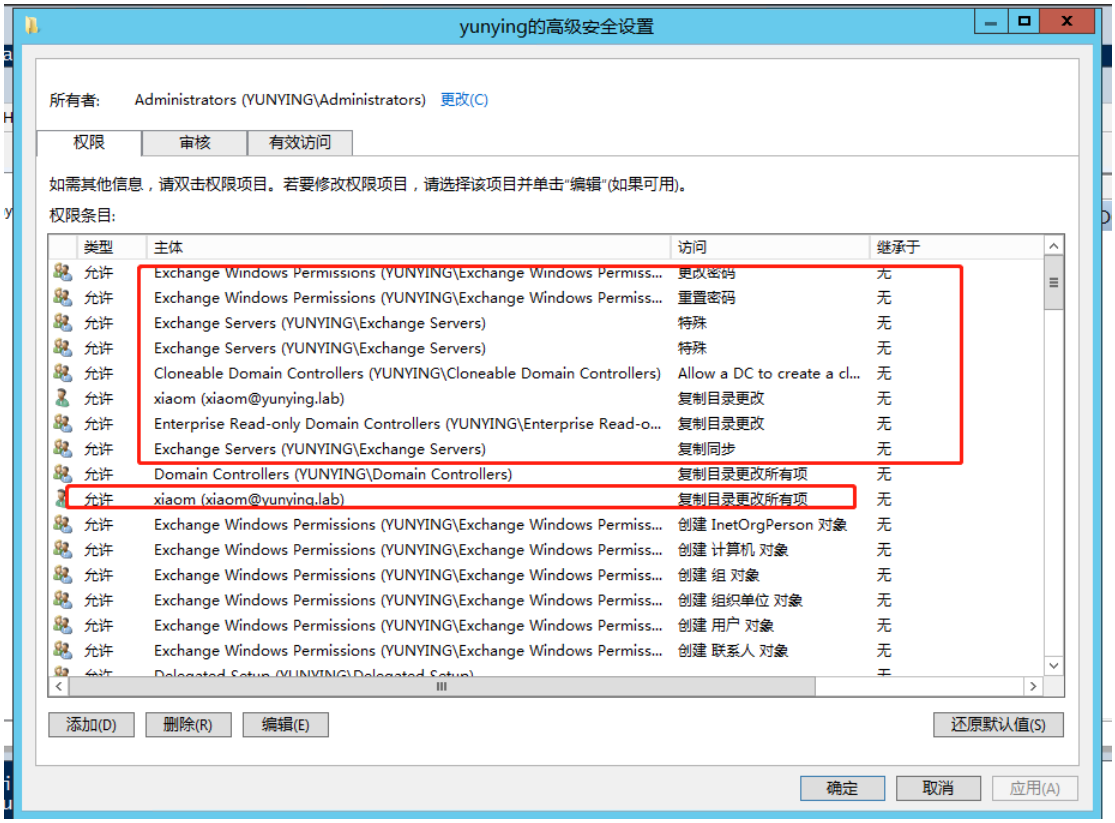

DSGetNCChanges功能
当第一个想要从第二个获取AD对象更新时，客户端DC向服务器发送DSGetNCChanges请求。响应包含客户端必须应用于其NC副本的一组更新。
对于仅一个响应消息，更新集可能太大。在这些情况下，会完成多个DSGetNCChanges请求和响应。此过程称为复制周期或简单循环。

DCSync 使用的就是 DRSUAPI 中的 DSGetNCChanges 接口。
文中描述可以理解为，当一个（攻击者）想到从另一个（域控）中获取更新时，就会发起 DSGetNCChanges 请求，响应包含客户端必须应用于其 NC 副本的一组更新（域用户 HASH 值）。

Delegating Rights to Pull Account data:

（获取数据的委派权限？感觉怪怪的）
可以使用常规域用户进行 DCSync，前提是要委派给这个域用户以下三个权限（应该是其中之一）。

复制目录更改 Replicating Directory Changes (DS-Replication-Get-Changes)
复制目录更改所有 Replicating Directory Changes All (DS-Replication-Get-Changes-All)（Exchange 用的就是这个）
正在复制筛选集中的目录更改 Replicating Directory Changes In Filtered Set (rare, only required in some environments)



把普通域账号 xiaom 添加了复制目录更改所有项之后，这个账号就可以在域中进行 DCSync

可以看到默认情况下 Administrators 组和 Domain Controller 组的成员具有这些权限。

DCSync 的检测

只要是非两个域控之间的 DsGetNCChange 请求都可以高度怀疑为 DCSync/DCShadow 攻击。

也就是说可以在防御的时候将域控之间设置为白名单（两个域控之间为正常），域内主机对发起攻击即判断为 DCSync 或者是 DCShadow。